



Routledge Studies in Conflict, Security and Technology

CYBERSECURITY IN LATVIA

FORGING RESILIENCE AMIDST EMERGING THREATS

Edited by
Mihails Potapovs and Kate E. Kanasta



Cybersecurity in Latvia

Drawing on expertise from professionals, government officials, and academics, this book uncovers the proactive measures taken by Latvia to build resilient cybersecurity capabilities.

The work offers a comprehensive exploration of Latvia's cyber domain, structured around three overarching themes: the ecosystem, its processes, and future perspectives. In doing so, it takes readers through the intricacies of Latvia's cybersecurity landscape and provides a nuanced understanding of its strengths, challenges, strategic considerations, and broader implications. One of the key contributions of the work lies in its exploration of Latvia's cybersecurity strategies and resilience. By delving into the nation's policies, collaborations, and technological advancements, this book uncovers how Latvia has proactively addressed cyber threats, emphasising the importance of tailored approaches for smaller countries in building robust cybersecurity defences. Highlighting the importance of studying cybersecurity in smaller nations, this book stresses Latvia's contributions to global cybersecurity efforts as an EU and NATO member. The volume advocates for innovation and collaboration, emphasising their crucial role in securing a digital future for nations worldwide.

This book will be of much interest to student of cybersecurity, Baltic politics, EU politics, global governance, and International Relations.

Mihails Potapovs is the Head of the European Union Cybersecurity Affairs Section at the Ministry of Defence of the Republic of Latvia and lecturer and PhD candidate at the Faculty of Economics and Social Sciences, University of Latvia.

Kate E. Kanasta is a representative of the Ministry of Defence of the Republic of Latvia to the European Union and a PhD candidate at the Faculty of Economics and Social Sciences, University of Latvia.

Routledge Studies in Conflict, Security and Technology

Series Editors: Mark Lacy, *Lancaster University*, Dan Prince, *Lancaster University*, and Sean Lawson, *University of Utah*

The Routledge Studies in Conflict, Technology and Security series aims to publish challenging studies that map the terrain of technology and security from a range of disciplinary perspectives, offering critical perspectives on the issues that concern publics, business and policymakers in a time of rapid and disruptive technological change.

Military Design Thinking

An Historical and Paradigmatic Analysis

Aaron P. Jackson

Theorising Cyber (In)Security

Information, Materiality, and Entropic Security

Noran Shafik Fouad

Creativity in Military Complexity

Design, Disruptors and Defence Forces

Cara Wrigley and Murray Simons

Digital (Dis)Information Operations

Fooling the Five Eyes

Edited by Melissa-Ellen Dowling

Cybersecurity in Latvia

Forging Resilience amidst Emerging Threats

Edited by Mihails Potapovs and Kate E. Kanasta

Cybersecurity in Latvia

Forging Resilience amidst Emerging Threats

Edited by

Mihails Potapovs and Kate E. Kanasta

First published 2026
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

© 2026 selection and editorial matter, Mihails Potapovs and Kate E. Kanasta;
individual chapters, the contributors

The right of Mihails Potapovs and Kate E. Kanasta to be identified as the
authors of the editorial material, and of the authors for their individual
chapters, has been asserted in accordance with sections 77 and 78 of the
Copyright, Designs and Patents Act 1988.

The Open Access version of this book, available at www.taylorfrancis.com,
has been made available under a Creative Commons Attribution-Non
Commercial-Share Alike (CC-BY-NC-SA) 4.0 International license.

Any third party material in this book is not included in the OA Creative
Commons license, unless indicated otherwise in a credit line to the material.
Please direct any permissions enquiries to the original rightsholder.

Trademark notice: Product or corporate names may be trademarks or
registered trademarks, and are used only for identification and explanation
without intent to infringe.

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

ISBN: 9781041071068 (hbk)

ISBN: 9781041071075 (pbk)

ISBN: 9781003638858 (ebk)

DOI: 10.4324/9781003638858

Typeset in Times New Roman
by codeMantra

To the cybersecurity professionals, researchers, policymakers, and all individuals who tirelessly work to protect our digital infrastructure.

To the guardians of Latvia's cyberspace, whose dedication and innovation have strengthened our nation's defence against ever-evolving threats.

To the visionaries who recognise that a secure digital future is built not just through technology, but through collaboration, education, and shared determination.

And to all who believe in the power of resilience, even in the face of the most daunting challenges.

May this work inspire continued efforts to safeguard the interconnected world we all share.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Contents

| | |
|---|-------------|
| <i>List of Figures</i> | <i>ix</i> |
| <i>List of Tables</i> | <i>xi</i> |
| <i>List of Boxes</i> | <i>xiii</i> |
| <i>List of Contributors</i> | <i>xv</i> |
| <i>Foreword</i> | <i>xvii</i> |
| <i>Acknowledgements</i> | <i>xix</i> |
| | |
| 1 Introduction: Why Study Cybersecurity in Latvia? | 1 |
| MIHAILS POTAPOVS AND KATE E. KANASTA | |
| | |
| 2 The Cybersecurity Ecosystem of Latvia: Mapping and Analysis | 11 |
| JĀNIS GRABIS AND LINDA VITKAUA | |
| | |
| 3 Governance of the Latvian Cybersecurity Ecosystem | 32 |
| MIHAILS POTAPOVS, IVETA REINHOLDE AND KRISTIĀNS TETERS | |
| | |
| 4 Evaluating National CSIRT Maturity: The Case of CERT.LV | 52 |
| MIHAILS POTAPOVS, KRISTIĀNS TETERS, JĀNIS FRĪDMANIS AND BERNHARDS BLUMBERGS | |
| | |
| 5 Societal Resilience in Latvia: The Cybersecurity Perspective | 74 |
| SIGITA STRUBERGA AND ŽANETA OZOLIŅA | |
| | |
| 6 Latvian Approach to Fighting Cybercrime: Criminal Liability, Problems, and Solutions | 99 |
| ULDIS ĶINIS | |

| | | |
|-----------|--|------------|
| 7 | Latvia in the European Cybersecurity Ecosystem | 129 |
| | MIHAILS POTAPOVS AND STELLA BLUMFELDE | |
| 8 | Cyber Diplomacy: Latvia's Voice in the World | 150 |
| | DIDZIS KĻAVIŅŠ | |
| 9 | Cybersecurity Transformation in Latvia | 175 |
| | HEINRIHS K. SKRODELIS, MĀRTIŅŠ ŠTĀLS AND ANDREJS ROMĀNOVS | |
| 10 | Shaping the Latvian Cyber Workforce of Tomorrow | 200 |
| | RŪTA PIRTA AND MATĪSS VEIGURS | |
| 11 | Cyber-Physical Systems: Securing Latvia's Future | 233 |
| | KRIŠJĀNIS NESENBERGS, EDUARDS BLUMBERGS AND PĒTERIS PAIKENS | |
| 12 | Cyber Threats of Tomorrow | 264 |
| | KATE E. KANASTA | |
| | <i>Index</i> | 275 |

Figures

| | | |
|------|--|-----|
| 2.1 | The cybersecurity ecosystem goals | 17 |
| 2.2 | Business goals of <i>education institutions</i> | 18 |
| 2.3 | The cybersecurity ecosystem roles | 20 |
| 2.4 | Relationships among the cybersecurity roles and the resilience roles | 21 |
| 2.5 | A fragment of the Latvian cybersecurity ecosystem graph | 26 |
| 2.6 | A view of the Latvian cybersecurity ecosystem graph showcasing events and individuals presenting at two or more events | 27 |
| 2.7 | Organisational entities organising or sponsoring at least two cybersecurity events | 28 |
| 2.8 | Community clusters in the Latvian cybersecurity ecosystem | 28 |
| 4.1 | Distribution of compromised IP addresses from incidents identified by CERT.LV in 2024 (CERT.LV, 2025) | 60 |
| 5.1 | Research methodology overview | 78 |
| 7.1 | A conceptual model of a fragment of the EU cybersecurity ecosystem | 132 |
| 10.1 | Research methodology | 206 |
| 10.2 | Latvian higher education system | 213 |
| 10.3 | Latvian CS professional standards | 217 |
| 10.4 | Latvian CS roles in organizations (survey data, 45 organizations) | 220 |
| 10.5 | Latvian CS specialists' education level (survey data, 45 organizations) | 221 |
| 10.6 | Competences gaps of Latvian organizations (survey data, 45 organizations) | 222 |
| 10.7 | Future CS competency needs (survey data, 45 organizations) | 222 |
| 11.1 | Total Bluetooth shipments by radio version (SIG, 2024) | 237 |
| 11.2 | Most popular IoT and ICS products in Latvia as indexed by Shodan (2024-07-24) | 244 |
| 11.3 | Products tagged as ICS by Shodan (2024-07-24) | 245 |
| 11.4 | Common internet-connected devices in Latvia identified by Shodan via favicon hashes (2024-07-24) | 247 |
| 11.5 | Potential mobile vulnerabilities, threats, and attack vectors. Figure by the authors | 253 |



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Tables

| | | |
|------|---|-----|
| 2.1 | Notation used to model Latvian cybersecurity ecosystem | 15 |
| 2.2 | Analysis of cybersecurity ecosystem roles defined in literature | 19 |
| 2.3 | The list of main cybersecurity events in Latvia | 22 |
| 2.4 | Organisational units fulfilling generic roles in the Latvian cybersecurity ecosystem | 24 |
| 2.5 | Top organisational entities by number of joint event participations | 27 |
| 3.1 | Types of path dependency observed in the case study | 45 |
| 4.1 | Classification of cyber incidents by severity. Adapted by CERT. LV from the UK’s National Cyber Security Centre (2023) | 60 |
| 6.1 | Registered criminal cases from 2021 to 2023 (Ministry of the Interior, 2024) | 123 |
| 7.1 | Assessment of Latvia’s involvement in the EU cybersecurity ecosystem – policy and legislation domain | 142 |
| 7.2 | Assessment of Latvia’s involvement in the EU cybersecurity ecosystem – capacity-building domain | 144 |
| 7.3 | Assessment of Latvia’s involvement in the EU cybersecurity ecosystem – cyber defence domain | 144 |
| 10.1 | CS knowledge, skills and competences matrix of Latvian general basic education standards (Ministru kabineta noteikumi Nr. 416, 2019; Ministru kabineta noteikumi Nr. 747, 2018) | 209 |
| 10.2 | Illustrative examples of CS courses in undergraduate and graduate study programmes | 216 |
| 10.3 | Latvian CS vacant roles overview (data on 15.03.2024) | 218 |
| 10.4 | Organizations recommendations for CS capabilities strengthening (data on 30.04.2024) | 226 |
| 10.5 | Future CS skills recommendations (data on 30.04.2024) | 229 |



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Boxes

| | | |
|-----|--|-----|
| 4.1 | Article 11(3) of the NIS Directive—Tasks of CSIRTs | 55 |
| 5.1 | Key Policy Recommendations for Strengthening Societal Cyber Resilience | 95 |
| 6.1 | Excerpt from Section 144 of the Criminal Law (1998) | 105 |
| 6.2 | Excerpts from Section 241 of the Criminal Law (1998) | 108 |
| 6.3 | Excerpt from Section 243 of the Criminal Law (1998) | 111 |
| 6.4 | Excerpts from Section 243 of the Criminal Law (1998) | 112 |
| 6.5 | Excerpt from Section 244 of the Criminal Law (1998) | 113 |
| 6.6 | Excerpt from Section 177 of the Criminal Law (1998) | 115 |
| 6.7 | Excerpt from Section 191 of the Criminal Procedure Law (2005) | 119 |
| 6.8 | Excerpt from Section 23(1) of the Law on the Procedures for Coming into Force and Application of the Criminal Law (1998) | 124 |



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Contributors

Bernhards Blumbergs is a lead cybersecurity expert at CERT.LV, Institute of Mathematics and Computer Science, University of Latvia, and visiting research professor at the Nara Institute of Science and Technology, Japan.

Eduards Blumbergs is a computer systems analyst at the Institute of Mathematics and Computer Science, University of Latvia, and research assistant at the Institute of Electronics and Computer Science, Latvia.

Stella Blumfelde is a postdoctoral researcher at the Department of Political and Social Sciences, University of Bologna, Italy, and an OSCE Young Expert in Cybersecurity, as well as an Alumnus of the Virtual Routes European Cybersecurity Fellowship

Jānis Frīdmanis is a systems analyst at CERT.LV, Institute of Mathematics and Computer Science, University of Latvia.

Jānis Grabis is a Professor and Director of the Information Technology Institute, Riga Technical University, Latvia.

Kate E. Kanasta is a representative of the Ministry of Defence of the Republic of Latvia to the European Union and a PhD candidate at the Faculty of Economics and Social Sciences, University of Latvia.

Uldis Ķinis is a Professor at the Faculty of Law, Riga Stradiņš University, Latvia, and a former Vice-President of the Constitutional Court of the Republic of Latvia.

Didzis Kļaviņš is a senior researcher at the Faculty of Economics and Social Sciences, University of Latvia.

Krišjānis Nesenbergs is a researcher and member of the Scientific Council at the Institute of Electronics and Computer Science, Latvia.

Žaneta Ozoliņa is a senior researcher at the Advanced Social and Political Research Institute, University of Latvia.

Pēteris Paikens is an Associate Professor at the Faculty of Science and Technology, University of Latvia, and a senior researcher at the Institute of Mathematics and Computer Science, University of Latvia.

Rūta Pirta is an Assistant Professor and a senior researcher at the Information Technology Institute, Riga Technical University, Latvia.

Mihails Potapovs is the Head of European Union Cybersecurity Affairs at the Ministry of Defence of the Republic of Latvia and a lecturer and PhD candidate at the Faculty of Economics and Social Sciences, University of Latvia.

Iveta Reinholde is the Vice-Dean for Research and Professor at the Faculty of Economics and Social Sciences, University of Latvia.

Andrejs Romānovs is an Associate Professor and a senior researcher at the Information Technology Institute, Riga Technical University, Latvia.

Heinrihs K. Skrodelis is a research assistant at the Information Technology Institute, Riga Technical University, Latvia.

Mārtiņš Štāls is a lecturer and researcher at the Institute of Computer Systems and Data Science, Latvia University of Life Sciences and Technologies.

Sigita Struberga is a lecturer at the Faculty of Economics and Social Sciences, University of Latvia, and the Secretary-General of the Latvian Transatlantic Organization (LATO).

Kristiāns Tetters is the Head of Governance and Compliance at CERT.LV, Institute of Mathematics and Computer Science, University of Latvia.

Matīss Veigurs is a systems analyst at the National Cybersecurity Centre, Ministry of Defence of the Republic of Latvia.

Linda Vitkaua is a former head of Cybersecurity Projects at the National Cybersecurity Centre, Ministry of Defence of the Republic of Latvia.

Foreword

Cybersecurity has become an indispensable element of national security in the 21st century. The hybrid nature of contemporary threats, as demonstrated by Russia's barbaric war of aggression against Ukraine, has underscored the critical role of cyber resilience in safeguarding our sovereignty, democratic values, and way of life. Cyber operations have become an integral part of modern warfare, targeting critical infrastructure, disrupting communication systems, and undermining public trust through disinformation. In this rapidly evolving threat landscape, Latvia remains resolute in its commitment to strengthening cybersecurity as a pillar of national defence.

The Latvian State Defence Concept 2023 emphasises the necessity of robust cybersecurity and cyber-defence capabilities to counteract growing threats. Our strategic approach is built upon resilience, deterrence, and collective defence, ensuring that Latvia can withstand and respond effectively to cyber and hybrid attacks. By integrating cybersecurity into our comprehensive state defence strategy, we are reinforcing our digital infrastructure, enhancing cooperation with our international allies, and fostering a whole-of-society approach to cyber resilience.

It is within this context that *Cybersecurity in Latvia* emerges as a pioneering academic contribution. This book is the first scholarly volume dedicated to analysing Latvia's cybersecurity ecosystem in depth, providing a thorough examination of its governance structures, threat environment, and resilience-building measures. Through a multidisciplinary approach, the authors illuminate Latvia's strategic responses to cybersecurity challenges, offering valuable insights for policymakers, researchers, and practitioners. This book serves not only as a record of Latvia's cybersecurity evolution but also as a roadmap for strengthening our national digital defences in an increasingly contested cyberspace.

Latvia's cybersecurity efforts are deeply intertwined with our membership in NATO and the European Union, where we play an active role in strengthening collective cybersecurity initiatives. The importance of international cooperation cannot be overstated, as cyber threats transcend borders and demand coordinated responses. Our enhanced collaboration with allies not only fortifies Latvia's capacity to protect its digital infrastructure against cyberattacks but also contributes to intelligence sharing, capability development, and the implementation of best practices in cyber defence. This reciprocal exchange not just strengthens Latvia's

cybersecurity posture but also reinforces the collective resilience of our allies, ensuring a safer and more secure digital environment for all.

Our cyber resilience is not solely dependent on government efforts. A strong cybersecurity culture requires active engagement from the private sector, academia, and civil society. Education and awareness are crucial in building a cyber-literate society capable of recognising and mitigating threats. Collaboration between these sectors fosters innovation, enhances threat detection, and strengthens national cyber defences. Moreover, investment in research and development, alongside international knowledge exchange, is essential for staying ahead of emerging cyber threats. This book highlights the significance of these efforts, reinforcing the notion that cybersecurity is a shared responsibility.

I commend the authors and contributors of *Cybersecurity in Latvia* for their dedication to this vital field. Their work provides a valuable foundation for understanding the challenges and opportunities in securing Latvia's digital landscape. In an era where cyber threats are ever-present and evolving, this book is an essential resource for those committed to safeguarding Latvia's national security in the digital age. Furthermore, the insights and strategies outlined in this volume are highly relevant for other like-minded nations facing similar threats. By sharing Latvia's experiences, this book contributes to the broader discourse on cyber resilience, fostering collaboration and knowledge exchange among countries striving to enhance their digital defences. I invite readers to explore the insights presented in this volume, engage with its findings, and contribute to the ongoing discussions on strengthening cybersecurity in an increasingly interconnected and volatile world.

Andris Sprūds
Minister of Defence of the Republic of Latvia

Acknowledgements

This publication is the result of a research conducted with the support of the European Cybersecurity Competence Centre (ECCC), co-funded by the European Union under the Digital Europe programme (Grant Agreement No. 101127985). The opinions expressed in this book are solely those of the authors in their capacity as academic researchers. They do not necessarily reflect the official positions or policies of the European Union, the government of Latvia, or any other institution.



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union



Ministry of Defence
Republic of Latvia



**National
Cybersecurity
Centre of Latvia**



Cyber Incident
Response Institution



Institute of Mathematics and
Computer Science University of Latvia



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

1 Introduction

Why Study Cybersecurity in Latvia?

Mihails Potapovs and Kate E. Kanasta

A Wake-Up Call for Europe: The Threats of Modern Warfare

On February 24, 2022, Russia launched a full-scale invasion of Ukraine, a move that stunned much of the world. Massive columns of vehicles and troops poured over the Ukrainian border from multiple directions, aiming to capture the capital Kyiv and major cities. Russian missiles struck targets across Ukraine, assault troops attempted to seize the airport of Hostomel near Kyiv, and clandestine operatives launched multiple assassination attempts on President Zelenskyy and his closest collaborators. The conventional military campaign was accompanied by a massive hybrid operation, including cyberattacks designed to disrupt and destroy Ukraine's critical infrastructure, as well as disinformation efforts to sow chaos and fear (Willett, 2022). This was the largest attack on a European country and the first full-scale war in Europe since the Second World War, showcasing the magnitude and complexity of threats we face today. These are not merely remnants of the past but the stark reality of the present.

While conventional armed conflicts in Europe have become less frequent, hybrid and cyber warfare have become the everyday reality for countries with the unfortunate "pleasure" of sharing a border with Russia, or being within Russia's "sphere of interests" (Barrinha, 2018; Kozlowski, 2014; Pernik et al., 2018; Stronski & Himes, 2022). Over the last two decades, Latvia, Estonia, and Lithuania have been targeted by countless cyberattacks, ranging in scale and complexity. Notably, Russia's first massive cyberattack against Estonia in 2007 served as a wake-up call for the region and the world, exposing the vulnerabilities of critical infrastructure, sparking efforts to build cyber resilience, and provoking discussions on the legal nature of cyber warfare (Haataja, 2017; Ilves, 2016; Mansfield-Devine, 2012). This attack was far from an isolated event; all three Baltic states have faced persistent and varied cyber threats ever since.

Following Russia's full-scale war of aggression against Ukraine, Poland, and the Baltic states, vocal proponents of providing military support to Ukraine became the top targets for Russia's cyberattacks in the European Union. In 2022–2023, Latvia, Estonia, and Lithuania collectively were targeted by approximately 32% of all cyberattacks against EU member states (CERT-EU, 2023). However, while the full-scale conventional invasion of Ukraine took many by surprise, the spike

2 *Cybersecurity in Latvia*

in cyberattacks did not surprise the Baltic states. Years of experience in dealing with Russia's malicious cyber activities have fostered resilience and prepared these nations to counter and adapt to such threats.

In an era where digital interconnectedness shapes the very fabric of our societies, cybersecurity has emerged as a paramount concern for nations, industries, and individuals alike. The exponential growth of digital technologies and the proliferation of cyber threats have propelled cybersecurity to the forefront of national security and global stability discourses. Effective mitigation of cyber threats requires a whole-of-society and whole-of-government approach that emphasises the necessity for collaboration across various sectors and levels of governance. In this framework, government entities, private organisations, and individual citizens are seen as integral components of a unified defence strategy. Amidst these developments, Latvia—a small but dynamic European nation with its comprehensive state defence system—has emerged as a case study in resilience, innovation, and collaboration in the face of growing cybersecurity challenges.

Why Latvia? Understanding Cyber Resilience in a Unique Geopolitical Context

Latvia's cybersecurity narrative is both unique and instructive. As a small nation with a population of less than 2 million, Latvia faces challenges distinct from those of larger countries. Limited resources, a concentrated and somewhat limited cyber workforce, and reliance on international cooperation are defining characteristics of its cybersecurity landscape. However, Latvia's experience underscores an essential truth: resilience is not solely a function of size but also of strategic foresight, adaptability, and innovation. Both in military domain and cyber realm, Latvia has adopted a comprehensive state defence system where every citizen has a role in contributing to the state's resilience.

Latvia's geopolitical location on the eastern border of the European Union positions it as a frontline state in the face of cyber threats emanating from neighbouring regions. The country's proximity to adversarial actors, including state-sponsored cyber threats, has compelled it to adopt proactive measures. From implementing robust national cybersecurity strategies to collaborating closely with international allies, Latvia serves as a microcosm of how smaller nations can punch above their weight in the global cybersecurity arena.

Latvia's membership in the European Union and NATO has catalysed its cybersecurity development. By aligning with the European legislation, notably the NIS and NIS2 directives, and actively engaging in collaborative structures such as the EU Agency for Cybersecurity (ENISA) and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Latvia has positioned itself as a vital contributor to regional and global cybersecurity efforts. This dual commitment to national and collective security highlights the interconnected nature of modern cybersecurity challenges and solutions.

To be fair, Latvia faces a significant number of challenges, and even the most well-conceived strategies can stall when confronted with resource limitations or

resistance to necessary shifts in mindset. Cultural change takes time—something a nation under constant hybrid attacks does not have the luxury of wasting. In Latvia's case, policymakers must balance long-term strategic goals with pressing short-term necessities, often doing so with a remarkable degree of success despite the constraints.

One of the central arguments of this book is that Latvia's approach to cybersecurity offers valuable lessons for other nations, particularly smaller states. While larger countries often dominate cybersecurity discourse, smaller nations like Latvia demonstrate the importance of tailored solutions, regional cooperation, and strategic prioritisation. The whole-of-society and whole-of-government approach is not only a wishful thinking, but also a must for a country with very limited resources, nothing short of "work smart, not hard" mantra.

Latvia's emphasis on resilience—the capacity to prepare for, respond to, and recover from cyber incidents—is a cornerstone of its cybersecurity strategy and a critical takeaway for other nations seeking to bolster their defences. Latvia's experience also underscores the importance of public-private partnerships, community engagement, and education in building societal cyber resilience. By fostering a culture of cybersecurity awareness and collaboration, Latvia has strengthened its ability to address not only technical vulnerabilities but also the human and organisational factors that contribute to cyber risks.

While this book focuses on Latvia, its insights extend far beyond the nation's borders. As cyber threats become increasingly transnational, the experiences of individual nations contribute to the collective knowledge needed to address global challenges. Latvia's active participation in international forums, its contributions to EU and NATO cybersecurity initiatives, and its collaborations with neighbouring Baltic states position it as a key player in the global cybersecurity landscape. Furthermore, the interconnected nature of cyberspace means that the security of smaller nations like Latvia has implications for the broader international community. Successful strategies and innovations developed in Latvia can serve as models for other nations, fostering a more secure and resilient digital ecosystem worldwide.

This book aims not only to inform but also to inspire. It is a call to action for policymakers, practitioners, researchers, and citizens to engage in the ongoing effort to strengthen cybersecurity. The challenges are significant, but so too are the opportunities for collaboration, innovation, and progress. By examining Latvia's journey, we hope to provide a blueprint for resilience that resonates across borders and disciplines. In the pages that follow, you will find an in-depth exploration of Latvia's cybersecurity ecosystem, its processes, and its vision for the future. Through case studies, analyses, and expert insights, this book seeks to illuminate the complexities of cybersecurity in a small nation and the broader lessons it offers for our increasingly interconnected world.

The Structure of This Book

This book delves into the foundational elements of Latvia's cybersecurity framework, exploring the ecosystem of stakeholders, including government agencies,

private sector entities, academic institutions, and non-governmental organisations, that collectively shape the nation's cyber resilience. Moreover, it examines the policies, strategies, and governance mechanisms underpinning Latvia's cybersecurity initiatives. Finally, it explores emerging challenges and opportunities in Latvia's cybersecurity landscape, such as artificial intelligence, cyber-physical systems, workforce development, and societal resilience. Together, these themes provide an integrated view of Latvia's past, present, and future cybersecurity efforts.

Cybersecurity is a multifaceted domain involving a wide range of stakeholders, from individual users and private sector entities to governmental institutions and malicious actors. In **Chapter 2**, Jānis Grabis and Linda Vitkaua provide an overview of Latvia's cybersecurity landscape, employing the ecosystem perspective. They explore the intricate web of participants and their interrelations, meticulously mapping the roles and dynamics within this complex network. To enhance the understanding of potential threats and the resources available for mitigation. The authors employ enterprise modelling as their research methodology, which enables them to systematically delineate the participants, their roles, and underlying intentions within Latvia's cybersecurity ecosystem. This analytical approach not only clarifies the structure of the ecosystem but also provides insights into its resilience.

By scrutinising the ecosystem model, the authors evaluate the roles played by key stakeholders, including governmental bodies, educational institutions, and businesses, in bolstering Latvia's cybersecurity resilience. Their analysis extends to examining how the Latvian ecosystem integrates with broader European and global cybersecurity efforts, thereby situating Latvia within the wider international context. Operationalising these models involves a comprehensive analysis of cybersecurity-related activities within Latvia, revealing both the strengths and limitations of the national framework. Ultimately, this chapter serves as a foundational resource for understanding Latvia's cybersecurity ecosystem, offering valuable insights for stakeholders seeking to enhance cybersecurity measures not only within the region but also in comparable settings globally.

Cybersecurity governance is a cornerstone of national resilience. Yet, as Savaş and Karataş (2022) aptly observe, the field remains underexplored, with no consensus on what constitutes a comprehensive cybersecurity governance framework. This gap underscores the importance of analysing institutional structures, processes, and policies across diverse contexts. **Chapter 3**, authored by Mihails Potapovs, Iveta Reinholde, and Kristiāns Teters, addresses this need by examining the evolution of Latvia's cybersecurity governance landscape through a public policy lens.

The chapter maps the institutional and legal evolution of Latvia's cybersecurity governance, identifying critical path dependency factors that have shaped the current framework. It explores how historical decisions continue to influence contemporary policy implementation and governance efficiency. Special attention is paid to Latvia's alignment with the European cybersecurity legislation and the national cybersecurity governance modernisation, culminating in the establishment of the National Cybersecurity Centre, which serve as pivotal moments in the nation's policy trajectory.

Moreover, the chapter delves into the processes within Latvia's cybersecurity ecosystem, exposing the interplay between digital and security policies in pursuit of a more cohesive governance model. Policy coordination emerges as a central theme, highlighting both challenges and opportunities for fostering synergy among stakeholders. The authors contribute to ongoing discussions on cybersecurity policy design by offering forward-looking recommendations. These proposals aim to overcome entrenched path dependencies and chart a course towards a sustainable and adaptive governance framework that aligns with both national needs and international obligations.

In **Chapter 4**, Mihails Potapovs, Kristiāns Teters, Jānis Frīdmanis, and Bernhards Blumbergs provide an in-depth look at the operations of CERT.LV, Latvia's national Computer Security Incident Response Team (CSIRT). The chapter utilises the Security Incident Management Maturity Model (SIM3 v2 interim) framework to evaluate CERT.LV's maturity across four key quadrants: organisation, human resources, tools, and processes. By comparing findings with a 2015 evaluation conducted in cooperation with ENISA, the study identifies key advancements, persistent challenges, and areas for future improvement. The research employs a practitioner-centric approach, drawing on documentary analysis of policy documents, technical reports, operational records, and professional insights.

The case study highlights the significant progress made by CERT.LV in formalising its governance structures, expanding its workforce, enhancing technological capabilities, and streamlining incident response procedures. Moreover, it showcases CERT.LV's efforts in strengthening its integration within the national cybersecurity framework and improving cooperation with international cybersecurity networks. The findings provide valuable insights into the evolution of national CSIRTs, offering policy recommendations for strengthening cyber resilience in an increasingly volatile digital environment.

Cyber resilience, a key theme of this book, encompasses multiple dimensions, some of which receive more scholarly attention than others. While there is substantial research on organisational cyber resilience and the robustness of ICT infrastructures, societal cyber resilience often remains underexplored. **Chapter 5**, authored by Sigita Struberga and Žaneta Ozoliņa, bridges this gap by focusing on the societal dimensions of cybersecurity in Latvia. This chapter examines how societal efforts contribute to resilience against cyber threats, emphasising the collective capacity of communities to prepare for, withstand, and recover from cyber incidents.

The authors analyse the critical roles of public-private partnerships, community engagement, and educational initiatives, presenting these as foundational pillars for societal cyber resilience. They approach the topic through three primary perspectives: national/governmental efforts, community-level activities (including local governments, civil society, and enterprises), and individual preparedness and awareness. Their research methodology includes extensive surveys, in-depth interviews, and co-creation workshops involving experts from Latvia's national cybersecurity competence community.

This collaborative approach allows the authors to gather diverse insights from stakeholders across multiple sectors, enriching their analysis of the societal

resilience landscape. The findings are not merely descriptive but instrumentalised into concrete policy recommendations, forming a basis for Latvia's national societal cyber resilience roadmap. By addressing gaps and proposing actionable strategies, this chapter contributes significantly to the broader discourse on societal cybersecurity, offering valuable insights for both policymakers and practitioners.

In **Chapter 6**, Uldis Ķinis undertakes a comprehensive analysis of Latvia's legal frameworks and procedural mechanisms for addressing cybercrime. He explores the intricacies of the country's national criminal law and procedural regulations, with a focus on their practical application in combating cyber offences. The chapter delves into the unique features of Latvia's legal system, identifying strengths and pinpointing areas where gaps or inconsistencies hinder effective enforcement. By examining regulations on offences such as information system breaches and computer fraud, the author highlights the robustness of existing measures while offering critical insights into potential areas for improvement.

This chapter further scrutinises the challenges associated with cybercrime jurisdiction, particularly in the acquisition, processing, and application of electronic evidence—a cornerstone of modern legal practice. Ķinis provides an in-depth look at the obstacles within Latvia's criminal justice system related to the detection, investigation, and adjudication of cybercrimes. In addition to diagnosing these challenges, the author proposes targeted enhancements to procedural and legal frameworks, aiming to strengthen the country's capacity to prosecute cybercriminals effectively.

Grounded in Latvian legal principles and supplemented by insights from both domestic and international legal scholarship, as well as real-world Latvian case studies, this chapter contributes a vital perspective to the broader discourse on cybercrime. Its findings offer not only a critical evaluation of Latvia's approach to combating cybercrime but also practical policy recommendations that can serve as a blueprint for improving the effectiveness of national and regional efforts in addressing cyber threats.

Building on the groundwork laid in the previous chapters, **Chapter 7**, by Mihails Potapovs and Stella Blumfelde, delves into how Latvia implements European Union cybersecurity frameworks, highlighting the interplay between European integration and national sovereignty. While the EU has traditionally had limited involvement in security and defence policies, it has emerged as a pivotal player in shaping comprehensive strategies across its member states, particularly in domains where the benefits of collaboration and common regulation supersede national sovereignty considerations. Latvia, with its unique geopolitical context as a small EU member state, offers a compelling case study of this dynamic.

Through an in-depth analysis of legislative and policy planning documents, this chapter reveals the EU's role as a catalyst for advancing Latvia's cybersecurity regulatory frameworks, capacity-building initiatives, and information-sharing mechanisms. The authors examine how Latvia navigates the challenges of aligning national security imperatives with supranational directives, emphasising the delicate balance between maintaining digital sovereignty and contributing to collective European cybersecurity efforts. By addressing both current practices and future

directions, the chapter underscores the complexities and opportunities inherent in Latvia's evolving relationship with the EU.

Furthermore, the research contributes valuable theoretical insights into the concept of digital sovereignty, demonstrating how Latvia exemplifies the equilibrium between national autonomy and collaborative governance within the broader European cybersecurity framework. This analysis not only highlights Latvia's proactive role in shaping regional cybersecurity but also provides a blueprint for other nations seeking to balance similar tensions.

Cyber diplomacy plays an increasingly vital role in shaping international relations, particularly in navigating the complexities of cyberspace and addressing the myriad challenges it presents. In **Chapter 8**, Didzis Kļaviņš offers a nuanced analysis of the intersection between cybersecurity and foreign policy. This chapter explores Latvia's active role in shaping international cyber diplomacy by participating in regional and global forums, including the United Nations Open-Ended Working Group (OEWG). Kļaviņš delves into the complexities of cyber diplomacy, examining its distinctive processes, stakeholders, and its pivotal role within Latvian foreign policy.

The chapter sheds light on the evolving nature of cyberspace and Latvia's strategic approaches to addressing cyber challenges on a global stage, notably tackling such key issues as attribution, the implementation of sanctions, and the use of frameworks like the EU's Cyber Diplomacy Toolbox. Through retrospective analysis, the chapter situates Latvian cyber diplomacy within the broader context of the Baltic Sea region, the European Union, and international cyber governance efforts. By illuminating the multifaceted challenges and accomplishments of Latvian cyber diplomacy, Kļaviņš provides critical insights into how smaller nations can amplify their influence and contribute to shaping the global cybersecurity agenda. This chapter not only highlights Latvia's proactive stance but also underscores the significance of cyber diplomacy as a tool for navigating the complexities of modern international relations.

Chapter 9, authored by Heinrihs K. Skrodelis, Mārtiņš Štāls, and Andrejs Romānovs, examines Latvia's efforts to modernise its cybersecurity landscape in response to the evolving global threat environment. The chapter delves into the challenges posed by technological advancements and competitive pressures, which continuously test the readiness and resources of cybersecurity providers. Against this backdrop, Latvia has implemented the provisions of the NIS2 directive and adopted a comprehensive cybersecurity strategy, aiming to create a unified approach to safeguarding digital infrastructure.

This chapter employs an organisational perspective, focusing on both public and private sector initiatives. It includes a comparative case study analysis of how different organisations are transforming their ICT infrastructure, cybersecurity policies, and processes. The research methodology integrates legal and policy document analyses, case studies, and expert interviews to offer a nuanced understanding of the ongoing cybersecurity transformation in Latvia. A key focus of the chapter is the critical decisions organisations face, such as whether to invest in proprietary cybersecurity solutions or outsource them, leading to a reevaluation of traditional perimeter defence architectures. Furthermore, the integration of

artificial intelligence adds complexity by reducing dependence on human labour while introducing new challenges in investigating and mitigating potential errors.

The authors' analysis highlights both the opportunities and risks inherent in adopting such advanced technologies. Through its detailed examination of legal frameworks, technological integration, and organisational strategies, this chapter provides valuable insights into Latvia's efforts to build resilience and adapt to the rapidly evolving cybersecurity landscape. It serves as a vital resource for policymakers, practitioners, and researchers seeking to understand the intricacies of cybersecurity transformation and resilience in a small but dynamic nation.

In an era marked by rapid technological advancements and a constantly evolving cyber threat landscape, the imperative to develop the cyber workforce of tomorrow has become paramount. In **Chapter 10**, Rūta Pirta and Matīss Veigurs delve into the critical imperative of workforce development and education in the rapidly evolving field of cybersecurity. The chapter highlights the pressing need to cultivate the skills and competencies essential for confronting future challenges, as technological advancements and sophisticated cyber threats continue to escalate.

Recognising that effective cybersecurity demands a multidisciplinary approach, the authors emphasise the integration of diverse fields, including legal frameworks, computer science, communication strategies, and psychological insights. They underline the importance of cybersecurity specialists possessing not only technical expertise but also general skills and behavioural traits that are crucial during crisis situations. The chapter also examines the profound impact of emerging technologies, particularly artificial intelligence, which simultaneously heighten cybersecurity challenges and redefine the competence requirements for professionals in this domain.

Acknowledging that cybersecurity knowledge must extend beyond professionals, Pirta and Veigurs advocate for widespread basic cyber hygiene education to enhance personal safety in the digital space. The chapter offers an in-depth examination of Latvia's cybersecurity education ecosystem, identifying gaps, forecasting future competency needs, and proposing strategic recommendations. These include addressing workforce requirements, aligning with technological trends, fostering collaboration, and promoting secure behavioural practices. Serving as a comprehensive guide, this chapter provides critical insights and actionable recommendations for policymakers, educators, and industry stakeholders, aiming to advance human performance and resilience in Latvia's cybersecurity domain.

In **Chapter 11**, Krišjānis Nesenbergs, Pēteris Paikens, and Eduards Blumbergs critically examine the pressing challenges posed by the growing ubiquity of consumer wireless devices, such as smartphones, wearables, and Internet of Things (IoT) devices. These technologies, seamlessly integrated into daily life, form a cyber-physical reality but also reveal a significant gap in security awareness and a lack of motivation among manufacturers to prioritise robust security measures.

Most of these IoT devices rely on diverse wireless communication protocols, including 4G and 5G networks, WiFi, Bluetooth, Bluetooth Low Energy, and mesh protocols like Zigbee. The proliferation of these wireless-enabled devices, combined with the decreasing cost of technologies such as software-defined radios, underscores the need for a comprehensive understanding of vulnerabilities and

proactive preventive measures. This chapter meticulously analyses present and emerging threats to cyber-physical environments, offering an in-depth assessment of vulnerabilities in both consumer and commercial devices. It further evaluates the societal risks posed by these weaknesses, emphasising the potential repercussions on critical systems and infrastructure.

The authors explore the types of cyber-physical systems prevalent in Latvia, identify current and anticipated threat categories, and assess the future implications of these threats within the national context. Concluding with actionable solutions, they propose proactive mitigation strategies, advocating for a robust classification system to inform responses. The chapter highlights the urgent need for collaborative efforts within the security community and calls for governmental interventions to enhance resilience. Serving as a valuable resource, this chapter provides nuanced perspectives on the evolving landscape of cyber-physical systems while presenting practical insights to strengthen Latvia's cybersecurity ecosystem.

The concluding **Chapter 12**, authored by Kate E. Kanasta, delves into the transformative impact of technological advancements on modern warfare and the consequential changes in organisational structures. Throughout the military history, technology has consistently been a pivotal factor, often determining the dominant power in shifting balance-of-power systems. However, some researchers debate whether cyber capabilities truly influence the balance of power today.

While it is undeniable that cyber capabilities enhance existing military operations, their implications do not fundamentally alter the nature of warfare itself. This perspective suggests that cyber developments represent an evolutionary change rather than a revolutionary shift. The chapter examines the impact of advancements in cyber capabilities on operational tactics, military doctrines, and organisational structures while taking the discussion one step further—how might these changes influence the balance of power in the future?

Together, these chapters provide a detailed and comprehensive exploration of Latvia's cybersecurity landscape. They offer valuable insights into the challenges faced by smaller nations and highlight strategies that have enabled Latvia to become a resilient and proactive player in the global cybersecurity arena. Through this layered approach, this book serves as a resource for policymakers, practitioners, academics, and anyone interested in understanding the complexities of cybersecurity in the context of smaller nations. It underscores the interdependence of global cybersecurity and advocates for collaboration, innovation, and resilience as key strategies in navigating the rapidly evolving digital landscape. Ultimately, this work aspires to contribute to a deeper understanding of the cybersecurity domain, offering actionable insights for enhancing resilience, building partnerships, and fostering a secure and interconnected future for all.

References

- Barrinha, A. (2018). Virtual neighbors: Russia and the EU in Cyberspace. *Insight Turkey*, 20(3), 29–42. <https://www.jstor.org/stable/26469842>
- CERT-EU. (2023). *Russia's War on Ukraine: One Year of Cyber Operations*. Retrieved from <https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf>

- Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation and Technology*, 9(2), 159–189. <https://doi.org/10.1080/17579961.2017.1377914>
- Ilves, T. H. (2016). The consequences of cyber attacks. *Journal of International Affairs*, 70(1), 175–181.
- Kozłowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal*, 3, 236. <https://core.ac.uk/reader/236412320>
- Mansfield-Devine, S. (2012). Estonia: what doesn't kill you makes you stronger. *Network Security*, 2012(7), 12–20. [https://doi.org/https://doi.org/10.1016/S1353-4858\(12\)70065-X](https://doi.org/https://doi.org/10.1016/S1353-4858(12)70065-X)
- Pernik, P., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., Linnell, J., Pawlak, P., Reinhold, T., Reshetnikov, A., Soldatov, A., & Vilmer, J.-B. J. (2018). The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine. In *Hacks, Leaks and Disruptions: Russian Cyber Strategies* (pp. 53–64). European Union Institute for Security Studies (EUISS). <https://www.jstor.org/stable/resrep21140.9>
- Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, 3(1), 7–34. <https://doi.org/10.1365/s43439-021-00045-4>
- Stronski, P., & Himes, A. (2022). *Russia's Game in the Balkans*. Carnegie Endowment for International Peace.
- Willett, M. (2022). The cyber dimension of the Russia–Ukraine war. *Survival*, 64(5), 7–26. <https://doi.org/10.1080/00396338.2022.2126193>

2 The Cybersecurity Ecosystem of Latvia

Mapping and Analysis

Jānis Grabis and Linda Vitkaua

Introduction

Information and communication technologies (ICTs) have become an integral part of human society affecting individuals, businesses, and states. Inevitably that has led to security concerns to prevent adverse impact of various incidents. Cybersecurity is a set of measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer (CNSSI, 2015). It concerns multiple actors starting with computer users, cybersecurity specialists as well as malicious actors. These actors are linked together in an intricate web of relationships forming a connected network. The actors have different impacts on each other, and the overall behaviour emerges as the result of actions performed by individual actors. The strength of the network depends on the right composition and positive dynamics of the systems. This kind of behaviour is characteristic to ecosystems, and this concept has recently been adopted for studying various socio-technical systems rather than just biological systems (Tsai et al., 2022).

A digital ecosystem is a distributed, adaptive, open socio-technical system with properties of self-organisation, scalability, and sustainability inspired from natural ecosystems (Briscoe & De Wilde, 2006). It is a complex network of people, businesses, and systems that use technology to interact with one another. In the case of the cybersecurity ecosystem, the backbone of the ecosystem is devices interconnected by computer networks. These devices are used by various actors ranging from computer users to cybersecurity specialists. The system is an open system due to its reliance on public networks and it is a socio-technical system because human factors often have more significant impact on its behaviour than the technical ones. There is some degree of oversight provided by governmental and public organisations though generally it is a self-organising system.

Understanding the ecosystem composition and motivation of entities involved is crucial for further analysis of the cybersecurity ecosystem and comprehension of its strengths and weaknesses. Therefore, this chapter focuses on identification of actors in the cybersecurity ecosystem as well as their goals.

The objective of this chapter is to map and to analyse the Latvian cybersecurity ecosystem. Enterprise modelling (Sandkuhl & Stirna, 2014) is used as a research method to identify ecosystem participants and their intentions. Resilience is one

of the desired characteristics of the ecosystem (Ferdinand & Benham, 2017). It characterises the ecosystem's ability to persist in changing and often adverse circumstances. The ecosystem models developed are used to assess the resilience of the Latvian cybersecurity ecosystem. The assessment is based on structural properties of the ecosystem identified in Tsai and Zdravkovic (2020) and Tsai et al. (2020).

The rest of this chapter is organised as follows. The Background section provides the background information in cybersecurity ecosystems and ecosystems modelling. That includes a brief review of existing work on cybersecurity ecosystem analysis. The Latvian cybersecurity ecosystem is presented in The Overall Ecosystem section. The ecosystem analysis is discussed in the Ecosystem Analysis section. Conclusions are provided in the closing section.

Background

The cybersecurity ecosystem has been investigated from various perspectives such as regulatory, business, and societal. This section reviews the existing work on mapping and analysing the cybersecurity ecosystem. By building on these investigations, this chapter attempts to uncover a holistic Latvian cybersecurity ecosystem. For these purposes, an enterprise modelling approach describing goals and actors involved in the cybersecurity ecosystem is employed.

Related Work

Current research and practice recognise the importance of the ecosystem perspective in addressing cybersecurity concerns. The DHS (2011) emphasises the analogy with natural ecosystems and presence of diversity of participants – private firms, non-profits, governments, individuals, processes, and cyber devices (i.e., computers, software, and communication technologies). More importantly, the participants interact with each other and might have their specific reasons for involvement. The diversity of participants is also highlighted and further extended in the definition of the information security ecosystem by D'Arcy and Hovav (2008). The list of participants includes hardware and software vendors, consultants, digital forensics experts, standardisation agencies, accreditation and education facilities, academic conferences and journals, books, magazines, hackers, and their paraphernalia. These participants drive development of cybersecurity products and services. Definition of key building blocks is another approach to defining cybersecurity ecosystem (DHS, 2011). The key building blocks are automation, interoperability and authentication. Automation concerns computer-aided decision-making and actuation in response to cybersecurity incidents. Interoperability allows “cyber participants to collaborate seamlessly and dynamically in automated community defense”. Authentication ensures trusted interactions in the cyber space.

Abazi (2022) argues that collaboration among government, private secretary, and academia is essential to increase cybersecurity performance. Duties of various stakeholders are also highlighted, for example, Information Society Agency is responsible for improving the overall cybersecurity maturity while Information and Privacy Agency addresses specific issues such as compliance with GDPR regulations.

A representation or view of the overall cybersecurity ecosystem depends on the perspective. This perspective can be defined from the viewpoint of societal importance starting with basic cyber hygiene and protection to critical assets to ensuring democracy and protecting human rights (ENISA, 2017). Governmental institutions and regulations play a major role to achieve the top-level objectives. Bederna and Rajnai (2022) analyse the cybersecurity ecosystem in the European Union (EU). They point out that ENISA and CERT are the core transnational players, who collaborate with national bodies. Critical infrastructure and identity services providers are main players at the member state level. Still, the European digital cybersecurity ecosystem is a part of the global cybersecurity ecosystem, and the relevant players and interactions should be accounted for. This way the Latvian cybersecurity ecosystem is also a part of the European cybersecurity ecosystem as well as the global cybersecurity ecosystem.

There have been some attempts to map the Latvian cybersecurity ecosystem. The European Telecommunications Standards Institute (ETSI) lists organisations involved in the Latvian cybersecurity ecosystem. The list has a strong emphasis on governmental and defence institutions. The Latvian case is analysed in the context of the global cybersecurity ecosystem. The global ecosystem is characterised by collaboration mechanisms used among the parties. Six groups of the collaboration mechanisms referred as to forums and activities are considered: (1) forums that develop techniques, technical standards, and operational practices; (2) major IT developer forums affecting cybersecurity; (3) activities for continuous information exchange; (4) centres of excellence; (5) reference libraries, continuing conferences; and (6) heritage sites and historical collections (ETSI, 2017).

An informal representation of the Latvian cybersecurity ecosystem is presented by Benetis (2023). It serves as a directory of specific organisations dealing with specific aspects of cybersecurity in Latvia. A distinguishing feature of this representation is the naming of many companies providing cybersecurity services and products. The key players of the Latvian cybersecurity ecosystem are also identified by CERT.LV. This representation focuses on the role of CERT.LV itself and its connections with other organisations.

Ecosystem Modelling

The ecosystem is modelled using the approach proposed in Grabis et al. (2022). This modelling approach focuses on the identification of ecosystem roles and ecosystem goals. The ecosystem participants are abstracted using ecosystem roles. The role is a part a participant plays in the ecosystem and the contribution they make through the application of their skills, knowledge, experience, and abilities. A generic role refers to a specific type of participant in the cybersecurity ecosystem. Such a generic role is fulfilled by a particular organisational unit, which stands for an identifiable organisation or business. The generic role abstraction allows to describe the structure of the organisational network underlying the cybersecurity ecosystem without being obstructed by ever-changing instantaneous network composition.

Goals are used to define intentions of participants of the cybersecurity ecosystem. It is assumed that participants (either generic or specific) have their

business goals. At the same time, there are ecosystem goals describing the purpose of the ecosystem as a whole. The business goals either contribute or hamper achieving the ecosystem goal. Representation of the goals allows understanding motivation of various participants and to analyse health of the ecosystem.

This chapter focuses on the overall cybersecurity ecosystem goals and identifies some of the specific business goals of selected participants.

The identified goals and roles can be used to assess resilience of the cybersecurity ecosystem. To achieve that, they are mapped to the typical resilience goals and roles identified in the literature. It is assumed that the pre-condition of the resilience is a support for the archetypal goals and roles of ecosystem resilience. These goals and roles have been identified and analysed in Tsai & Zdravkovic (2020) and Tsai et al. (2020), respectively. The resilience roles in the digital ecosystem are: (1) *driver* – sets the vision for the ecosystem and facilitates its growth; (2) *aggregator* – aggregates capabilities and resources; (3) *modular producer* – provides resources; (4) *complementor* – provides resources that complement the core resources; (5) *customer* – pays for ecosystem's services; (6) *end-user* – uses ecosystem's services; (7) *governor* – governs all actors within an ecosystem by providing the standards, laws, etc.; and (8) *reputation guardian* – ensures trustworthiness.

The resilience goals in the digital ecosystem are diversity, efficiency, adaptability, and cohesion. Diversity is the variety of actors for organisational units and roles, the collection of multiple resources and resource variety, and the collection of multiple capabilities and capabilities variety in a digital ecosystem. Efficiency is the resource productivity and utilisation in an ecosystem and value delivered relative to total resource consumption. Adaptability is transparency in terms of exposing the means of adaptation and flexibility as the ease with which a digital ecosystem can be changed. Cohesion denotes the strength of partnerships, the alignment and tightness among actors, and their capabilities towards fulfilling the mission of a digital ecosystem.

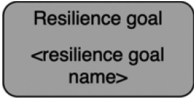
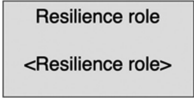
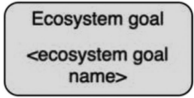
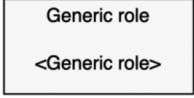
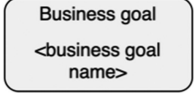
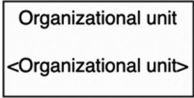
The goals and roles are categorised as resilience, ecosystem and business goal and ecosystem and generic roles and organisational units, respectively (Table 2.1). The relationship between goals is defined as the ecosystem goals supporting the resilience goals and the business goals supporting the ecosystem goals. Similarly, the relationship between roles implies that the generic roles fulfil the ecosystem roles, and the organisation units fulfil the generic roles. The relationship between goals and roles defines that certain roles are required to fulfil the goal.

Cybersecurity Goals and Roles

The overall information security goals have been defined as the CIA triad and include confidentiality, integrity, and availability (Dhillon & Backhouse, 2001). Confidentiality protects information (data) from unauthorised access. Integrity is the accuracy and consistency of data as well as the completeness and reliability of systems. Availability is the ability for users to access systems and information when needed, even under duress.

The list of goals has been expanded to account for new risks emerging in collaborative environments (Cherdantseva & Hilton, 2013), and the extended list

Table 2.1 Notation used to model Latvian cybersecurity ecosystem

| <i>What needs to be represented</i> | <i>Concept</i> | <i>Graphical symbol</i> |
|---|--|---|
| Intention concerning ecosystem resilience | Ecosystem resilience goals |  |
| Role necessary for ecosystem resilience | Ecosystem resilience role |  |
| Intention of the ecosystem | Ecosystem goal (commonly agreed goal among ecosystem participants) |  |
| Generic role significant to the ecosystem | Generic role (specific to business domain or case) |  |
| Intention of the ecosystem participant | Business goal |  |
| Organisational unit fulfilling a generic role | Specific organisational unit |  |

includes: confidentiality, integrity, availability, privacy, authenticity and trustworthiness, and non-repudiation. The empirical analysis shows that the most important goals of organisations are information integrity, confidentiality, accountability, and availability (Qingxiong et al., 2008). This list has been further expanded to include confidentiality, availability, integrity, accountability, assurance, anonymity, authentication, authorisation, correctness, identification, non-repudiation, policy compliance, privacy, secrecy, and trust, and it can be mapped to the NIST SP 800-27 standard (Adach et al., 2022a).

CISA has formulated Cross-Sector Cybersecurity Performance Goals (CPGs) addressing some of the most common and impactful cyber risks (CISA, 2023). The CPG model aims to implement an easy-to-implement set of IT and operational technology (OT) cybersecurity measures. It prescribes the following goal definition components:

- Outcome,
- TTP/risk addresses,
- Security practices,
- Scope,
- Recommended action, and
- NIST CSF reference.

The goals are allocated to one of seven groups including: account security, device security, data security, governance and training, vulnerability management, supply chain/third party, and response and recovery. Sample goals are prohibit connection of unauthorised devices, OT cybersecurity training, and vendor/supplier cybersecurity requirements. From the ecosystem perspective, ecosystem members should strive to adhere to these foundational goals to limit their risk exposure as well as harmful effects on other members of the ecosystem. Many of the technical concerns can be addressed in a collaborative manner (Meng et al., 2015). The overarching goal of collaborative security is to make more effective and robust decisions. However, some of the challenges to be resolved in collaborative security systems include accuracy, privacy, incentives, robustness, and scalability.

Besides technical aspects, human goals also play a vital role in the cybersecurity ecosystem and security is one of the primary human goals (Chulef et al., 2021). National and personal security are essential to achieve these goals (Madrueño-Aguilar, 2016).

The aforementioned goals are pursued by ecosystem participants having various roles. The cybersecurity ecosystem is inherently global (Bederna & Rajnai, 2022) and an organisation operates in collaboration with state-wise players, which in turn collaborate with regional (e.g., EU) players and global players. The organisation uses various IT and business services, which are subject to cybersecurity regulations provided by European bodies such as ENISA and CERT-EU. It is also affected by other regulations when interacting with other countries outside EU and global technological developments. ENISA or European Union Agency for Cybersecurity is the Union's agency aiming to achieve a high common level of cybersecurity across Europe. It follows the EU Cybersecurity Act and Directives on Security of Network and Information System. It focuses on collaboration among the member states, knowledge sharing, cybersecurity capacity building, and awareness raising. CERT or Computer Emergency Response Team is an expert group that handles computer security incidents. It maintains information about cybersecurity incidents, helps government and society institutions to cope with incidents, and raises awareness about cybersecurity threats and protective measures. The ETSI is an independent, not-for-profit, standardisation organisation operating in the field of information and communications. ETSI supports the development and testing of global technical standards for ICT-enabled systems, applications, and services.

The players involved in cybersecurity ecosystem can be classified as macro-level and micro-level players (Kuzminykh et al., 2021). The macro-level players are governments, regulators, policymakers, and standards-setting organisations. Key micro stakeholders include end-users, consumers, governments, private companies, corporations, Small and Medium Enterprises (SMEs), financial institutions, and security consultants who micro-connect other players. DHS states that cybersecurity ecosystem includes diverse participants – private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communications technologies).

This discussion paper explores (DHS, 2011) resilience of cybersecurity ecosystems what should lead to fundamentally more secure systems. Participants of resilient cyber ecosystem are expected to work together in near-real time to anticipate

and prevent cyberattacks, limit the spread of attacks across participating devices, minimise the consequences of attacks, and recover to a trusted state.

Das (2015) places an organisation at the centre of the cybersecurity ecosystem and defines its relationships with other involved actors. Software vendors are referred as to keystone players, while network, hardware, and cloud providers are referred as to niche players. The ecosystem also emphasises the role of governmental institutions and cyber insurers. The ecosystem includes adversaries such as individuals and groups of cyber criminals attacking the organisation and its assets. The adversaries use online and P2P networking resources to carry out the attacks.

The Overall Ecosystem

The Latvian cybersecurity ecosystem model is developed by merging relevant entities defined in the European cybersecurity ecosystem and the global cybersecurity ecosystem and entities derived from Latvian legislation as well as specific national entities. These goals and roles are mapped to the resilience goals and roles, respectively, to analyse the resilience of the Latvian cybersecurity ecosystem.

Goals

The goal model shows the ecosystem goals to ensure cybersecurity in Latvia (Figure 2.1). The identified goals are:

- To ensure national security – serves as a foundation to achieving other cybersecurity objectives. It concerns measures, policies, and practices implemented by a nation to protect its information systems, critical infrastructure, and digital assets from internal and external cyber threats and attacks,
- To provide secure critical infrastructure – digital services rely on critical communication and data infrastructure and it should safeguarded against cyberattacks,
- To guarantee personal security – citizens should be safe while using digital services for communication and data processing as well as personal data protection should be enforced,
- To ensure information security – all members of ecosystem should be able to process, store, and transmit data safely without compromising confidentiality, integrity, and availability,

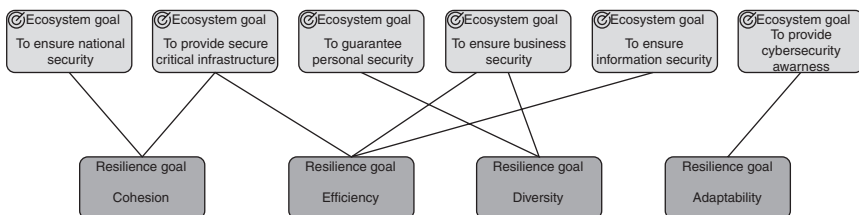


Figure 2.1 The cybersecurity ecosystem goals.

- To ensure business security – digital business transaction should be performed in a secure and reliable environment, and
- To provide cybersecurity awareness – all ecosystem participants should be aware of cybersecurity risks and opportunities. That includes cybersecurity education.

These goals directly follow from Latvian legislation, primarily, National Cybersecurity Law (2024) and the National Cybersecurity Strategy of Latvia (2023–2026) (Ministry of Defence, 2023).

The high-level cybersecurity ecosystem goals in Latvia are similar to those of other countries as Latvia is a part of the European and Global ecosystem.

The ecosystem goals are mapped to the resilience goals. The critical infrastructure provides means for all ecosystem entities to access required services and ensure efficient functioning of the whole system. The efficiency is also the primary concern for business and information security. However, the personal security is essential to ensure wider involvement in the ecosystem and it supports the diversity goal. The national security jointly with critical infrastructure ensures cohesion in the cybersecurity ecosystem. The cybersecurity awareness and education enable ecosystem participants to adapt to specific situations.

The mapping shows that the cybersecurity ecosystem fulfils necessary conditions for ensuring ecosystem resilience because the established ecosystem goals support the known resilience goals.

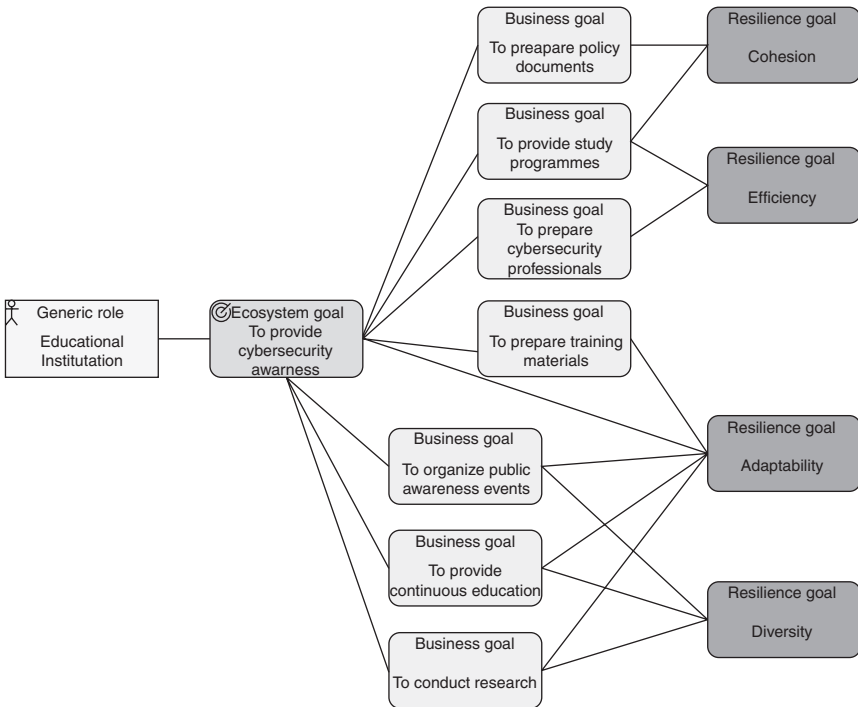


Figure 2.2 Business goals of education institutions.

However, analysis of business or specific goals of different actors or individual ecosystem participants reveals additional information about the ecosystem. The business goals are defined for an actor *Education institution* (see Section 3.2) (Figure 2.2), which is primarily responsible for providing the cybersecurity awareness ecosystem goal:

- To provide study programmes – the goal concerns design, development, and delivery of educational courses and curricula to provide knowledge, skills, and competencies to learners,
- To prepare training materials – training materials accommodate the delivery of educational courses to provide learners with in-depth insights into cybersecurity,
- To provide continuous education – knowledge and skills should be continuously renewed in the face of evolving cybersecurity threats,
- To prepare cybersecurity professionals – educational courses and study programmes are delivered to prepare cybersecurity professionals,
- To conduct research – new methods and technologies are elaborated to deal with cybersecurity threats more efficiently,
- To prepare policy documents – contributions to policy documents are made,
- To prepare information materials – information materials targeting general public are prepared and distributed to increase awareness about cybersecurity challenges, and
- To organise public awareness events – events are organised to improve knowledge about cybersecurity issues and to build trust in the cybersecurity ecosystem.

The business goals are mapped to the resilience goals what highlights that cybersecurity awareness contributes to achieving all four resilience goals. In particular, the adaptability goal is emphasised by providing research, training materials, events, and continuous education. That allows participants of the cybersecurity

Table 2.2 Analysis of cybersecurity ecosystem roles defined in literature

| <i>Source</i> | <i>Roles</i> |
|----------------------------|--|
| National Cybersecurity Law | Critical Infrastructure Providers Governmental institutions Organisations and businesses Citizens |
| CERT.LV | CERT network and international organisations Media Citizens Governmental institutions Municipalities and businesses ICT service providers |
| Benetis (2023) | Technology Developers, Resellers, Integrators, Consultancy Distributors Educators, Research, Communities National Capabilities |

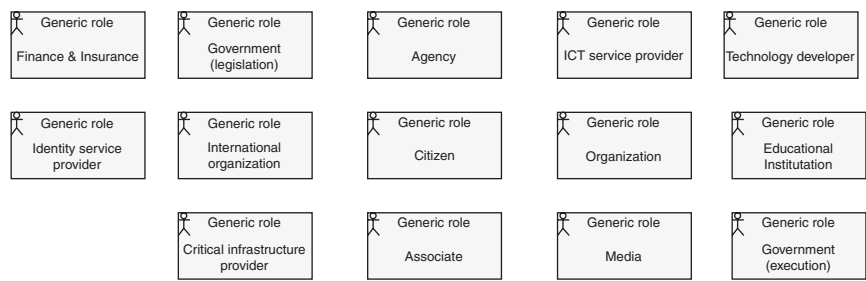


Figure 2.3 The cybersecurity ecosystem roles.

ecosystem to use cybersecurity knowledge to develop new services and prepare for various cybersecurity threats. The study programmes are often developed according to cybersecurity standards and best practices thus facilitating dissemination of common truth across the ecosystem. The efficiency resilience goal was primarily addressed from the business perspective, and the cybersecurity awareness contributes to providing a pool of cybersecurity professionals.

At the same time, there could be individuals or organisations having malicious business goals, e.g., cyber extortion. The ecosystem model presented in this chapter focuses on non-malicious intents.

Roles

The legislation and literature analysis reveals a number of typical roles involved in the cybersecurity ecosystem. Table 2.2 lists roles mentioned in various descriptions and models of the cybersecurity ecosystem. National Cybersecurity Law identifies key roles at the state level as well as organisations fulfilling these roles. The key institution here is National Cybersecurity Centre, which acts as a cybersecurity coordination centre. CERT.LV focuses on mutual interactions among different roles and joining various stakeholders (CERT.LV, 2025) while Benetis (2023) focuses on the business aspects of cybersecurity ecosystem.

The following roles have been identified in the cybersecurity ecosystem (Figure 2.3):

- *Government (legislation)* – provides legal basis for cybersecurity,
- *Government (executive)* – enforces cybersecurity regulations,
- *Agency* – an independent governmental organisation tasked with addressing specific cybersecurity challenges (e.g., CERT.LV),
- *Citizen* – state citizens,
- *Organisation* – an organisational non-business entity having strong interest and exposure to cybersecurity concerns,
- *International organisation*,
- *Business* – companies working in various industries with strong interest and exposure to cybersecurity concerns,

- *Association* – industrial, professional or other type of association providing a joint forum for addressing cybersecurity challenges,
- *Technology developer* – develops new cybersecurity tools,
- *ICT service provider* – provides ICT and cybersecurity services to citizens, organisations, and businesses,
- *Identity service provider* – maintains and verifies the identity of users of digital services,
- *Finance and insurance* – helps dealing with financial risks associated with cybersecurity,
- *Education institution* – provides knowledge, training, and research in the area of cybersecurity,
- *Critical infrastructure provider* – systems supporting vital ICT services, and
- *Media* – various news and analytical outlets distributing information on cybersecurity matters.

Cybersecurity directly concerns citizens, organisations, and businesses. They can be perceived as both customers of cybersecurity services as well as end-users directly affected by cybersecurity concerns (Figure 2.4). At the same time, typically they do not assume the *Driver* role. Despite the growing importance of cybersecurity, there are few end-users of digital services who perceive cybersecurity as a driving concern. The *Driver* role is assumed by governmental institutions, specialised agencies, associations, and technology developers. *Organisations*, businesses, and citizens assume the roles of both *customer* and *end-user*. The cybersecurity ecosystem is governed by legislative bodies and much of the regulations are derived from international regulations and standards, especially, those set by the EU. *Technology developers* also act as *modular producers* providing various components for building cybersecurity systems. *ICT service providers*, however, are *Aggregators* connecting the components and servicing customers and end-users. The aggregation is performed on the top of the critical infrastructure layer. Trust is a major concern in cybersecurity and

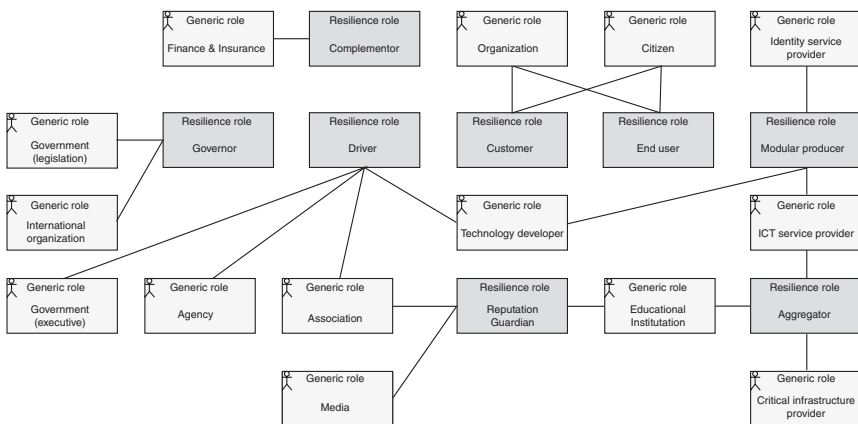


Figure 2.4 Relationships among the cybersecurity roles and the resilience roles.

Table 2.3 The list of main cybersecurity events in Latvia

| <i>Event</i> | <i>Accessed</i> | <i>Link</i> |
|--|-----------------|---|
| CyberChess 2023 conference | 04.07.2024. | https://cyberchess.lv/cc23/ |
| CyberChess 2022 conference | 04.07.2024. | https://cyberchess.lv/cc22/ |
| CyberShield 2023 Cybersecurity Forum | 05.07.2024. | https://www.eventbrite.dk/e/kiberdrosibas-forums-cybershield-2023-tickets-709358358947 |
| Open Data Conference | 05.07.2024. | https://www.lata.org.lv/konference-2023 |
| RIGA COMM 2023 Conference | 15.07.2024. | https://rigacomm.com/lv/programma/ |
| Workshop “Esi drošs” (“Be safe”) | 05.07.2024. | https://cert.lv/lv/2023/11/it-drosibas-seminars-esi-dross-decebri |
| “Digitālā nedēļa” 2023 (Digital Week) | 15.07.2024. | https://eprasmes.lv/iepazisties-ar-eiropas-digitalas-nedelas-2023-latvija-tematiskajam-dienam/ |
| “Kibernakts” 2023 (Cyber Night) | 15.07.2024. | https://www.lvrte.lv/kibernakts-2023/ |
| Cybersecurity Technology Seminar | 15.07.2024. | https://events.datigroup.com/kiberdrosibas-tehnologiju-seminars |
| Annual Data Protection and Cybersecurity Forum | 15.07.2024. | https://digitalaera.lv/ |
| ESET Security Day Latvia | 16.07.2024. | https://www.eset.com/lv/eset-security-day/ |
| Conference on Digital Maturity and Cyber Resilience for the Sustainability of Latvia | 16.07.2024. | https://lvportals.lv/dienaskartiba/349629-latvijas-universitate-notiks-augsta-limena-ekspertu-konference-digitalais-briedums-un-kibernoturiba-latvijas-ilgtspejai-2023 |
| CyberCommando’s Meetup RIGA 2023 | 16.07.2024. | https://cybercommando.eu/ |

Reputation guardians help to increase the trust level in resilient cybersecurity systems. This role is assumed by several players including *associations, media, and education institutions*. *Associations, technology developers, and education institutions* emerge as roles connecting various aspects of the ecosystem resilience.

The generic roles are fulfilled by specific organisations. Virtually all organisations in Latvia are a part of cybersecurity ecosystem because 99% (Oficiālais statistikas portāls, 2023) of businesses and 90% (Oficiālais statistikas portāls, 2023) of citizens, respectively, are using the broadband internet.

The National Cybersecurity Strategy of Latvia and ETSI (2017) provide an exhaustive list of governmental institutions and agencies. Benetis (2023) describes some of the key technology developers and ICT service providers. An additional analysis of the organisations involved in the Latvian cybersecurity ecosystem is provided in Section 4.

Ecosystem Analysis

The aforementioned models describe the Latvian cybersecurity ecosystem and its main participants and their objectives. To understand the impact of the participants

and the most active cybersecurity communities, cybersecurity-related events and their participants are analysed. There are several main cybersecurity events organised in Latvia on annual basis (Table 2.3). For the purpose of this study, the events taking place in 2022 and 2023 are considered. The following information is extracted from publicly published schedules:

- Individuals giving presentations,
- Titles of presentations, and
- Organisational entities involved as event organisers or sponsors.

Events were attended by numerous attendees from various organisational entities though this information is not available in public sources.

The Latvian cybersecurity ecosystem graph (Figure 2.5) includes the following nodes:

- Cybersecurity events,
- Individuals participating in the events, and
- Organisational entities participating in the events.

The following edges or connections in the graph are made among the nodes:

- An edge between a participant and an organisational entity showing that the participant represents the organisational entity,
- An edge between a participant and an event showing that the participant participates at the event, and
- An edge between an organisational entity and an event showing that the organisational entity is involved with the event.

Organisations are assigned specific generic roles. The Latvian cybersecurity ecosystem graph constructed includes 13 events, 157 organisational entities, and 197 individuals. The graph is perceived as an instantiated fragment of the Latvian cybersecurity ecosystem showing the most active members of the ecosystem participating in public events.

The graph is analysed to answer the following questions:

Is the Latvian cybersecurity ecosystem resilient from the organisational perspective, i.e. are all resilience roles represented in the graph?

Which individuals and organisational entities are the most active participants?

Are there any communities within the Latvian cybersecurity ecosystem?

Building on Figure 2.2 about generic roles, organisations fulfilling these roles in the Latvian cybersecurity ecosystem are identified (Table 2.4). It can be observed by ICT service providers and technology companies are very actively involved. However, they are often involved as sponsors and exhibitors in the events and fulfil the modular producer role from the resilience perspective. Governmental institutions and agencies are also active participants ensuring governor and driver functions in the cybersecurity ecosystem. There are very few media and end-user representatives. The media might be present also indirectly by publishing and

Table 2.4 Organisational units fulfilling generic roles in the Latvian cybersecurity ecosystem

| <i>Role</i> | <i>Organisations</i> | <i>Number of organisations</i> |
|--------------------------------------|--|--------------------------------|
| Agency | CERT.LV, Swedish Civil Contingencies Agency, CERT-LT, CERT-EE, Canadian Centre for Cybersecurity, the National Cybersecurity Centre Finland, Estonian Information System Authority, CERT.pl, National Cybersecurity Centre, Republic of Ireland, Luxembourg House of cybersecurity, Computer Emergency Response Team of Ukraine CERT-UA, European Union Agency for cybersecurity, Geospatial Information Agency, State Land Service, Enterprise Register, Centre for Disease Prevention and Control, State Construction Control Office, Central Finance and Contracts Agency, State Real Estate, State Data Inspectorate, Bank of Latvia | 21 |
| Association | Latvian Information and Communications Technology Association, ISACA Latvian Chapter, Latvian Internet Association, LATA, Latvian Digital Accelerator, Women4Cyber Finland, Latvian Medical Association, Latvian Formula 2050, Financial Industry Association, Latvian Blockchain Association, Latvian Security and Defense Federation, Latvian Cyberpsychology Association, Latvian Association of Certified Personal Data Protection Specialists | 13 |
| Business | New Black, Oschadbank Ukraina, KPMG Latvija, meteocontrol, Medicīnas centrs ARS, Longenesis, Evolution, Centrālā Laboratorija, SEB banka, Latvijas Valsts Meži | 10 |
| Critical infrastructure provider | LVRTC, NETNOD | 2 |
| Educational and research institution | New York University Abu Dhabi, Netherlands Defence Academy, Vrije Universiteit Amsterdam, Institute of Electronics and Computer Science, Constellation Research, Institute of Mathematics and Computer Science (LV), Riga Technical University, ICS-FORTH, SANS Institute, CLICO Baltics, Fraunhofer FKIE, CTF Tech, Institute of Electronics and Computer Science (EDI), KnowBe4, Tel Aviv University, BA School of Business and Finance, University of Latvia, Tartu University, RISEBA, Vidzeme University of Applied Sciences | 20 |
| Government (executive) | Ministry of Defence, Swedish National Coordination Centre, Foreign Commonwealth and Development Office (UK), Ministry of National Defence of the Republic of Lithuania, Latvian National Coordination Centre, VARAM, State Police, Embassy of Latvia in the United Kingdom, Chancellery of the State President, State Chancellery, Ministry of Economics, Liepāja municipality, European Commission | 13 |

(Continued)

Table 2.4 (Continued)

| <i>Role</i> | <i>Organisations</i> | <i>Number of organisations</i> |
|----------------------------|---|--------------------------------|
| Government (legislation) | Saeima | 1 |
| ICT service provider | NIC.LV, ARNES, Sentinel One, Tet, UA registry, Hostmaster Ltd, VirustTotal, Estonian Internet Foundation, LMT, Recorded Future, Artic Security, Internet Service Centre at Kaunas University of Technology, NASK, Team Internet Group, DE registry, DENIC, CSC Corporate Domain, SIA Cyber Circle, Synergy Consulting, CentralNic Registry, Team Cymru, Dots, Cybexer Technologies, Possible Security, Zerofox, Fortinet, PaloAlto, ESET Latvija, Cytactic, SIDCON Consulting Company, Excellent Business Solutions Eesti, Cybers, NS Advisory, CITM Advisory, KyberX, Bakotech, PricewaterhouseCoopers, StellarCyber, Teamwire, DATI Group, DeepInstinct, IT-Harvest, Appgate, OptiCom, ITEKSPERTS | 43 |
| Identity service provider | OneSpan, Senhasegura | 2 |
| International organisation | European Cybersecurity Competence Centre, Council of European National Top-Level Domain Registries | 2 |
| Media | Podium North, caurumi.lv | 2 |
| Military | NATO Strategic Communications Centre of Excellence, Canadian Armed Forces, Canadian Joint Forces Cyber Component, NATO SHAPE CyOC, Zemessardzes Kiberaizsardzības vienība, Zemessardze | 6 |
| Organisation | EURid, ICANN, DataProtection.lv, Tiesu administrācija | 4 |
| Technology developer | Microsoft, ZZ Dats, Vmware, IBM, CISCO, Trend Micro, Radware, Bitdefender, Samsung, Asus, Nextcloud, Headtechnology, Pentera, Forescout, Logpoint, SQUALIO, Veriato, Kingston Technology | 18 |
| Finance and insurance | – | 0 |

distributing information about events. Active end-user participation in the events is not expected though they could have been represented by end-user associations or communities. Educational institutions participated in many events including universities and research organisations from other countries what highlights their important role as an aggregator in the ecosystem. Although several financial institutions have participated, none of them is identified as providing finance and insurance services specifically tailored to cybersecurity. There are also relatively few business institutions taking an active part in the events though their representatives could be among attendees.

Figure 2.6 shows individuals presenting more than one in the selected events. 15% of all individuals have given several presentations what indicates that there is

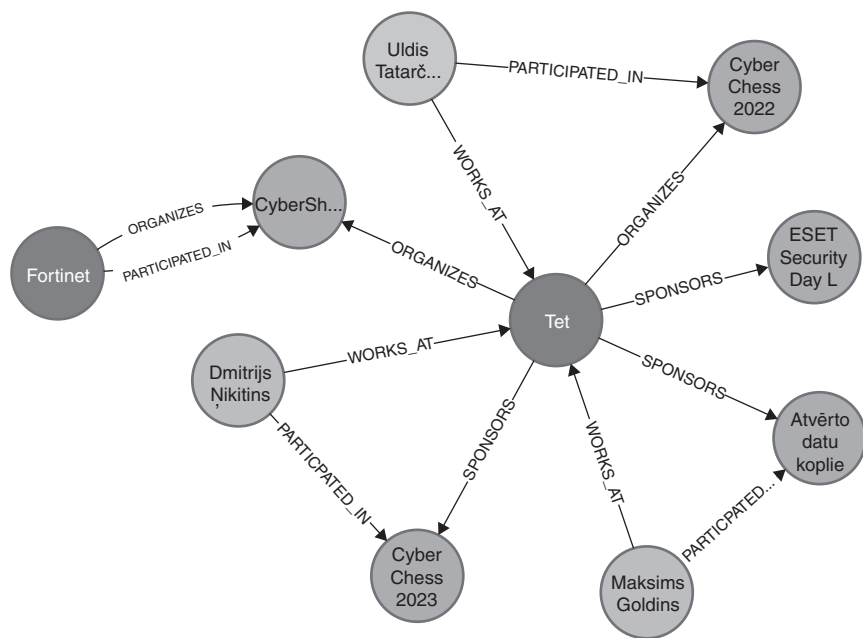


Figure 2.5 A fragment of the Latvian cybersecurity ecosystem graph.

a significant concentration of individuals forming opinions in the Latvian cybersecurity ecosystem. Similarly, a few organisational entities are significant promoters of activities in the Latvian cybersecurity ecosystem (Figure 2.7). CERT.LV, LVTRC (state data transmission and data centre management company), TET (largest internet service provider in Latvia and major ICT company), and Ministry of Defence are the most central organisational entities. The positive aspect is that they represent various roles in the ecosystems, thus supporting various perspectives and aspects of cybersecurity.

Figure 2.8 shows all the organisational entities from the graph. Organisational entities in this figure are connected based on the events in which organisations participated. If two organisations either organised, sponsored, or had people representing them at a specific event, organisations were connected. New edges were created for every distinct event. The community identification algorithm is applied to identify which organisations tend to work together. The organisational entities from the red cluster all participated in “RIGA COMM 2023” conference, but none of these entities participated in any other events. It is important to note that “RIGA COMM 2023” includes a lot of IT and business-related conferences, one of them being a conference about cybersecurity. Only the organisations participating in the cybersecurity section of “RIGA COMM 2023” were included in the graph

The orange community canters around ICT service providers, while the purple community is mainly driven by governmental institutions. Nevertheless, there are strong interaction among various roles (Table 2.5). CERT.LV and the Ministry of

Table 2.5 Top organisational entities by number of joint event participations

| <i>Organisational entity 1</i> | <i>Organisational entity 2</i> | <i>Event count</i> |
|--------------------------------|--------------------------------|--------------------|
| CERT.LV | Ministry of Defence | 7 |
| CERT.LV | LVRTC | 5 |
| CERT.LV | Riga Technical University | 4 |
| CERT.LV | Tet | 4 |
| CERT.LV | LMT | 4 |
| Ministry of Defence | LMT | 4 |

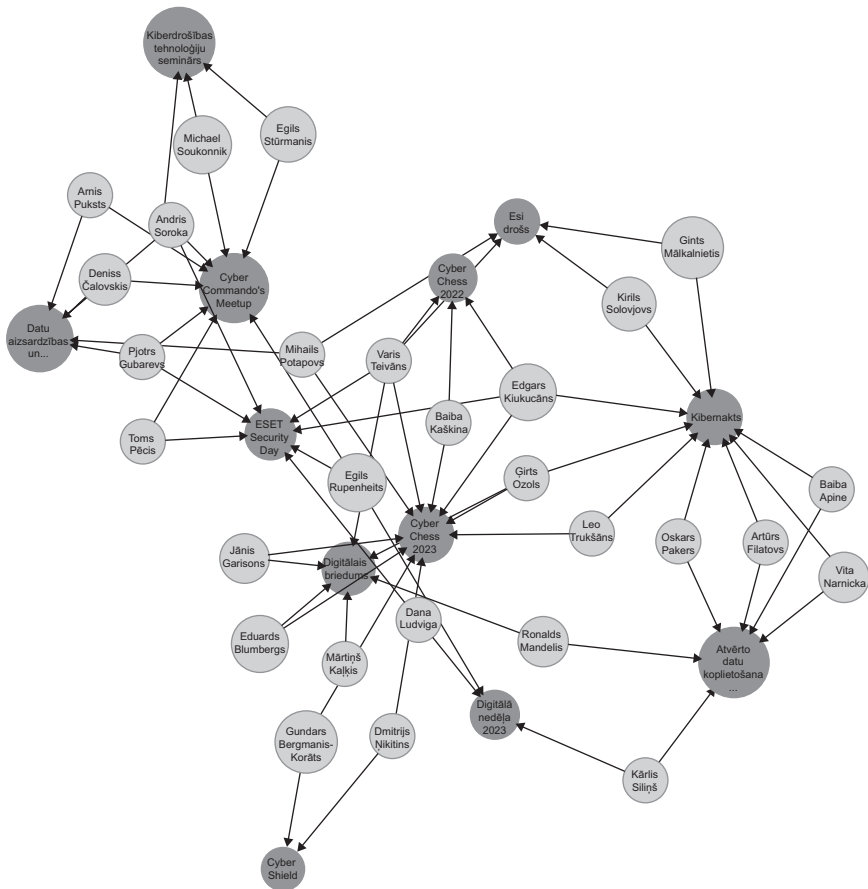


Figure 2.6 A view of the Latvian cybersecurity ecosystem graph showcasing events and individuals presenting at two or more events.

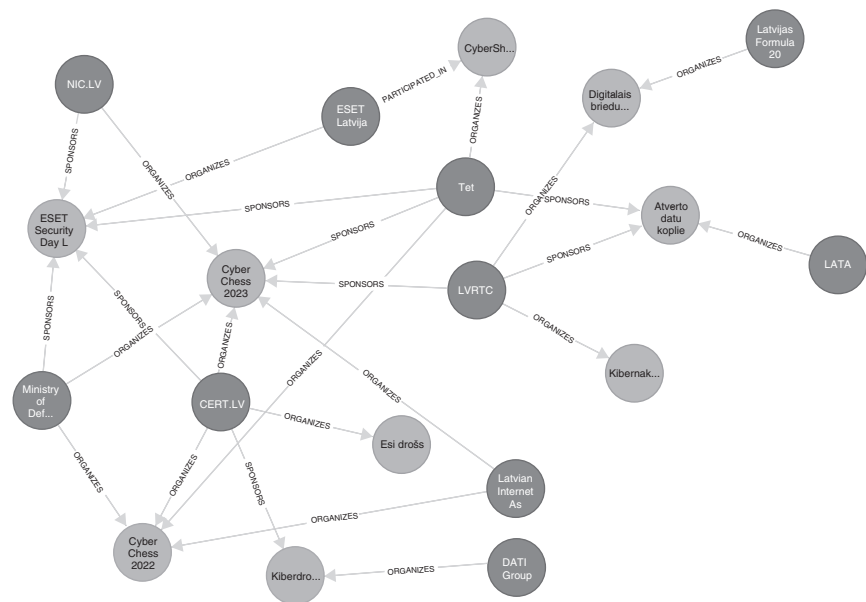


Figure 2.7 Organisational entities organising or sponsoring at least two cybersecurity events.

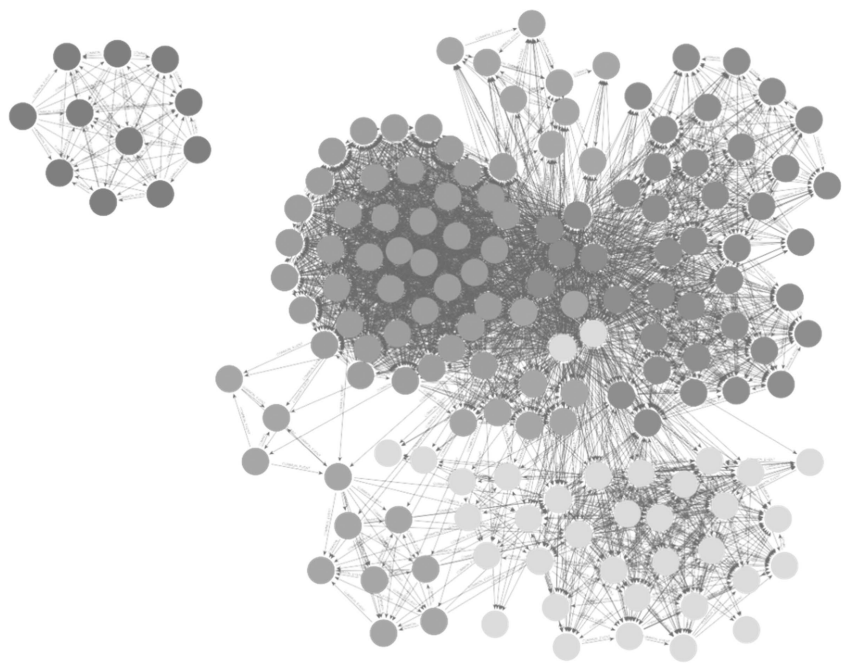


Figure 2.8 Community clusters in the Latvian cybersecurity ecosystem.

Defence are two organisational entities that have participated in the most events together, having appeared together in half of the events – 7 out of 13. Many events are attended also by participants from abroad, primarily, from the US, Poland, and Estonia.

The graph directly does not yield information about support for cybersecurity goals and resilience goals. That can be indirectly inferred from the topic of presentations and discussions. For example, CyberChess 2023 had DNS security and Cyber Warfare as keynotes and thematic sessions devoted to Strategic and political matters, DNS, and together technical matters. Thus, the main cybersecurity ecosystem goals addressed were to ensure national security and to provide secure critical infrastructure. However, Digital Week 2023 focused on the goal of rising cybersecurity awareness and involved many participants from agencies, organisations, and educational institutions. The presentations were also on know-how of business and information security. Personal and information security were the key aspects in the Annual Data Protection and Cybersecurity Forum. Thus, preliminary observations show that the events address all cybersecurity goals.

Conclusion

There is a significant theoretical and practical interest in analysing cybersecurity ecosystems because cybersecurity requires collaboration among a multitude of players. The Latvian cybersecurity ecosystem is a part of the European and Global security ecosystem. It shares many commonalities with cybersecurity ecosystems in the other EU member states. Its goals are determined by the common EU regulations and implementation is guided by common organisations such as ENISA and CERT as well as NATO.

The enterprise modelling and network analysis techniques have been used in the chapter to explore the Latvian cybersecurity ecosystem. That allows for structured and quantitative analysis. The Latvian cybersecurity ecosystem can be perceived as resilient because it addresses all resilience goals and involves participants fulfilling all resilience roles. There are clear governors and drivers in the system. The ICT service providers and educational institutions address aggregation concerns, and companies such as TET, LMT (mobile communications company), and RTU (Riga Technical University) actively engage with other participants of the ecosystem. While professional associations and media serve as reputation guardians in the ecosystem

The ecosystem analysis conducted is restricted to the events analysed. Still, that gives a good overview of the most active players in the Latvian cybersecurity ecosystem. The events are organised by governmental institutions and agencies as well as ICT service providers assuming either aggregator or modular produced roles. Currently, the Ministry of Defence and CERT.LV are the most active participants and many of the most influential individuals are also affiliated with these organisations. The new Latvian National Cybersecurity Law has come into effect on September 1, 2024, and it is expected that the National Cybersecurity Centre will assume an even larger role in driving the Latvian cybersecurity ecosystem.

The cybersecurity ecosystem communities are well-connected though there are few noticeable connections with other communities like employers or consumers associations. One exception is connections with the financial sector and the Financial Industry Association in particular.

The ecosystem analysis concerns only non-malicious participants. That applies to the generic ecosystem roles as well ecosystem goals even though some of the generic roles could have malicious business goals. Analysis of adversaries is considered out of the scope for this chapter.

References

- Abazi, B. (2022). Establishing the National Cybersecurity (Resilience) Ecosystem. In K. P. (Ed.), *IFAC-PapersOnLine* (Vol. 55, Issue 39, pp. 42–47). Elsevier B.V. <https://doi.org/10.1016/j.ifacol.2022.12.008>
- Adach, M., Hänninen, K., & Lundqvist, K. (2022a). Security Ontologies: A Systematic Literature Review. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 13585, pp. 36–53). Springer, Cham. https://doi.org/10.1007/978-3-031-17604-3_3
- Bederna, Z., & Rajnai, Z. (2022). Analysis of the Cybersecurity Ecosystem in the European Union. *International Cybersecurity Law Review*, 3(1), 35–49. <https://doi.org/10.1365/s43439-022-00048-9>
- Benetis, V. (2023). Cybersecurity-Latvia-Map. <https://Github.Com/Vibenas/Cybersecurity-Latvia-Map>
- Briscoe, G., & De Wilde, P. (2006). Digital Ecosystems: Evolving service-oriented architectures. In *Conference on Bio-Inspired Models of Network, Information and Computing Systems*. IEEE Press.
- CERT.LV. (2025). <https://cert.lv/lv/par-mums>
- Cherdantseva, Y., & Hilton, J. (2013). A reference model of information assurance & security. *Proceedings -2013 International Conference on Availability, Reliability and Security, ARES 2013*, 546–555. <https://doi.org/10.1109/ARES.2013.72>
- Chulef, A. S., Read, S. J., & Walsh, D. A. (2001). A Hierarchical Taxonomy of Human Goals. *Motivation and Emotion*, 25, 191–232. <https://doi.org/10.1023/A:1012225223418>
- CISA. (2023). CPG: Cross-Sector Cybersecurity Performance Goals. https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
- CNSSI. (2015). Glossary, Committee on National Security Systems (4009).
- D’Arcy, J., & Hovav, A. (2008). An Integrative Framework for the Study of Information Security Management Research. In Gupta, J. N. D., Sharma, S. K. (Eds.), *Handbook of Research on Information Security and Assurance* (pp. 55–67). IGI Global. <https://doi.org/10.4018/978-1-59904-855-0.ch006>
- Das, S. (2015). The Cybersecurity Ecosystem: Post-global Financial Crisis. In Chatterjee, S., Singh, N., Goyal, D., Gupta, N. (Eds.), *Managing in Recovering Markets* (pp. 453–459). Springer, New Delhi. https://doi.org/10.1007/978-81-322-1979-8_36
- Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. *Information Systems Journal*, 11(2), 127–153.
- DHS. (2011). Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action. <https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf>
- ENISA. (2017). ENISA overview of cybersecurity and related terminology. https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurity-AndRelatedTechnology.pdf

- ETSI. (2017). *CYBER: Global Cybersecurity Ecosystem*. European Telecommunications Standards Institute. https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.02.01_60/tr_103306v010201p.pdf
- Ferdinand, J., & Benham, R. (2017). The Cybersecurity Ecosystem: Defining a Taxonomy of Existing, Emerging and Future Cyber Threats. <https://www.swift.com/swift-resource/252223/download>
- Grabis, J., Tsai, C. H., Zdravkovic, J., & Stirna, J. (2022). Endurant Ecosystems: Model-Based Assessment of Resilience of Digital Business Ecosystems. *Lecture Notes in Business Information Processing* (Vol. 462, pp. 53–68). Springer, Cham. https://doi.org/10.1007/978-3-031-16947-2_4
- Kuzminykh, I., Yevdokymenko, M., Yeremenko, O., & Lemeshko, O. (2021). Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks. *International Journal of Modern Education and Computer Science*, 13(6), 60–68. <https://doi.org/10.5815/ijmecs.2021.06.06>
- Madrueno-Aguilar, R. (2016). Human Security and the New Global Threats: Discourse, Taxonomy and Implications. *Global Policy*, 7(2), 156–173. <https://doi.org/10.1111/1758-5899.12290>
- Meng, G., Liu, Y., Zhang, J., Pokluda, A., & Boutaba, R. (2015). Collaborative Security: A Survey and Taxonomy. *ACM Computing Surveys*, 48(1). <https://doi.org/10.1145/2785733>
- Ministry of Defence. (2023). National Cybersecurity Strategy 2023–2026. https://www.mod.gov.lv/sites/mod/files/document/Latvijas%20kiberdro%C5%A1%C4%ABas%20strat%C4%93%C4%A3ija%202023.-2026.gadam_.pdf
- National Cybersecurity Law (2024). <https://likumi.lv/ta/id/353390>
- Oficiālais statistikas portāls. (2023). 91,4% iedzīvotāju regulāri lieto internetu. <https://stat.gov.lv/lv/statistikas-temas/informacijas-tehn/ikt-majsaimniecibas/preses-relizes/14303-iedzivotaju-interneta?themeCode=EK>
- Oficiālais statistikas portāls. (2023). 2023. gadā sava tīmekļa vietnē ir 67,3% uzņēmumu. <https://stat.gov.lv/lv/statistikas-temas/informacijas-tehn/interneta-lietosana/preses-relizes/20982-informacijas-un?themeCode=DL>
- Qingxiong, M., Johnston, A. C., & Pearson, J. M. (2008). Information Security Management Objectives and Practices: A Parsimonious Framework. *Information Management and Computer Security*, 16(3), 251–270. <https://doi.org/10.1108/09685220810893207>
- Sandkuhl, K., Wißotzki, M., Stirna, J., & Persson, A. (2014). Enterprise Modeling: Tackling Business Challenges with the 4EM Method. *Enterprise Engineering Series*, 1–309. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083973574&partnerID=40&md5=a5942081613ca9ba889deed690bad63b>
- Tsai, C. H., & Zdravkovic, J. (2020). A Survey of Roles and Responsibilities in Digital Business Ecosystems. In S. J. Asensio E. S. (Ed.), *CEUR Workshop Proceedings* (Vol. 2793, pp. 44–53). CEUR-WS.
- Tsai, C. H., Zdravkovic, J., & Stirna, J. (2020). Capability Management of Digital Business Ecosystems – A Case of Resilience Modeling in the Healthcare Domain. *Lecture Notes in Business Information Processing* (Vol. 386, pp. 126–137). Springer, Cham. https://doi.org/10.1007/978-3-030-58135-0_11
- Tsai, C. H., Zdravkovic, J., & Stirna, J. (2022). Modeling Digital Business Ecosystems: A Systematic Literature Review. *Complex Systems Informatics and Modeling Quarterly*, 2022(30), 1–30. <https://doi.org/10.7250/csimq.2022-30.01>

3 Governance of the Latvian Cybersecurity Ecosystem

*Mihails Potapovs, Iveta Reinholde
and Kristiāns Teters*

Introduction

Although critical in our modern digital landscape, cybersecurity remains a relatively new study area, particularly within the public policy domain. As the world becomes increasingly interconnected through technological advancements, the importance of safeguarding digital infrastructure cannot be overstated. Cybersecurity encompasses a broad spectrum of practices designed to protect networks, information systems, and data from malicious acts, damage, or unauthorised access. This domain has rapidly evolved from a niche concern to a fundamental national security and economic stability component.

In the context of public policy, cybersecurity presents unique challenges and opportunities. Traditional governance frameworks, developed in an era of limited technological integration, often need help to keep up with the digital age's rapid innovations and evolving threats. The digital revolution has transformed how we communicate and conduct business and introduced new vulnerabilities that malicious actors can exploit. These changes necessitate re-evaluating existing policies and developing new strategies to mitigate risks and protect the digital assets of individuals, organisations, and nations.

The technological advancements of the 21st century have significantly altered human reality, creating a digital environment where information is ubiquitous and accessible. Interconnectedness, while fostering innovation and efficiency, also exposes critical infrastructures to potential cyber threats. As such, cybersecurity governance is not merely a technical issue but a multidimensional challenge involving legal, economic, social, and political considerations, and even factors of human behaviour. Effective cybersecurity governance requires collaboration across various sectors, including government, private industry, academia, and civil society, to develop and implement comprehensive and resilient strategies.

Like many other nations, Latvia faces the daunting task of securing cyberspace amidst these rapid technological changes. The Latvian cybersecurity ecosystem is shaped by its unique geopolitical context, regulatory environment, and the specific needs of its digital economy. Understanding the governance of the ecosystem involves examining the policies, institutions, and collaborative efforts underpinning Latvia's cybersecurity approach. By analysing these elements, this chapter

aims to provide a detailed overview of how Latvia navigates the complexities of cybersecurity governance, ensuring the protection of its digital infrastructure while promoting technological innovation and growth.

As Latvia moves forward with its modernisation efforts, the challenge will be to effectively integrate these new elements while overcoming the inertia of established practices. The new governance model aims to foster greater coordination and efficiency. Still, its success will depend on cohesively and proactively aligning various stakeholders, from governmental agencies to private sector partners. By building on its historical foundations and embracing innovative approaches, Latvia seeks to fortify its cybersecurity posture, ensuring a secure and resilient digital environment for citizens and institutions.

Thus, this chapter aims to research the critical factors shaping Latvian cybersecurity governance. It identifies and reveals path dependency factors by exploring Latvia's institutional and legal evolution in cybersecurity. By mapping the processes within the cyber ecosystem, this study seeks to uncover the intricacies of Latvia's digital and security policy, providing insights that may guide the search for a more effective and resilient governance model.

A key focus of this chapter is analysing how historical developments and previous policy decisions influence current cybersecurity practices and structures. This chapter aims to contribute to ongoing discussions on cybersecurity policy design and implementation by examining the current state of policy coordination and identifying areas for improvement. This research provides actionable insights to help policymakers and stakeholders move beyond harmful path dependencies, fostering the development of reliable future scenarios that enhance Latvia's digital security.

The Concept of Path Dependency

Path dependence refers to the concept that the decisions policymakers and bureaucrats face for given circumstances are limited by the decisions once made in the past. Page (2006) argued that path dependence means that current and future choices and organisational actions are strongly affected by past decisions. Path dependence has been applied to governmental policies (Hacker, 2002) and the selection of institutions (North, 1991). Page identifies four types of path dependence: "increasing returns, self-reinforcement, positive feedback, and lock-in" (Page, 2006).

Pierson (2000) explained that being in a state of path dependence means policymakers are constrained by positive feedback on their past policies, leading them to become locked into continuing the same policies. This positive feedback motivates and provides recognition, making it challenging to change course. As a result, policies persist until strong external forces emerge to alter the trajectory (Krasner, 1984) or until the costs of reversing the policy become higher than the costs of maintaining it (Pierson, 2000). External factors must be so influential that policymakers are willing to accept high reversal costs, which might not be politically welcomed.

Besides the types of path dependence, Page (2006) also identified two basic models of path dependence within dynamic systems: the dynamic system approach and the decision-making approach. Path dependence is strongly connected with human behavioural patterns, social connections, and institutions (Pierson, 2000). Page (2006) states that a dynamic system produces specific outcomes within a limited period. However, this limited timeframe may induce outcome dependence, where the system, governmental policy, or governmental agency becomes dependent on producing specific outcomes within that period. Consequently, the system may rely on previous paths, processes, or outcomes to generate the next iteration.

Path-dependent decision-making assumes that policymakers follow sequential steps. This approach posits that policymakers operate within bounded rationality, making decisions they can understand and whose externalities they can forecast. According to Page (2006), policymakers are likely to rely on positive past experiences and choose policy alternatives that are expected to bring positive value in the future. This reliance on familiar and previously successful strategies reinforces the continuation of established policies and practices and forces policymakers to “lock-in” and continue to stick to the previous policies (Goldstein et al., 2023). Meanwhile, path dependence allows us to explain the institutional changes and organisational decision-making processes (Beyer, 2010). Thus, path dependence can also be applied to explain the changes in the system of governance at different levels—*macro* (institutions), *meso* (technology and management), and *micro* (resources) (Vergne & Durand, 2010).

The composite-standard model of path dependence, as Boas (2007) proposed, extends the understanding of path dependence by emphasising the interplay between continuity and incremental change. The model builds on the concept of increasing returns but adapts it to accommodate the evolution of complex systems and institutions. Unlike traditional models that stress rigidity and lock-in, such as the QWERTY-inspired frameworks, the composite-standard model uses the Internet as a metaphor for systems that evolve by accumulating changes to their parts while maintaining overarching stability (Boas, 2007). This model explains how institutions adapt and transform over time without discarding their foundational structure by integrating mechanisms like layering (adding new elements) and conversion (reorienting existing elements for new purposes). The composite-standard model thus bridges the gap between stasis and change, offering a nuanced perspective on how path-dependent systems can exhibit both continuity and flexibility, making it particularly relevant for analysing institutional evolution and policy adjustments in dynamic governance systems.

Methods and Approach

To reveal the path dependency, the authors will split the Latvian experience into three main periods of evolution. Each period will be analysed and structured, with particular attention to the key factors determining policy, uncertainties and risks the policy designers faced, and the type of policy coordination tools used.

Path dependency generally refers to how an organisation or system's historical choices and established practices influence its current behaviour and future decisions. Under the analysis category "factors", the authors will reveal such issues as historical precedents (like previous decisions made and non-decisions), organisational inertia, interests of different stakeholders, and resource allocation. Legal and regulatory frameworks frame the factors; thus, the critical legal acts will also be explored. Within the category "uncertainties", this chapter will reveal such an issue as geopolitical and technological changes and economic fluctuation to the extent they can affect cybersecurity. Finally, the category "policy coordination tools" includes intergovernmental coordination tools, strategies and strategic frameworks, capacity-building strategies, and implementation tools of the governmental visions.

This chapter assumes that path dependence is strongly related to a long period of institutional stability that allows organisations to reach an equilibrium (Baumgartner & Jones, 1993; Mahoney, 2000). Therefore, this chapter will also explore whether all four types of path dependence identified by Page (2006): "increasing returns, self-reinforcement, positive feedback, and lock-in", are present in the different stages of the evolution of cybersecurity governance. Such an approach, where other criteria are mixed, allows for capturing the unique cybersecurity features in Latvia and designing the future model.

Evolution of Cybersecurity Governance

Latvia's cybersecurity governance has evolved over more than two decades, during which the country has continually adapted to new realities. Domestic and EU-driven legal reforms have played a pivotal role in shaping its regulatory environment. Technological advancements have also been a significant driving force, with each innovation introducing new vulnerabilities and necessitating updated security measures. The dynamic nature of cyber threats has required a responsive and adaptive approach to cybersecurity, with strategies evolving to address emerging forms of cybercrime, espionage, and other malicious activities.

Global trends have also influenced Latvia's cybersecurity strategies. Adopting zero-trust principles, which assume that threats can come from inside and outside the network, has become increasingly important. Additionally, rising concerns about supply chain security have highlighted the need for comprehensive strategies to protect against vulnerabilities in the broader ecosystem of suppliers and partners.

In 2022, the Latvian government embarked on the most extensive modernisation of cybersecurity governance in the country's history. This ambitious effort represents a pivotal moment for Latvia, carrying profound implications. The modernisation introduces a semi-centralised cybersecurity governance model, expands the institutions' mandates, and combines a novel regulatory framework with robust enforcement mechanisms to ensure compliance and resilience across sectors (Ministry of Defence, 2022).

However, implementing the modernisation effort comes with significant challenges, primarily shaped by the path dependency of previous governmental actions.

Over the past two decades, Latvia's cybersecurity governance has evolved through incremental transformations, with each new development building upon existing structures. These changes have been driven by a combination of national and EU legal reforms, rapid technological advancements, and an increasingly complex threat landscape. While these factors have pushed Latvia towards greater resilience, they have also reinforced established frameworks, making structural shifts more challenging to implement.

First Period (2002–2013)

The first formal IT security requirements for state information systems were put in place with the Law on State Information Systems (2002) and the Cabinet Regulation No 765 "General Security Requirements for State Information Systems" (2005). These regulatory frameworks marked a significant milestone in Latvia's IT security field by providing, for the first time, a structured approach to security at the technical, procedural, and document levels. However, these requirements initially applied only to a limited number of "state information systems"—a defined category encompassing structured sets of information technologies and databases that facilitate the initiation, creation, collection, accumulation, processing, use, and destruction of information necessary for performing governmental functions.

Latvia took a significant step in strengthening formal cybersecurity requirements at the legal level in 2010 by adopting the IT Security Law (2010). This development was partly catalysed by the so-called "Neo case". In 2009–2010, a researcher and whistleblower Ilmārs Poikāns, known as "Neo", accessed approximately 7.5 million classified files from Latvia's tax authority, the State Revenue Service (VID). Exploiting a relatively simple flaw in the electronic security system of the VID's Electronic Declaration System, "Neo" obtained sensitive data over the course of three months and subsequently leaked selected information to the public. This high-profile incident exposed critical vulnerabilities in national cybersecurity infrastructure and underscored the urgent need for regulatory improvements (Collier & Zablovskā, 2013).

For the first time, the IT Security Law (2010) defined the entities subject to cybersecurity requirements, primarily central and local government institutions. Among the most notable changes was introducing a formal requirement for each entity to employ a chief information security officer (CISO). The CISO's primary responsibilities included: (1) establishing an IT security regime within their institution, (2) conducting annual cybersecurity training for employees, and (3) attending training events organised by CERT.LV at least once a year.

Additionally, institutions were mandated to report IT security incidents to the national Computer Security Incident Response Team (CSIRT), enhancing coordination and strengthening the national response to cybersecurity threats. Latvia addressed the need for a national CSIRT by establishing CERT.LV back in 2011. Initially, CERT.LV operated under the authority of the Ministry of Transport (2011) as the national IT security incident response institution. However, in 2013, responsibility for the overall ICT security policy and authority over CERT.LV

was transferred to the Ministry of Defence (Kaškina, 2021). Notably, CERT.LV was, and remains, formally a laboratory within the Institute of Mathematics and Computer Science of the University of Latvia. At the time of its establishment, this allocation was a logical choice due to the Institute's domain expertise, as the Institute had operated LATNET CERT, the first CSIRT in Latvia, since 2006, providing foundational knowledge in handling cybersecurity incidents (Kaškina, 2021), initially within the academic network (Skutelis, 2024). While the functions and responsibilities of CERT.LV under the Ministry of Defence have expanded significantly over time, its connection to the research institution has been maintained. Such an arrangement has introduced some administrative complexities like double supervision. Meanwhile, it also fostered closer ties with academia and research.

It should be noted that while entities falling under the scope of the IT Security Law had specific obligations, there were no dedicated supervision or enforcement mechanisms in place. In theory, each institution was accountable to a hierarchically higher entity (e.g., an executive agency reporting to a ministry, or a ministry accountable to the government). However, in practice, operational or technical cybersecurity oversight often did not occur (Ministry of Defence, 2022). The only category of entities where supervision was explicitly enforced was national critical ICT infrastructure, which was included on a classified list under the National Security Law (2000) and supervised by the Constitution Protection Bureau (SAB), Latvia's external intelligence agency. In 2011, the Cabinet Regulation No 100 was adopted, establishing baseline security measures for national critical ICT infrastructure. It is important to note that these requirements differed from those applied to physical critical infrastructure, which was managed by a partially overlapping set of entities under the supervision of the State Security Service (VDD), Latvia's domestic intelligence agency.

In 2011, the National IT Security Council was established to improve horizontal coordination among responsible ministries and agencies, particularly on strategic cybersecurity issues. Initially, the Ministry of Transport performed the secretariat functions of the council, a role later transferred to the Ministry of Defence (LETA, 2013). Although the council's overall role has mainly been consultative, supportive, and collaborative, it convened relatively high-ranking officials, including state secretaries, deputy state secretaries, and heads of agencies, and achieved good level of coordination and mutual understanding. The high-level representation provided an opportunity to elevate cybersecurity issues to the top management's agenda. The council also served as a platform for conducting high-level tabletop exercises, fostering preparedness and collaboration. Notably, the first such exercise with involvement of the government was organised by CERT.LV in 2012 (Petrāne, 2012).

In 2013, Latvia established the Cyber Defence Unit (CDU) within the National Guard, part of the National Armed Forces, to bolster the nation's cyber resilience in the face of escalating threats in the digital domain. The initiative aimed to create a reserve force of highly skilled information technology experts from the private sector and public institutions, who could support the national cyber defence efforts during crises or wartime. Essentially similar to the Estonian Defence League's

Cyber Unit (Cardash et al., 2013), the CDU was designed to operate collaboratively with CERT.LV, the country's primary cyber incident responders, focused on rapid response to cyber incidents, conducting expert assessments, and participating in national and international cyber defence training. By leveraging the expertise of patriotic volunteers and fostering public-private partnerships, the CDU sought to enhance Latvia's capability to address critical cyber threats while promoting the professional development of IT specialists and strengthening national security (Ministry of Defence, 2013).

Second Period (2014–2020)

The second period was marked by a significant deterioration in the security environment in the region, primarily driven by Russia's war of aggression against Ukraine and the illegal annexation of Crimea. These events underscored growing geopolitical instability, prompting heightened concerns about regional security and the need for stronger defence and resilience-building measures among NATO and EU member states. This period also witnessed the adoption of key legal acts that shaped Europe's cybersecurity landscape.

With the adoption of the Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS), Latvia faced a significant challenge. The country lacked a formal supervisory authority for entities subject to eIDAS requirements. Furthermore, no single institution was responsible for overseeing cybersecurity at the national level. Responsibilities were fragmented across multiple bodies, with CERT.LV and the Ministry of Defence playing key roles. However, with limited supervisory powers, these entities lacked the authority to enforce cybersecurity standards, effectively leaving organisations to handle their cybersecurity independently, without external oversight or support. Meanwhile, sectoral ministries maintained general oversight within their respective domains, but without the mandate to enforce specific cybersecurity requirements, further contributing to a fragmented and uncoordinated security landscape.

To address the regulatory requirements introduced by eIDAS, the Ministry of Environmental Protection and Regional Development (VARAM) (2015) made several proposals to establish an oversight body capable of ensuring compliance and providing effective supervision:

The **decentralised model** proposed dividing supervisory functions between the Ministry of Defence and the State Data Inspectorate (DVI), an executive agency under the Ministry of Justice, as both had relevant experience and evolving responsibilities in their respective domains. The DVI, already tasked with overseeing data processing activities and set to become the competent authority under the GDPR, would take on responsibility for supervising electronic identification and trust service providers in the context of eIDAS. Meanwhile, the Ministry of Defence, which had been gradually consolidating its cybersecurity policy portfolio, would assume responsibility for national cybersecurity, overseeing the security

of the Internet, private networks, and information systems. Under this model, other ministries would retain their specialised roles. Notably, the VARAM would continue monitoring the general security of state information systems, consistent with its broader responsibilities for digital policy. In contrast, the Ministry of Transport would remain responsible for managing emergency situations related to the state electronic communications networks and services, and overseeing the top-level domain.lv and the electronic numbering system (ENUM) registrar.

The “**centralised**” model proposed transferring all supervisory authority functions to the Ministry of Defence. This model envisioned creating a unified ICT security competence centre under the Ministry of Defence. Within this centre, a new supervisory authority would be established to oversee qualified electronic identification and trust service providers and handle national competence functions related to the security of networks and information systems. Despite its name, this model did not imply the new competence centre would absorb the functions of other key institutions. VARAM would continue monitoring the general security of state information systems, aligning with its digital policy role; the Ministry of Transport would retain responsibility for managing emergencies involving the state electronic communications networks and services, as well as overseeing the top-level domain.lv and the ENUM registrar. The DVI would continue to handle security aspects related to personal data protection. This model aimed to streamline supervisory functions under the Ministry of Defence while preserving the specialised roles of other institutions in their respective domains.

The compromise, the **semi-centralised model** proposed the establishment of a unified ICT security competence centre, functioning as a collegial body rather than a new supervisory institution, to minimise administrative burden. This new body would take the form of an interinstitutional committee, comprising representatives from the Ministry of Defence, the Ministry of Justice, the DVI, the VARAM, the Ministry of Transport, the Ministry of the Interior, and the CERT.LV. The Ministry of Defence would serve as the secretariat for the committee, managing administrative functions and steering its work, while CERT.LV would provide technical support, ensuring the necessary expertise for performing supervisory functions over qualified electronic identification and trust service providers. Over time, the new body would also assume the responsibilities of the national competent authority for the security of networks and information systems. This model aimed to balance centralisation and collaboration, leveraging the strengths of existing institutions while creating a more cohesive and efficient framework for cybersecurity oversight.

The compromise approach was deemed the most appropriate, considering the roles and interests of the involved stakeholders, who wished to maintain their involvement in the process. Consequently, on 1 November 2016, the Cabinet of Ministers, through Regulation No 695, established a new collegial body, officially appearing on 4 November 2016 as the Electronic Identification Supervisory Committee (EIUK). In 2017, the committee was renamed the Digital Security Supervisory Committee (DDUK) to reflect its evolving scope. Initially, the committee was tasked with supervising electronic identification and trust services. However,

its mandate expanded significantly following the adoption of the Network and Information Systems (NIS) directive in 2016, the EU's first comprehensive cybersecurity legislation. This marked the beginning of its broader role in ensuring digital security and overseeing the implementation of the directive's requirements.

The implementation of the NIS directive brought significant changes to Latvia's cybersecurity landscape:

- 1 **Designation of Entities under NIS:** The directive introduced two categories of entities under its scope: "operators of essential services" (OES) and "digital service providers" (DSPs). Latvia adopted a semi-centralised approach to the designation of OESs by issuing the Cabinet Regulation No 43 (2019). This regulation assigned sectoral ministries the responsibility for designating OESs within their respective areas. These designations were then forwarded to the Ministry of Defence, acting as the secretariat for the Digital Security Supervisory Committee. The Ministry aggregated the lists, ensuring horizontal coordination and situational awareness of essential cyber infrastructure. The Committee subsequently approved the national OES list. For DSPs, Latvia adopted a self-assessment approach during the implementation of the NIS directive and its associated changes to the ICT Security Law. This method allowed DSPs to evaluate their own compliance, a practice that was later extended following the adoption of the NIS2 directive (2022) for "important" and "essential" entities.
- 2 **Incident Response Requirements:** The NIS directive required EU member states to report major ICT security incidents to the European Union Agency for Cybersecurity (ENISA) and the European Commission. Latvia addressed this requirement through Cabinet Regulation No 15 (2019), which adopted a matrix-based approach to defining incident thresholds and identification criteria. The matrix assessed incidents based on two main factors: the number of users affected and the duration of the incident. Additionally, Latvia implemented ENISA's CIRAS-T notification system, distributing accounts to responsible entities to ensure prompt reporting of NIS incidents. Notably, Latvia has not recorded any significant NIS incidents to date.
- 3 **Establishment of Universal Requirements:** A significant milestone during this period was the creation of universal ICT security requirements, introduced through Cabinet Regulation No 442 (2015). These requirements built upon the earlier Cabinet Regulation No 765 (2005), incorporating updated practices and international standards, particularly ISO/IEC 27001:2013. The regulation established a standardised ICT security benchmark for entities under the IT Security Law, initially covering central and local government institutions and later expanding to include OESs and DSPs. The regulation specified documentary, technical, and organisational ICT security measures at the information system level. Over time, Latvia has shifted its focus from solely information system-oriented measures to a broader, more holistic approach to ICT security.

The second period is also marked by the establishment of a second national-level CSIRT, the Military Computer Emergency Response Team (MilCERT), which is

responsible for cyber incident response within the Ministry of Defence, the National Armed Forces, and other defence institutions (Gnēze, 2016). While MilCERT was formally placed under the authority of the State Secretary of the Ministry of Defence, it has effectively operated as a unit within the Defence Intelligence and Security Service (MIDD), an intelligence agency under the Ministry of Defence. Due to the specific nature of its operations, the scope of MilCERT's activities is considerably narrower than that of CERT.LV. MilCERT does not engage in activities such as research or public awareness raising. However, there is strong collaboration and information exchange between MilCERT and CERT.LV, as outlined in the National Cybersecurity Strategy of Latvia (Ministry of Defence, 2019). This cooperation ensures a cohesive approach to addressing cybersecurity threats at both civilian and military levels. Despite the creation of MilCERT, CERT.LV has maintained its role as Latvia's national CSIRT, handling broader cybersecurity responsibilities, including public awareness, research, and civilian-focused incident response.

Third Period (2021 to Current)

The latest period in the evolution of Latvian cybersecurity governance is marked by a comprehensive modernisation effort that is still underway. This reform has been driven by several critical factors, reflecting internal and external pressures that have necessitated a significant overhaul of the existing framework. One of the primary reasons for this modernisation is the growing complexity and number of cyberattacks, coupled with the worsening security situation in the region.

In 2022, Latvia emerged as one of the most targeted countries by cyberattacks in the European Union, ranking second only to Poland, with approximately 16% of the total incidents reported among EU member states. The number of registered cyber incidents in Latvian government institutions saw a dramatic surge, almost quadrupling compared to 2021, highlighting the escalating cyber threats (LETA, 2023). While Advanced Persistent Threat groups linked to the Russian Federation have been active in Latvian cyberspace long before Russia's full-scale invasion of Ukraine (VDD, 2020), the deteriorating geopolitical environment has elevated the importance of securing cyberspace from national security to an existential statehood issue. For Latvia, ensuring the integrity and security of its digital infrastructure is crucial not just for its operational continuity but also for its sovereignty and stability.

Additionally, there has been a growing consensus among cybersecurity experts that the *laissez-faire* approach towards organisational cybersecurity is no longer effective. With robust legal and institutional frameworks, it is easier to ascertain the compliance levels of various entities with existing legislation, even within the public sector. This lack of oversight and accountability has highlighted the need for a more structured and enforceable governance model (Ministry of Defence, 2022). However, the impetus from the European Union has also played a significant role in driving Latvia's cybersecurity modernisation. The negotiations on the NIS2 directive further highlighted member states' need to enhance their cybersecurity

frameworks. For Latvia, it became apparent that more resources and the current governance model needed to be improved for implementing the new legislation, particularly regarding the supervision and enforcement of baseline cybersecurity requirements. The sheer scale of this task is underscored by the dramatic increase in the number of entities to be supervised, rising from a two-digit figure to over 2,000 (Saeima, 2024).

At the time, various policy options were discussed to address Latvia's pressing need for cybersecurity modernisation. All these discussions converged on the necessity of changes in the institutional structure, ultimately leading to the creation of the National Cybersecurity Centre (NCSC), akin to similar institutions in several other EU member states (Backman, 2015). The aim was to consolidate existing resources, allocate additional resources, and increase personnel to enhance Latvia's cybersecurity capabilities. The primary debate centred around the institutional setting of the NCSC—whether it should be established as a separate institution or integrated within the existing framework. In its report “On Improving National Cybersecurity Governance”, the Ministry of Defence (2022) proposed three policy options for consideration:

- 1 **NCSC as an Executive Agency:** This option proposed creating a new executive agency subordinate to the Minister of Defence by consolidating the Ministry's National Cybersecurity Policy Coordination Section and CERT.LV. This approach aimed to streamline operations and centralise resources under a single authoritative body.
- 2 **NCSC as a Ministry Department:** Another option was to maintain the current system, which includes the functions of the Ministry of Defence and CERT.LV are separate. This would involve establishing the NCSC as a unit, more precisely a department, within the Ministry of Defence, replacing the National Cybersecurity Policy Coordination Section, and maintaining the role and responsibilities of CERT.LV.
- 3 **The Hybrid Solution:** The third option, ultimately recommended by the Ministry of Defence as the prime option, was to create a “virtual” NCSC. This hybrid model combines functions performed by the personnel of both CERT.LV and the Ministry of Defence, while also establishing a Cybersecurity Policy Department within the Ministry to replace the National Cybersecurity Policy Coordination Section and maintaining the institutional autonomy of CERT.LV. This solution was a compromise, offering a blend of centralised oversight and distributed operational capabilities.

Adopted on 7 June 2022, the report acknowledged establishing the NCSC as a separate agency as a potential long-term solution. However, no immediate decision was made to implement this concept, and a hybrid solution was chosen instead. Despite the ambitions and political will for change, the adopted approach did not significantly deviate from the existing institutional setup. The new model retained a unit within the Ministry of Defence as the central authority with policy coordination functions. This unit was also tasked with supervising essential and important entities

under the NIS2 directive. As part of the Institute of Mathematics and Computer Science of the University of Latvia, CERT.LV continued with its existing functions. Counterintuitively, the Digital Security Supervisory Committee was not disbanded. Instead, it was assigned the additional task of approving the list of essential and important entities—a responsibility that could have been more efficiently handled by the NCSC, avoiding the burdensome interinstitutional decision-making procedure. Furthermore, the National IT Security Council was renamed the National Cybersecurity Council, but its functions remained unchanged, primarily serving as a strategic, consultative body (Prime Minister, 2024).

While establishing the hybrid NCSC was perceived as largely symbolic rather than driven by operational necessity, it marked a notable development in Latvia's cybersecurity framework. Despite maintaining much of the status quo, one significant change was allocating additional resources to the NCSC. By 2025, these resources will include an expanded budget and the creation of 47 additional positions within the Ministry of Defence and CERT.LV (Cabinet of Ministers, 2022). Additionally, the National Cybersecurity Policy Coordination Section within the Ministry of Defence was reorganised into the Cybersecurity Policy Department, operating under the authority of the Undersecretary of State-Policy Director, who also became the formal head of the NCSC.

More importantly, this represented a key step in Latvia's broader cybersecurity modernisation efforts. The second, more complex phase involved drafting, negotiating, and adopting the National Cybersecurity Law, a cornerstone legislative act. Adopted on 20 June 2024 and effective 1 September 2024, this law replaced the previous IT Security Law. A key feature of the new legislation was its significantly broadened scope, driven primarily by the requirements of the NIS2 directive. The law also formally established the NCSC, solidifying its role within Latvia's cybersecurity landscape.

Under NIS2, the EU's focus has shifted from OES and DSPs to essential and important entities, encompassing a broader range of sectors. This expansion includes transport, food and water supply, industrial production, and more, reflecting the growing recognition of the interconnected nature of modern ICT infrastructure. With supply chains extending beyond national borders, comprehensive cybersecurity measures across all high-priority sectors are of utmost importance. While directives, with their indirect applicability, allow for interpretation by member states, Latvia has adopted a more comprehensive approach with its new legislation. The scope of entities covered has been significantly broadened beyond the minimum requirements of the NIS2 directive. For instance, Latvia has included all local governments (municipal councils) and all independent institutions at the central government level, such as the *Saeima* (Parliament), the central bank, and the courts. This inclusion builds upon the framework of the previous IT Security Law which already included all central and local government institutions.

It is important to note that while some essential entities overlapped with the national ICT critical infrastructure, their special status was preserved, with the SAB—rather than the NCSC—retaining supervisory authority over them. Despite the administrative complexity, a positive development emerged: SAB expressed

willingness to align the baseline requirements for national critical ICT entities with those for essential and important entities under a unified Cabinet Regulation. The draft Cabinet Regulation, titled “Baseline Cybersecurity Requirements”, is currently being negotiated by the responsible institutions.¹ This regulation represents a significant shift in Latvia’s cybersecurity framework. For the first time, it introduces comprehensive requirements for entities and clear supervision and enforcement mechanisms, including sanctions for non-compliance.

The new requirements mark a substantial departure from the information system-centric approach seen in Cabinet Regulations No 765 and No 442. Instead, they adopt a more holistic focus on the cybersecurity of organisations as a whole. Key changes include: (1) consolidation of documentation and notification requirements, (2) clearly defined roles of the CISO and the organisation’s management, (3) implementation of controls and self-assessments, (4) alignment with globally accepted standards such as ISO/IEC 27001:2022 and NIST frameworks, and (5) emphasis on supply chain security. This approach reflects a broader, more integrated vision for cybersecurity, ensuring that organisations are better equipped to manage risks across their entire structure.

Results and Discussion

Latvia’s approach to cybersecurity governance has evolved in three distinct periods, each marked by milestones such as the IT Security Law in 2011, the influence of the first NIS directive in 2016, and the comprehensive modernisation of 2022. This trajectory highlights a progressive response to both internal demands and EU requirements. Latvia’s cybersecurity governance reflects strongly inclined path dependence, where previous decisions and established practices strongly shape current policy directions. For Latvia, path dependence manifests mainly through self-reinforcement, positive feedback, and lock-in (in some cases also increasing returns), making shifts challenging unless substantial external pressures emerge (see Table 3.1).

Each of the three stages of Latvia’s cybersecurity policy evolution has been shaped by significant incidents (e.g., the Neo case), EU legislation (such as the eIDAS regulation and the NIS and NIS2 directives), and escalating geopolitical threats, particularly from Russia. These developments have exposed vulnerabilities in the existing approach and underscored the need for reform. As part of the 2022 reform, the hybrid NCSC model was established, signalling Latvia’s commitment to modernisation while retaining elements of the existing governance framework. This decision reflects the influence of path dependency, as historical structures and practices were preserved despite the introduction of the NCSC. CERT.LV and the Ministry of Defence continue to operate with distinct operational and policy responsibilities, maintaining much of the pre-existing institutional setup.

Latvia’s experience offers valuable insights for other countries grappling with the challenges of modernising their cybersecurity governance in the context of path dependency and external pressures. The evolution of Latvia’s cybersecurity governance, marked by the interplay of EU requirements, domestic incidents, and

Table 3.1 Types of path dependency observed in the case study

| <i>Path dependency type</i> | <i>Description</i> | <i>Examples</i> |
|-----------------------------|---|--|
| Increasing returns | Benefits increase as an institution/system continues down a path, making deviations less likely. | Development of CERT.LV within the Institute of Mathematics and Computer Science allowed for cumulative expertise and operational capacity, strengthening its central role in national cybersecurity. The academic link provided ongoing research benefits, making changes to its institutional framework less attractive despite administrative complexities. |
| Self-reinforcement | The system develops dynamics that stabilise the current path and reduce the likelihood of change. | Hierarchical accountability under the IT Security Law reinforced decentralised supervision structures, even though operational oversight is often lacking. Despite inefficiencies in its inter-institutional decision-making processes, retention of the Digital Security Supervisory Committee under the NIS2 directive showcased the reinforcement of existing institutional roles. |
| Positive feedback | Success or perceived success of past actions reinforces the continuation of similar strategies. | The expansion of the IT Security Law and its requirements to include more entities under subsequent regulations reflects reliance on familiar, successful policy models. Continued reliance on Cabinet Regulations (e.g., No 765 and No 442) to set cybersecurity requirements, building on past practices perceived as effective, despite evolving needs for enforcement mechanisms. |
| Lock-in | Changing the path becomes prohibitively costly or politically unfeasible. | CERT.LV's placement within academia persisted due to its historical success and integration, making a transition to a standalone model administratively and politically complex. The SAB's supervisory role over critical ICT infrastructure remained under the NIS2 directive, reflecting lock-in to existing structures despite the administrative challenges of managing overlapping oversight responsibilities. |

geopolitical threats, highlights a pattern of incremental progress constrained by historical structures. This case underscores the importance of balancing innovation with institutional stability—a challenge many nations face. One key takeaway from Latvia's approach is the role of EU legislation as an external force driving reform. For instance, the NIS and NIS2 directives served as catalysts for Latvia to expand the scope of its cybersecurity governance. Similar patterns can be observed in other EU member states, where directives provide a framework for harmonisation but allow flexibility in implementation (Adams et al., 2015).

Another relevant finding is the enduring influence of path dependency in shaping governance structures. While operationally effective, Latvia's reliance on CERT.LV reflects the challenges of transitioning away from entrenched frameworks. This phenomenon is not unique to Latvia; countries with deeply rooted institutional arrangements often face similar difficulties in restructuring governance models. For example, Germany's federal cybersecurity framework has struggled with decentralisation issues (Ulmer, 2021), mirroring Latvia's challenges with distributed responsibilities among ministries. Understanding and addressing such dependencies can help nations build more cohesive cybersecurity strategies without completely dismantling established systems.

The semi-centralised governance model, in which a unified cybersecurity competence centre operates as a collegial body, highlights key elements of the cybersecurity ecosystem in place. Pedersen (2023) defines the essential aspects of a science-for-policy ecosystem, which can be effectively applied to cybersecurity governance as well. According to Pedersen, an ecosystem is most effective when its members share a common understanding and uphold high levels of transparency, responsibility, and accountability.

An effective cybersecurity ecosystem also requires mechanisms for continuous learning and adaptation. The NCSC, as the unified cybersecurity competence centre, with CERT.LV playing a pivotal role, has maintained and continues to develop its function as Latvia's national CSIRT. It handles a broad range of cybersecurity responsibilities, including public awareness, research, and civilian-focused incident response. These functions are crucial for organisational learning in complex organisational settings, as a cybersecurity ecosystem comprises many interconnected actors.

The new National Cybersecurity Law (2024) represents an ambitious step forward in cybersecurity governance. It expands the scope of cybersecurity measures beyond the minimum requirements of EU directives, incorporating a wider range of actors, including local governments and important service providers, as well as setting higher security standards for critical infrastructure operators. By establishing baseline cybersecurity requirements for both public and private sectors, the government demonstrates a strong commitment to comprehensive cyber resilience.

A cybersecurity ecosystem is composed of central and local government bodies, private companies, non-governmental organisations, individuals, and an ever-expanding universe of digital data, technologies, and infrastructure. Like any other ecosystem, it is characterised by connectivity, coordination, and continuous

learning (Pedersen, 2023). Sadik et al. (2020) emphasise the importance of a well-functioning cybersecurity ecosystem in protecting system participants from cyber threats, such as vulnerability exploitation and data breaches. They argue that connectivity fosters shared learning, enabling organisations to implement the most effective risk mitigation strategies in cyberspace.

Furthermore, continuous monitoring, auditing, reviewing, and compliance assessments are critical to maintaining cyber resilience (Sadik et al., 2020). In Latvia, these oversight functions are assigned to the NCSC. However, fostering effective learning and knowledge-sharing among ecosystem participants remains a challenge due to the broad and cross-sectoral nature of Latvia's cybersecurity landscape. Addressing these challenges will require enhanced mechanisms for knowledge exchange, improved sectoral coordination, and strengthened collaborative cybersecurity frameworks.

Conclusion and Policy Recommendations

Latvia's cybersecurity ecosystem governance reflects a complex interplay of historical path dependencies, emerging risks, and evolving policy tools. While incremental progress has fortified foundational capabilities, persistent fragmentation and reliance on legacy practices constrain systemic efficacy. Nevertheless, the new National Cybersecurity Law (2024) and the hybrid NCSC model illustrate that incremental progress is possible, even in the face of path dependency.

The hybrid approach exemplifies an attempt to balance continuity with innovation, though its long-term success hinges on aligning institutional roles and resources. By integrating historical strengths, such as CERT.LV's domain expertise, with modern demands for accountability and enforcement, Latvia has demonstrated a pathway for other nations to enhance their cybersecurity resilience. While challenges remain, particularly in aligning institutional roles and responsibilities, Latvia's experience highlights the importance of adaptability, innovation, and sustained political commitment in navigating the complexities of cybersecurity ecosystem governance.

To transcend harmful path dependencies, Latvia is expected to:

- 1 **Accelerate centralisation of supervisory authority to eliminate inefficiencies.** A more centralised cybersecurity governance model, with the NCSC as the unified competence centre, would streamline oversight, reduce bureaucratic complexity, and improve the enforcement of cybersecurity policies. This would ensure a more coherent approach to national cybersecurity and facilitate better coordination among key stakeholders.
- 2 **Transition responsibilities from legacy bodies like the DDUK to the NCSC.** Consolidating responsibilities under the NCSC would enhance operational efficiency by reducing redundancies and ensuring a single authoritative body oversees and enforces the implementation of national cybersecurity policies. This would enable a clearer division of responsibilities and a more agile response to emerging threats.

- 3 **Clarify roles between the responsible institutions (notably SAB and NCSC).** Clearly delineating the responsibilities of supervisory institutions would prevent overlapping mandates and potential functional duplication, enhance accountability, and ensure that cybersecurity policies and enforcement mechanisms are efficiently executed.
- 4 **Emphasise enforcement and compliance mechanisms to enhance accountability.** Strengthening regulatory enforcement, introducing more stringent compliance checks, and applying penalties for non-compliance would ensure that all essential and important entities adhere to national and European cybersecurity standards.
- 5 **Invest in capacity-building initiatives to address the growing demand for cybersecurity expertise.** Expanding training programmes, increasing funding for cybersecurity education and skills, making use of the relevant EU instruments, such as the Digital Europe programme, and fostering collaboration with academic institutions and the cybersecurity competence community, would help bridge the cybersecurity skills gap and develop a stronger workforce capable of addressing evolving cyber threats.
- 6 **Leverage CERT.LV's academic ties for research and training, ensuring operational alignment with the NCSC.** Strengthening the relationship between the NCSC and the academic sector would facilitate ongoing research, promote innovation in cybersecurity practices, and provide structured training programmes that align with national cybersecurity policy objectives.
- 7 **Foster public-private partnerships to address supply chain vulnerabilities.** Enhanced collaboration with private sector stakeholders, would enable better risk assessment, knowledge-sharing, and joint cybersecurity initiatives to mitigate threats arising from supply chain dependencies.

Note

- 1 Data as of February 2025.

Bibliography

- Adams, S., Brokx, M., Dalla Corte, L., Galič, M., Kala, K., Koops, B. J., Leenes, R., Schellekens, M., Silva, K. E., & Skorvanek, I. (2015). *The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK*. Tilburg University. <https://research.tilburguniversity.edu/en/publications/de7f8bd7-3f76-477b-9dc0-560b86ac7e85>
- Backman, S. (2015). Organising National Cybersecurity Centres. *Information & Security*, 32(1), 9–16. <https://doi.org/10.11610/isij.3206>
- Baumgartner, F. R., & Jones, B. D. (1993). *Agendas and instability in American politics*. University of Chicago Press. <https://doi.org/10.7208/chicago/9780226039534.001.0001>
- Beyer, J. (2010). The Same or Not the Same-on the Variety of Mechanisms of Path Dependence. *International Journal of Humanities and Social Sciences*, 4(3), 186–196. https://www.researchgate.net/publication/242586728_The_Same_or_Not_the_Same_-_On_the_Variety_of_Mechanisms_of_Path_Dependence

- Boas, T. C. (2007). Conceptualizing Continuity and Change: The Composite-Standard Model of Path Dependence. *Journal of Theoretical Politics*, 19(1), 33–54. <https://doi.org/10.1177/0951629807071016>
- Cabinet of Ministers. (2022). Minutes of the Cabinet Meeting of 7 June 2022. (N°30/4.§). <https://tapportal.mk.gov.lv/meetings/protocols/116bc8fa-d771-48c4-840c-2257befde8f1#meeting-protocol-preview-30>
- Cabinet Regulation N°15 of 15 January 2019 “Regulations Regarding the Security Incident Relevance Criteria, Reporting Procedures, and Content of Report”. <https://likumi.lv/ta/id/304284>
- Cabinet Regulation N°43 of 15 January 2019 “Regulations Regarding the Conditions for the Determination of Significant Disruptive Effect of a Security Incident and the Procedures by which the Status of an Operator of Essential Services and Essential Services are Granted, Reviewed, and Terminated”. <https://likumi.lv/ta/id/304327>
- Cabinet Regulation N°100 of 1 February 2011 “Procedures for the Planning and Implementation of Security Measures for the Critical Infrastructure of Information Technologies”. <https://likumi.lv/ta/id/225776>
- Cabinet Regulation N°442 of 28 July 2015 “Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements”. <https://likumi.lv/ta/id/275671/redakcijas-datums/2023/03/15>
- Cabinet Regulation N°695 of 1 November 2016 “By-Laws of the Electronic Identification Supervisory Committee”. <https://likumi.lv/ta/id/286009/redakcijas-datums/2016/11/04>
- Cabinet Regulation N°765 of 11 October 2005 “General Security Requirements for State Information Systems”. <https://likumi.lv/ta/id/118990/redakcijas-datums/2011/02/04>
- Cardash, S. L., Cilluffo, F. J., & Ottis, R. (2013). Estonia’s Cyber Defence League: A Model for the United States? *Studies in Conflict & Terrorism*, 36(9), 777–787. <https://doi.org/10.1080/1057610X.2013.813273>
- Collier, M., & Zablovskā, Z. (2013, 3 November). Is the case against ‘Neo’ a warning to Latvia’s whistleblowers? *Re: Baltica*. <https://en.rebaltica.lv/2013/11/is-the-case-against-neo-a-warning-to-latvias-whistleblowers/>
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). <https://data.europa.eu/eli/dir/2016/1148/oj>
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). <https://data.europa.eu/eli/dir/2022/2555/oj>
- Gnēze, A. (2016, 15 February). Ministry of Defence launches Military Computer Emergency Readiness Team. *Ministry of Defence of the Republic of Latvia*. <https://www.mod.gov.lv/lv/zinas/izveido-militaro-informacijas-tehnologiju-drosibas-incidentu-komandu>
- Goldstein, J. E., Neimark, B., Garvey, B., & Phelps, J. (2023). Unlocking “Lock-in” and Path Dependency: A Review Across Disciplines and Socio-Environmental Contexts. *World Development*, 161(2023), 106116. <https://doi.org/10.1016/j.worlddev.2022.106116>
- Hacker, J. S. (2002). *The divided welfare state: The battle over public and private social benefits in the United States*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511817298>
- Information Technology Security Law. (2010). <https://likumi.lv/ta/id/220962>
- Kāšķina, B. (2021, 1 February). 10. gadadienu atzīmē institūcija, kas ik dienu rūpējas par Latvijas kibertelpas drošību – “CERT.LV”. *Sargs.lv*. <https://www.sargs.lv/lv/latvija/2021-02-01/10-gadadienu-atzime-institucija-kas-ik-dienu-rupejas-par-latvijas-kibertelpas>

- Krasner, S. D. (1984). Approaches to the State: Alternative Conceptions and Historical Dynamics [On the Autonomy of the Democratic State, Eric Nordlinger; Negara: The Theatre State in Nineteenth Century Bali, Clifford Geertz; Building a New American State: The Expansion of National Administrative Capacities, Stephen Skowronek; The Formation of National States in Western Europe, Charles Tilly; Crises of Political Development in Europe and the United States, Raymond Grew; Revolution from Above: Military Bureaucrats and Development in Japan, Turkey, Egypt, and Peru, Ellen Kay Trimberger]. *Comparative Politics*, 16(2), 223–246. <https://doi.org/10.2307/421608>
- LETA. (2013, 20 August). Nacionālās IT drošības padomi plāno nodot AM pārziņā. *TVNET*. <https://www.tvnet.lv/5329129/nacionalas-it-drosibas-padomi-plano-nodot-am-parzina>
- LETA. (2023, 26 April). “Cert.lv”: Pērn ES kibertelpā visvairāk uzbrukts Polijai un Latvijai. *Sargs.lv*. <https://www.sargs.lv/lv/latvija/2023-04-26/certlv-pern-es-kibertelpa-visvairak-uzbrukts-polijai-un-latvijai>
- Mahoney, J. (2000). Path Dependence in Historical Sociology. *Theory and Society*, 29(4), 507–548. <https://www.jstor.org/stable/3108585>
- Ministry of Defence. (2013). National Armed Forces Cyber Defence Unit (CDU) concept. https://www.zs.mil.lv/sites/zs/files/document/cyberzs_April_2013_EN_final.pdf
- Ministry of Defence. (2019). National Cybersecurity Strategy of Latvia 2019–2022. <https://likumi.lv/ta/id/342302>
- Ministry of Defence. (2022). On Improving National Cybersecurity Governance (Report). https://tapportals.mk.gov.lv/legal_acts/3496512f-0307-4e7a-9951-579b79cc3eb2#
- Ministry of Environmental Protection and Regional Development. (2015). On the Competent and Responsible Authority That Will Ensure the Supervision of Qualified and High Security Qualified Electronic Identification Service Providers (Report).
- Ministry of Transport. (2011). On Preventing Information Technology Security Incidents (Press Release). *Latvijas Vēstnesis*. <https://www.vestnesis.lv/ta/id/225230>
- National Cybersecurity Law. (2024). <https://likumi.lv/ta/id/353390>
- National Security Law. (2000). <https://likumi.lv/ta/id/14011>
- North, D. C. (1991). Institutions. *Journal of Economic Perspectives*, 5(1), 97–112. <https://doi.org/10.1257/jep.5.1.97>
- Page, S. E. (2006). Path Dependence. *Quarterly Journal of Political Science*, 1(1), 87–115. <https://doi.org/10.1561/100.00000006>
- Pedersen, D. B. (2023). An evaluation framework for institutional capacity of science-for-policy ecosystems in EU Member States. Krieger, K. & Melchor, L. (Eds.). *Developing an evaluation framework for science-for-policy ecosystems*. Publications Office of the European Union. <https://doi.org/10.2760/609597>
- Petrāne, L. (2012, 7 December). Ministru kabinetā simulē IT traģēdiju. *Dienas Bizness*. <https://www.db.lv/zinas/ministru-kabineta-simule-it-tragediju-384027>
- Pierson, P. (2000). Increasing Returns, Path Dependence, and the Study of Politics. *American Political Science Review*, 94(2), 251–267. <https://doi.org/10.2307/2586011>
- Prime Minister. (2024). *On National Cybersecurity Council* (Executive Order). (2024/1.2.1.-416). *Latvijas Vēstnesis*. <https://likumi.lv/ta/id/357025>
- Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. K. M. N. (2020). Toward a Sustainable Cybersecurity Ecosystem. *Computers*, 9(3), 74. <https://doi.org/10.3390/computers9030074>
- Saeima. (2024, 20 June). New law significantly strengthens cybersecurity in Latvia (Press Release). [https://www.saeima.lv/en/news/saeima-news/33693-new-LAW-significantly-strengthens-cybersecurity-in-latvia?phrase=cybersecurity](https://www.saeima.lv/en/news/saeima-news/33693-new-law-significantly-strengthens-cybersecurity-in-latvia?phrase=cybersecurity)

- Skutelis, K. (2024, 30 September). Intervija: Kāda ir CERT.LV kiberdrošības vienības vēsture un kā tā palīdz aizsargāt Latviju no kiberuzbrukumiem. *Kursors.lv*. <https://kursors.lv/2024/09/30/intervija-kada-ir-cert-lv-kiberdrosibas-vienibas-vesture-un-ka-ta-palidz-aizsargat-latviju-no-kiberuzbrukumiem/>
- Ulmer, K. (2021). *Cyber risks and cybersecurity: risk communication and regulation strategies in the United States and Germany* (PhD Thesis). University of Stuttgart. <https://doi.org/10.18419/opus-11444>
- VDD. (2020, 20 March). VDD: pērn Latviju apdraudēja Krievijā bāzētas hakeru grupas. *Sargs.lv*. <https://www.sargs.lv/lv/latvija/2020-03-20/vdd-pern-latviju-apdraudeja-krievija-bazetas-hakeru-grupas>
- Vergne, J. P., & Durand, R. (2010). The Missing Link between the Theory and Empirics of Path Dependence: Conceptual Clarification, Testability Issue, and Methodological Implications. *Journal of Management Studies*, 47(4), 736–759. <https://doi.org/10.1111/j.1467-6486.2009.00913.x>

4 Evaluating National CSIRT Maturity

The Case of CERT.LV

*Mihails Potapovs, Kristiāns Teters,
Jānis Frīdmanis and Bernhards Blumbergs*

Introduction

Cybersecurity has become a critical component of national security, economic stability, and societal resilience. As states, businesses, and individuals increasingly rely on digital infrastructure, the ability to detect, prevent, and respond to cyber incidents is essential. Computer Security Incident Response Teams (CSIRTs) play a crucial role in safeguarding cyberspace by managing cyber threats, coordinating responses to incidents, and facilitating collaboration between public and private sector stakeholders. CERT.LV, Latvia's national and governmental CSIRT, has played a central role in the country's cybersecurity ecosystem since its establishment.

CERT.LV was formally created in 2011 following the enactment of the Information Technology Security Law (2010). However, its origins can be traced back to earlier efforts to develop cybersecurity capabilities in the mid-2000s. Initially, operating within the academic sector as CERT NIC.LV and LATNET CERT, the team transitioned into a national-level CSIRT under the supervision of the Ministry of Transport, and later the Ministry of Defence. Over the years, CERT.LV has expanded its scope, integrating new technologies and practices to strengthen Latvia's cyber resilience.

The importance of effective cyber incident response has been further underscored by geopolitical developments, particularly the sharp increase in cyber threats following Russia's full-scale war of aggression against Ukraine. Since February 2022, Latvia—along with other Baltic and European nations—has witnessed a surge in cyber incidents. CERT.LV has played a central role in defending against these threats, working closely with government agencies, private sector partners, and international allies to mitigate risks and coordinate responses.

As Latvia strengthens its cybersecurity posture, evaluating the national CSIRT's maturity becomes increasingly important. This chapter examines CERT.LV's maturity utilising the Security Incident Management Maturity Model (SIM3). By comparing its current state with a previous evaluation conducted in 2015, this case study provides insight into how CERT.LV has evolved over the past decade, identifying key advancements, ongoing challenges, and areas for future development.

The Role of National CSIRTs in Cybersecurity Governance

Understanding CSIRTs: Definition and Core Functions

CSIRTs are specialised entities responsible for detecting, analysing, responding to, and preventing cybersecurity incidents. Their primary goal is to minimise damage, reduce recovery time, and enhance overall security resilience. The concept of CSIRTs or Computer Emergency Response Teams (CERTs) originated in the late 1980s following the Morris Worm incident, one of the first widely recognised cybersecurity breaches that highlighted the need for coordinated incident response mechanisms (Spafford, 1989). Since then, CSIRTs have evolved into a global network of entities that specialise in responding to cyber incidents, fostering national and international cooperation, and developing proactive cybersecurity strategies.

Since then, CSIRTs have become fundamental components of cybersecurity strategies worldwide, operating within governments, corporations, academia, and international organisations (Killcrece et al., 2003). The key functions of CSIRTs can be categorised into “proactive and reactive services, as well as security quality management functions” (Skierka et al., 2015). Reactive functions involve direct responses to cyber incidents, such as malware outbreaks, data breaches, and denial-of-service attacks. These functions include incident detection, forensic investigation, containment, mitigation, and recovery efforts (Killcrece et al., 2003). Proactive functions focus on minimising the risk of cyber incidents through security audits, vulnerability assessments, penetration testing, and security awareness training (Wiik et al., 2006). Over the past three decades, the operational scope of CSIRTs has expanded beyond incident containment to include threat intelligence sharing, cybersecurity capacity building, and policy advisory functions (West-Brown et al., 2003).

The operational scope of CSIRTs varies depending on their constituency, which may include government agencies, critical infrastructure operators, businesses, or academic institutions. While some CSIRTs function exclusively within an organisation, others collaborate across sectors and national borders to share cyber threat intelligence and coordinate responses to large-scale cyber incidents (Killcrece et al., 2003; Novak et al., 2021). The emergence of national CSIRTs has been a fundamental response to the growing complexity of cyber threats in an increasingly interconnected world. As digital infrastructures underpin critical sectors, including energy, finance, healthcare, and public administration, safeguarding these systems against cyber incidents has become a strategic priority.

National CSIRTs play a pivotal role in this landscape, serving as the primary entities responsible for incident detection, response coordination, and cyber threat mitigation at the national level (Haller et al., 2011; Newmeyer, 2015; West-Brown et al., 2003). According to the latest data¹ from the International Telecommunication Union (ITU), there are currently 139 national CSIRTs (ITU, 2025). In comparison, the Forum of Incident Response and Security Teams (FIRST) lists 773 CSIRTs across various levels and sectors, including national teams, spanning 111 countries worldwide (FIRST, 2025). Meanwhile, the European Union Agency for

Cybersecurity (ENISA) identifies 758 CSIRTs across Europe, with 583 operating within EU member states (ENISA, 2024).

Organisational Models of National CSIRTs

The structural composition of national CSIRTs varies significantly across jurisdictions, reflecting differences in governmental priorities, institutional capacities, and legal frameworks. The organisational structure of a national CSIRT within governmental frameworks remains an open question, encompassing considerations related to its placement, funding, and staffing. Most national CSIRTs operate under ministries, information security agencies, or telecommunications authorities; others function as part of a National Cyber Security Centre (NCSC) or as independent entities. Broadly, national CSIRTs can be categorised into three primary models: government-led, independent, and hybrid CSIRTs.

- **Government-led CSIRTs** operate within the state apparatus, often as divisions of national security agencies, ministries of defence or digital affairs, or telecommunications regulatory authorities. These CSIRTs prioritise the protection of government networks, classified information, and critical national infrastructure, functioning as the technical arm of national cybersecurity strategy implementation. Their authority may allow them to enforce mandatory cybersecurity standards, issue regulatory directives, and coordinate national cyber crisis response efforts.
- **Independent CSIRTs** function autonomously, either as non-profit organisations, academic institutions, or industry consortia. While they may receive government funding, their operational independence allows them to serve a broader constituency, including businesses and civil society organisations. Independent CSIRTs often focus on technical research, security consultancy, and public-private cooperation in cyber incident management.
- **Hybrid CSIRTs** combine elements of both government-led and independent models, operating as public-private partnerships. This structure is particularly effective in nations where private sector entities manage significant portions of critical infrastructure. Hybrid CSIRTs facilitate collaborative threat intelligence sharing while benefiting from the regulatory oversight of governmental institutions.

Morgus et al. (2015) contend that to maximise their effectiveness, national CSIRTs should maintain operational independence while retaining access to policymakers and senior government officials. Positioned between government and the private sector, they should serve as coordinators for incident response and as central hubs for information exchange. While collaboration with intelligence and law enforcement agencies has become increasingly common, Morgus et al. (2015) stress the importance of establishing clear boundaries to prevent conflicts of interest. To safeguard trust and maintain operational efficiency, national CSIRTs should neither be integrated into nor directly subordinate to these agencies. In particular, excessive proximity to

intelligence services could erode public confidence in a national CSIRT and limit its operational effectiveness. Moreover, any involvement of law enforcement or intelligence agencies in incident response should be strictly limited to well-defined legal mandates that adhere to principles of responsible handling of personally identifiable information, including purpose specification, use limitation, and data minimisation.

National CSIRTs in the European Union

While national CSIRTs operate globally, the European Union has distinct regulatory requirements governing their establishment and operation. Notably, EU legislation mandates that member states establish national CSIRTs. The Directive 2016/1148, widely known as the Networks and Information Systems Security Directive (NIS Directive), required each member state to designate one or more CSIRTs, ensuring compliance with requirements on the availability of communications, security of premises, business continuity, and participation in international cooperation networks. Member states were also responsible for providing adequate resources to enable their CSIRTs to fulfil their mandates effectively.

Annex I of the NIS Directive outlined the core responsibilities of CSIRTs, which included: (1) monitoring cybersecurity incidents at the national level, (2) providing early warnings, alerts, announcements, and disseminating relevant information to stakeholders regarding risks and incidents, (3) responding to incidents, (4) conducting dynamic risk and incident analysis to enhance situational awareness, and (5) participating in the CSIRTs network. Furthermore, CSIRTs were required to establish cooperative relationships with the private sector and promote the adoption of standardised practices for incident and risk-handling procedures, as well as for incident, risk, and information classification schemes.

To foster trust and facilitate efficient operational collaboration among national CSIRTs, the NIS Directive also established the CSIRTs network. The revised NIS2 Directive (2022/2555) retained and reinforced these regulatory requirements while expanding CSIRT obligations. Notably, NIS2 introduced additional responsibilities, such as peer reviews and the management of coordinated vulnerability disclosure processes (see Box 4.1).

Box 4.1 Article 11(3) of the NIS Directive—Tasks of CSIRTs

3. The CSIRTs Shall have the Following Tasks:

- a monitoring and analysing cyber threats, vulnerabilities, and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;
- b providing early warnings, alerts, announcements, and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities, and incidents, if possible in near real time;

- c responding to incidents and providing assistance to the essential and important entities concerned, where applicable;
- d collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;
- e providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;
- f participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;
- g where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);
- h contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).

The CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of the entities' services.

When carrying out the tasks referred to in the first subparagraph, the CSIRTs may prioritise particular tasks on the basis of a risk-based approach.

Methods and Approach

The study employs a case study approach to evaluate the maturity of CERT.LV's cyber incident response capabilities. The evaluation is based on the SIM3 v2 interim standard developed by Stikvoort et al. (2023), which provides a structured methodology for measuring the operational effectiveness of a CSIRT. The evaluation considers 45 parameters across four core quadrants:

- **O—Organisation** (governance, authority, and mandate)
- **H—Human** (staffing, training, and resilience)
- **T—Tools** (technical infrastructure and resources)
- **P—Processes** (incident response workflows and best practices)

The maturity level for each parameter is assessed on a five-point scale ranging from 0 to 4, reflecting the extent to which it is defined, documented, and formally implemented within CSIRT's operations. The levels are structured as follows (Stikvoort et al., 2023):

- **0** = not available/undefined/unaware,
- **1** = implicit (known/considered but not written down, "between the ears"),
- **2** = explicit, internal (written down but not formalised in any way),

- 3 = explicit, formalised on authority of the CSIRT head or above (rubberstamped or published), and
- 4 = explicit, audited on authority of governance levels above the CSIRT head (subject to control process/audit/enforcement).

This study adopts a practitioner-centric approach, leveraging a documentary analysis of publicly available materials, regulatory frameworks, and operational reports, supplemented by the personal experience of the co-authors. The research integrates comparative analysis by cross-referencing CERT.LV's current maturity level with a previous evaluation (ENISA, 2015). This allows to evaluate progress over time and identifies areas where CERT.LV has evolved or faces persistent challenges.

While this study provides a structured and comprehensive evaluation of CERT.LV's cyber incident response maturity, several limitations must be acknowledged. First, certain operational details of CERT.LV's incident response framework may be classified or otherwise restricted from public disclosure. As a result, some elements of the evaluation are based on indirect evidence, such as regulatory compliance, policy documents, and reports from international cybersecurity bodies (notably ENISA), complemented by first-hand testimonies of the co-authors. This means that while the evaluation provides a strong indication of CERT.LV's maturity, it does not necessarily account for all nuances of its internal procedures and decision-making processes.

Second, the evaluation relies on the SIM3 v2 as the primary evaluation framework. While SIM3 v2 is widely recognised and used for evaluating CSIRT capabilities, alternative evaluation models, such as the three-tier approach used by ENISA (2019) or the combined Global CSIRT Maturity Framework (Duijnhoven et al., 2019), may offer additional perspectives on certain maturity aspects. Furthermore, the comparative analysis in this study references an earlier evaluation of CERT.LV's maturity (ENISA, 2015), which used the SIM3 v1 parameters (Stikvoort, 2015). Given that SIM3 v2 introduces refinements and expanded criteria compared to its predecessor, direct comparisons between the two evaluations must be approached with caution. Although broad trends and improvements can be identified, differences in methodology may influence specific parameter ratings. Despite these limitations, the study provides a valuable insight into CERT.LV's cyber incident response maturity, offering a structured evaluation that highlights progress over time while identifying areas for further development.

CERT.LV Maturity Case Study

Quadrant 1: Organisation

O-1 Mandate. The mandate of CERT.LV originates from the highest governance levels and is enshrined in the National Cybersecurity Law (2024). As part of the NCSC-LV, CERT.LV operates under the supervision of the Ministry of Defence of the Republic of Latvia. Each year, the Ministry of Defence concludes a delegation agreement, formally designating CERT.LV to perform national CSIRT functions.

Supervision is conducted through a review process involving quarterly and annual reports submitted by the Head of CERT.LV to the Ministry of Defence. Additionally, as a public body, CERT.LV is subject to audits by the State Audit Office (*Valsts kontrole*) of the Republic of Latvia.

O-2 Constituency. The National Cybersecurity Law (2024) defines the constituency of CERT.LV, which comprises essential and important service providers as specified in the NIS2 Directive (2022/2555), critical ICT infrastructure operators, as well as all public and private ICT infrastructure in Latvia. However, entities in the defence sector fall under the jurisdiction of MilCERT, the Military CSIRT. Beyond its designated constituency, CERT.LV also extends its services to the general public, offering cybersecurity support to all natural and legal persons in Latvia.

O-3 Authority. The authority of CERT.LV is outlined in the National Cybersecurity Law (2024). Section 11 establishes the rights of the two national-level CSIRTs, CERT.LV and MilCERT. Additionally, as part of the NCSC-LV, CERT.LV also falls under Section 6, which defines the rights and responsibilities of the NCSC-LV.

O-4 Responsibility. CERT.LV's responsibilities are defined in the National Cybersecurity Law (2024). Section 10 delineates the responsibilities of CERT.LV and MilCERT, while Section 5 defines the responsibilities of the NCSC-LV, of which CERT.LV is a part. The law explicitly states that CERT.LV is responsible for fulfilling NCSC-LV's duties outlined in Section 10(1), paragraphs 17 to 23.

O-5 Service Description. The service description of CERT.LV is specified in the delegation agreements between the Ministry of Defence and CERT.LV, which are signed annually and reviewed in accordance with established procedures. The legal basis for these delegation agreements is set out in Section 5(3) of the National Cybersecurity Law (2024). CERT.LV also has an official RFC2350 document which is based on RFC2350—*Expectations for Computer Security Incident Response*—document benchmark, widely used by CSIRT teams across the EU (Brownlee & Guttman, 1998).

O-6 Public Media Policy. While CERT.LV actively engages with public media and maintains a strong public presence, it has also established internal policies and procedures for media interactions. A dedicated Public Relations Team serves as the primary point of contact for media inquiries, ensuring that official positions are coordinated and communicated effectively. This is often done in close collaboration with the Military-Public Relations Department of the Ministry of Defence. However, despite being implemented in practice, this media policy remains undocumented.

O-7 Service-Level Description. Due to the broad scope of its constituency, CERT.LV is authorised to manage or assist in managing any type of cyber incident. General service level is described in the CERT.LV's RFC2350 document, however the level of CERT.LV's support varies depending on the nature of the incident, the type of constituent affected, the number of impacted users, and the potential for further damage. Generally, an initial response is provided within one working day. However, due to financial and personnel constraints, CERT.LV does not currently

operate a 24/7 incident response service. That said, round-the-clock operations can be activated if necessary, particularly in the event of major cyber incidents or national crises. The service-level description is documented in internal CERT.LV procedures and approved by the Head of CERT.LV.

O-8 Incident Classification. Since 2017, CERT.LV has used a cyber incident taxonomy based on the eCSIRT.net model, which is fully aligned with international standards. This taxonomy is formally documented in internal CERT.LV documents, approved by the Head of CERT.LV. Additionally, the taxonomy has been incorporated into the draft Cabinet Regulation on Baseline Cybersecurity Requirements, a secondary legislative act currently under negotiation, which implements the technical provisions of the NIS2 Directive (2022/2555). Once finalised, the incident classification taxonomy will be enshrined in national law. Internally, CERT.LV utilises a cyber incident classification matrix based on the model developed by the NCSC of the United Kingdom (National Cyber Security Centre, 2023). This matrix assesses cyber incidents by cross-referencing their impact with the importance of the affected entity, allowing for a categorisation of significance ranging from C6 (lowest) to C1 (highest) (Table 4.1). An example of the matrix's application, illustrating the distribution of compromised IP addresses from incidents identified in 2024, is provided in Figure 4.1.

O-9 Participation in CSIRT Systems. CERT.LV has actively participated in international CSIRT communities since its early years. Even before its formal establishment, it became a full member of FIRST in 2009 and achieved Trusted Introducer accreditation in 2008. In 2016, CERT.LV advanced to Trusted Introducer certification status, which requires renewal every three years. CERT.LV successfully recertified in 2019 and 2022, with the next recertification scheduled for 2025. CERT.LV also represents Latvia in the EU CSIRTs Network, which was established under the NIS Directive (2016/1148). Within this network, CERT.LV actively participates in working groups focused on cybersecurity maturity, situational awareness, and other critical topics.

O-10 Organisational Framework. The National Cybersecurity Law (2024) provides a general description of CERT.LV's role within Latvia's cybersecurity governance ecosystem. Additionally, as a Trusted Introducer-certified team, CERT.LV maintains an RFC 2,350 document, which details its organisational structure and operational framework. Furthermore, CERT.LV has an internal handbook, serving as the primary reference document for its organisational framework, operational procedures, and best practices. This handbook is also used extensively for training new personnel.

O-11 Security Policy. CERT.LV has adopted a security policy based on the ISO 27001:2022 framework, incorporating national legislative requirements. As a laboratory within the Institute of Mathematics and Computer Science at the University of Latvia, CERT.LV is required to comply with the rules applicable to public institutions, which themselves fall under the NIS2 Directive (2022/2555) and the National Cybersecurity Law (2024) as essential entities. CERT.LV's compliance with baseline cybersecurity requirements is supervised by an independent public authority.

Table 4.1 Classification of cyber incidents by severity. Adapted by CERT.LV from the UK’s National Cyber Security Centre (2023)

| <i>Category</i> | <i>Description</i> |
|-----------------|---|
| C1 | national-level threat, affected provision of basic services, threatened public administration and economic or political stability |
| C2 | threats of high importance, affected state institutions, national IT infrastructure |
| C3 | significant threats, wide affect the commercial sector, state and local government institutions |
| C4 | significant threats, medium impact on the commercial sector, state and local government institutions |
| C5 | moderate threats, minor affect the commercial sector, state, and local government institutions |
| C6 | daily threats, affecting individual recipients of IT services, insignificant impact on companies or state and local government institutions |

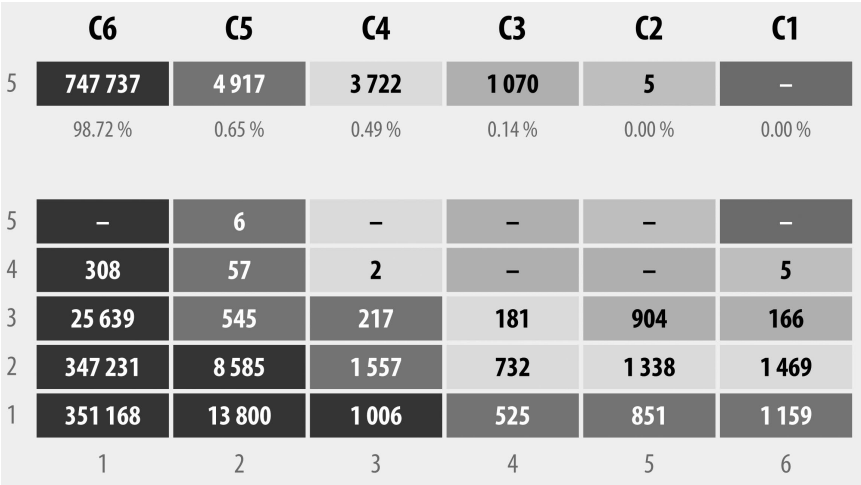


Figure 4.1 Distribution of compromised IP addresses from incidents identified by CERT.LV in 2024 (CERT.LV, 2025).

Quadrant 2: Human

H-1 Code of Conduct/Practice/Ethics. CERT.LV has established its own code of conduct and ethics, which incorporates requirements from the Trusted Introducer’s CSIRT Code of Practice as well as the ethical guidelines of the Ministry of Defence. The document outlines legal obligations, including compliance with foreign legislation in the event of cross-border cyber incidents. It also sets clear rules for responsible handling of sensitive information, ensuring conflict-of-interest avoidance, and maintaining professional and respectful behaviour in all professional interactions.

H-2 Staff Resilience. As part of Latvia's ongoing cybersecurity governance modernisation, detailed in the previous chapter of this book, CERT.LV has undergone significant personnel expansion. Five new operational units have been established to enhance its capabilities:

- 1 Governance and Compliance Group
- 2 Cybersecurity Testing Group (Red Team)
- 3 Threat Hunting Operations Group
- 4 Network and Infrastructure Group
- 5 Security Operations Centre (SOC)

To support staff resilience, CERT.LV has implemented remote working procedures, ensuring operational continuity in various scenarios. Furthermore, legal provisions now enable CERT.LV to receive assistance from the Cyber Defence and Electromagnetic Warfare Battalion of the National Guard in the event of a major cyber incident or crisis. This interoperability between CERT.LV and the National Guard is regularly tested in joint cybersecurity exercises, including the NATO CCDCOE Locked Shields exercise (CERT.LV, 2024b).

H-3 Skillset Description. Each CERT.LV position has a defined job description, which is formally included in employment contracts. The full list of positions is approved in collaboration with the Ministry of Defence, and every new role must have a detailed skillset requirement. Key skillsets within CERT.LV include incident handling, malware analysis, programming, IT project management, IT auditing, and systems analysis, among others. When hiring, CERT.LV assesses the existing team's capabilities, matches them against organisational needs, and recruits candidates with complementary expertise based on job market availability.

H-4 Staff Development. New CERT.LV employees undergo a structured onboarding process, which includes familiarisation with key CERT.LV tools (e.g., RTIR, internal customer database), introduction to the organisational structure and team operations, as well as briefings on information classification and sharing, security procedures, and code of ethics. Certain aspects of this training are conducted by the Institute of Mathematics and Computer Science and the Ministry of Defence. In addition to formal mentorship programmes, CERT.LV offers a range of educational activities open to all employees. Where possible, external training participants share their acquired knowledge internally. The organisation also promotes informal training sessions, such as internal presentations, knowledge-sharing forums, and "Insecurity Day" activities. The CERT.LV Handbook, alongside the RFC 2350 document, serves as a comprehensive reference for internal training, ensuring both process standardisation and operational knowledge retention.

H-5 Technical Training. All new team members are required to complete mandatory technical training, including TRANSITS I course (covering CSIRT fundamentals), as well as information security training provided by the Ministry of Defence. Participation in external training programmes is tailored to individual needs and subject to available resources. CERT.LV allocates an annual budget for external training, considering employee profiles and organisational priorities.

Team members regularly attend ENISA and NATO CCDCOE training sessions, TRANSITS II courses, and, where possible, international cybersecurity exercises. Several CERT.LV professionals hold industry-recognised certifications, such as Certified Ethical Hacker and Certified Information Systems Auditor.

H-6 Soft Skills Training. Currently, CERT.LV does not have a dedicated communication training programme; however, plans are in place to implement one. Some team members have already participated in communication training as part of exercises and TRANSITS II courses. Members of the Public Relations Team possess extensive media-handling experience, including public communication, media relations, and information dissemination. Additionally, senior CERT.LV staff members frequently participate in radio and television interviews, having developed their media engagement skills through experience and cybersecurity exercises.

H-7 External Networking. CERT.LV actively engages in international CSIRT cooperation, participating in TF-CSIRT, Trusted Introducer, and FIRST events, as well as representing Latvia in the EU CSIRTs network. These responsibilities are formalised in the annual delegation agreement with the Ministry of Defence. CERT.LV also takes part in a broad range of international networking activities, including cybersecurity forums, conferences, and policy initiatives. Notably, it contributes to EU-wide cybersecurity policymaking through involvement in the European Cybersecurity Certification Group. CERT.LV also establishes bilateral partnerships and negotiates Memorandums of Understanding (MoUs) on a case-by-case basis. These agreements facilitate collaboration with foreign CSIRTs, private-sector cybersecurity firms, as well as security researchers, vendors, and service providers.

Quadrant 3: Tools

T-1 IT Assets and Configurations. As a national CSIRT, it would be impractical for CERT.LV to maintain a comprehensive inventory of all IT assets and configurations used by its entire constituency. Instead, a two-tiered governance model is in place, where NIS2 essential and important entities are legally required to identify their own assets and maintain an internal catalogue of ICT assets and information systems. As part of its supervisory role within NCSC-LV, CERT.LV has the authority to request access to these catalogues when necessary. Although this process is not yet fully implemented, it is enshrined in the draft Cabinet Regulation on Baseline Cybersecurity Requirements, which is currently under negotiation and scheduled for adoption in 2025. In addition to this broader governance approach, CERT.LV maintains detailed information on high-priority institutions, particularly concerning online resources and content management systems (CMS) in use. This data is stored in CERT.LV's user database, which allows filtering institutions by specific CMS platforms, facilitating targeted cybersecurity advisories.

T-2 Information Sources List. CERT.LV maintains an integrated list of information sources, which is linked to its customer management system. Threat intelligence feeds from these sources are automatically processed and distributed to constituents daily. Additionally, CERT.LV publishes updates on the latest vulnerabilities and malware daily on its website. For threat intelligence and analysis,

CERT.LV relies on both automatic and manually curated sources, including MISP, *Shadowserver*, and other intelligence platforms. Several of these sources are also utilised to develop cyber awareness materials.

T-3 Consolidated Messaging System(s). CERT.LV has established a national contact point where all messages sent to its central email address are automatically logged in the Request Tracker for Incident Response (RTIR) system. All responses are sent and archived within RTIR, ensuring a fully traceable communication process. All CERT.LV employees have access to this system for incident management purposes. Additional email lists are maintained for specific operational tasks (e.g., event registration and constituency contact lists), though these are accessible only to relevant team members. Unlike RTIR, these email lists are not centrally archived, but their usage is documented in the CERT.LV Handbook.

T-4 Incident Tracking System. CERT.LV makes full use of RTIR to track and manage cyber incidents. Internal documentation provides detailed guidance on RTIR usage, outlining the incident lifecycle, including when to log incidents, generate reports, and escalate cases. CERT.LV also employs an in-house developer to implement custom modifications and ensure system adaptability as operational needs evolve.

T-5 Resilient Voice Calls. CERT.LV relies on landline phones as its primary voice communication method, with contractual requirements set for reliability with its service provider. As a fallback mechanism, mobile phones with encryption capabilities are available to all employees. Additionally, CERT.LV utilises alternative communication platforms, including *Webex*, *Mattermost*, and *Signal*, to ensure resilient and secure communication.

T-6 Resilient Messaging. CERT.LV's email services are provided by the Sigmanet Laboratory of the Institute of Mathematics and Computer Science of the University of Latvia and maintained by CERT.LV team members. There is a Service-Level Agreement with Sigmanet. A robust set of security features, including encryption, is implemented to protect email communications from unauthorised access and interception.

T-7 Resilient Internet Access. CERT.LV has multiple redundant internet connections provided by different Latvian and foreign internet service providers. Additionally, redundant physical connections ensure continued internet availability. CERT.LV also has direct access to Latvia's national crisis network, providing a backup communication channel in case of major disruptions. To further enhance network resilience, CERT.LV's internet traffic is routed through the Government Internet Exchange Point (GLV-IX), which is supervised by the Ministry of Defence. This configuration ensures that domestic internet traffic remains functional even in cases of global internet disruptions.

T-8 Incident Prevention Toolset. While CERT.LV primarily serves a coordinating function as a national CSIRT, it also performs certain proactive cybersecurity measures as a governmental CSIRT. Among CERT.LV's preventive services, its SOC and DNS RPZ (DNS firewall) services play a crucial role. The DNS firewall leverages data from early warning sensors, enabling real-time threat mitigation by blocking malicious domains before they can impact users. Since its introduction,

the DNS firewall service has evolved significantly and is now accessible via mobile applications, making it available to the general public (CERT.LV, 2024a). Other preventive tools include:

- Spam traps and honeypots for cyber threat analysis.
- Direct intelligence-sharing arrangements with select institutions.
- Penetration testing and security audits for designated constituents, as permitted under CERT.LV's legal mandate.

T-9 Incident Detection Toolset. CERT.LV leverages external sources to obtain intelligence on cyber threats and provide targeted warnings to its constituents. Under the National Cybersecurity Law (2024), CERT.LV is authorised to collect network traffic data from constituents based on mutual agreements. This provision has enabled the deployment of early warning sensors within the constituency, which feed anomalous pattern recognition and indicator of compromise detection capabilities. These sensors operate under formal cooperation agreements, where the constituent defines the scope of monitored network flows. The collected data is aggregated and correlated centrally within CERT.LV infrastructure, allowing CERT.LV to notify affected constituents with detailed threat intelligence. The depth of information in these alerts depends on the extent of network traffic provided by the constituent. For more comprehensive, continuous monitoring, CERT.LV offers a SOC service that extends visibility into global and regional threats while enabling automated threat mitigation. Both early warning sensors and the SOC service are regulated under the National Cybersecurity Law (2024).

T-10 Incident Resolution Toolset. Over years of operation, CERT.LV has built an extensive incident resolution toolset, comprising open-source, in-house-developed, and externally acquired tools. Given its academic origins, CERT.LV maintains strong connections with the scientific community, enabling collaboration on the development and testing of experimental cybersecurity tools. All tools used for incident resolution are well-documented in internal CERT.LV procedures, ensuring a structured approach to threat mitigation and response.

Quadrant 4: Processes

P-1 Escalation to Governance Level. As CERT.LV operates under the supervision of the Ministry of Defence, which is responsible for national cybersecurity and defence in Latvia, formal escalation procedures are in place. The National Cybersecurity Law (2024) and the delegation agreement between CERT.LV and the Ministry of Defence outline protocols for information exchange. Additionally, a classified national cyber crisis management plan defines the roles and responsibilities of relevant institutions in the event of a major cyber incident or crisis. This classified plan is fully integrated with Latvia's national defence strategy, ensuring that, if activated, it enables escalation to the highest governance levels when necessary.

P-2 Escalation to Press Function. The information flow between CERT.LV and the Ministry of Defence is regulated by the National Cybersecurity Law and the delegation agreement. CERT.LV has the mandate to inform the public or require affected constituents to do so when it determines that public disclosure of a cyber incident is in the public interest. In cases involving specific incidents, messages are coordinated with the affected institution before being made public. Public communication about major cyber incidents is carried out in close coordination with the Military-Public Relations Department of the Ministry of Defence. CERT.LV has also established direct contacts with major media outlets to ensure efficient dissemination of cybersecurity information.

P-3 Escalation to Legal Function. The legal escalation process for CERT.LV is outlined in the delegation agreement with the Ministry of Defence. This includes a requirement for CERT.LV to submit all international agreements and MoUs for approval. CERT.LV has in-house legal expertise, and its legal expert actively participates in both domestic and international cybersecurity exercises, including NATO CCDCOE's Locked Shields. A Cabinet-level instruction on cyber incident attribution is currently being drafted by the Ministry of Foreign Affairs. This new regulation will define CERT.LV's role and responsibilities in the cyber attribution process.

P-4 Incident Prevention Process. CERT.LV employs a range of incident prevention measures, as outlined in parameter T-8. Its primary focus is on raising cybersecurity awareness, issuing advisories, and providing targeted warnings to constituents. Additionally, CERT.LV implements direct incident prevention initiatives for specific groups, including cyber threat intelligence sharing and penetration testing. The incident prevention process is documented in the CERT.LV Handbook and maintained in an internal wiki accessible to CERT.LV employees.

P-5 Incident Detection Process. CERT.LV uses a combination of early warning sensors deployed in constituents' networks, its SOC service, and automated analysis of external threat intelligence sources (see parameter T-9). The procedures for incident detection are fully documented in the CERT.LV Handbook and internal wiki, ensuring all employees have clear guidance on incident detection processes.

P-6 Incident Resolution Process. CERT.LV follows a comprehensive incident resolution framework, supported by the tools and methodologies outlined in parameter T-10. The entire lifecycle of a cyber incident is covered in internal documentation, ensuring a structured and effective response. This incident resolution process is fully documented in the CERT.LV Handbook and internal wiki and is accessible to all responsible employees.

P-7 Specific Incident Processes. CERT.LV does not maintain separate workflows for different categories of cyber incidents. Instead, its incident resolution process is designed to handle all types of incidents while taking into account the incident's priority level and severity.

P-8 Audit and Feedback Process. CERT.LV adheres to strict reporting requirements for both tasks and financial expenditures. It is obligated to submit quarterly and annual reports to the Ministry of Defence, which are subject to formal review and written approval within a defined timeline. Non-compliance with these

reporting requirements can lead to disciplinary measures and, in extreme cases, termination of the delegation contract. CERT.LV also publishes public quarterly and annual reports to ensure transparency and public scrutiny. As a public institution, CERT.LV is subject to audits conducted by the State Audit Office of the Republic of Latvia, which reviews its financial management and operational effectiveness.

P-9 Emergency Reachability Process. CERT.LV maintains a 24/7 helpdesk in cooperation with the Institute of Mathematics and Computer Science of the University of Latvia. Helpdesk operators are trained in emergency protocols and instructed on how to contact the appropriate CERT.LV personnel outside of normal working hours. The contact information of CERT.LV leadership is available to upper-level management at the Ministry of Defence, law enforcement agencies, national security services, and other key stakeholders. For international emergency situations, CERT.LV maintains up-to-date contact records in the Trusted Introducer database, ensuring it can be reached promptly by international partners and CSIRTs.

P-10 Best Practice Internet Presence. CERT.LV maintains a dedicated website in both Latvian and English (*cert.lv*) and actively engages with the public through social media platforms, including *X* (formerly *Twitter*), *Facebook*, *YouTube*, *LinkedIn*, and *draugiem.lv*. Standard contact information for CERT.LV is available in its RFC 2350 document and on its official website. This includes email addresses formatted as *name.surname@cert.lv*, as well as public PGP keys for employees with public-facing roles. The primary email address for reporting incidents is *cert@cert.lv*, but CERT.LV also supports a range of dedicated aliases such as *abuse@cert.lv* and *spam@cert.lv* for specific cybersecurity concerns. Additional dedicated email addresses are available for purposes such as event registration and contact information updates. CERT.LV also manages a specialised cybersecurity awareness platform (*esidross.lv*) that provides guidance on secure ICT usage and fundamental cyber hygiene practices.

P-11 Secure Information Handling Process. CERT.LV follows strict regulations for handling sensitive information, in full compliance with national laws. All CERT.LV employees are legally required to obtain security clearance, having been vetted by national security authorities. Additionally, all employees undergo mandatory training on secure information handling. For secure communication with governmental institutions, CERT.LV employs a separate technical solution for sensitive information exchange. Procedures are also in place for handling national, EU, and NATO-classified information, which are reviewed in cooperation with the Ministry of Defence and national security authorities. For public-facing security measures, CERT.LV provides guidance on secure communication, including publishing PGP keys on its website. In addition to national classification protocols, CERT.LV utilises the Traffic Light Protocol for both national and international information exchange.

P-12 Information Sources Process. The CERT.LV Handbook contains internal procedures for the collection, processing, and usage of information sources. Additionally, CERT.LV maintains an up-to-date list of relevant information sources within its internal wiki.

P-13 Outreach Process. CERT.LV operates an extensive outreach programme to engage with both public and private sector stakeholders. At the national level, CERT.LV organises various cybersecurity seminars and training sessions. Key initiatives include the annual *CyberChess* conference, a leading cybersecurity event in the Baltics, as well as the *Esi drošs* (“Be Safe”) workshop series, held twice a year to provide hands-on training for ICT professionals. In cooperation with the Ministry of Defence, CERT.LV also conducts on-site and online workshops to update the public and private sectors on emerging cybersecurity threats, new legislation, regulatory changes, and best practices for compliance. CERT.LV has established a strong social media presence, and its leadership frequently comment on cybersecurity developments on national television. Additionally, CERT.LV runs public awareness campaigns, develops informational materials, and actively participates in policy discussions on cybersecurity regulations. The outreach process is fully documented in the CERT.LV Handbook and internal wiki, with key outreach activities also formalised in the delegation agreement between CERT.LV and the Ministry of Defence.

P-14 Governance Reporting Process. CERT.LV submits quarterly and annual reports to the Ministry of Defence (see parameter P-8). Based on these reports, CERT.LV also produces public versions of its quarterly and annual cybersecurity reports, which are made available online. The level of detail and classification differs between the public and internal reports, with reporting procedures clearly defined in the delegation agreement between CERT.LV and the Ministry of Defence.

P-15 Constituency Reporting Process. CERT.LV compiles monthly cyber incident statistics, following the cyber incident classification framework outlined earlier. These statistics are published on the CERT.LV website and included in its quarterly and annual reports, ensuring public accessibility to relevant cybersecurity data.

P-16 Meeting Process. CERT.LV holds monthly all-team meetings, where each team member presents key activities and upcoming plans. During these meetings, the event calendar is updated, and formal notes are recorded, with responsibility for note-taking rotating among team members. While internal unit meetings occur more frequently, they do not follow a strict schedule. However, the CERT.LV technical division hosts dedicated meetings to encourage technical discussions and knowledge sharing. Information exchange within CERT.LV is generally informal but follows the “need to know” principle to ensure operational security. CERT.LV also conducts weekly Situational Report (SITREP) meetings with representatives from the Cybersecurity Policy Department of the Ministry of Defence. These meetings cover major cybersecurity incidents in Latvia, situational developments in Latvian cyberspace, as well as key tasks and priorities for the week. Following these meetings, classified reports summarising key developments are submitted to senior leadership at the Ministry of Defence and other key stakeholders. The meeting process is documented in the CERT.LV Handbook.

P-17 Peer Collaboration Process. CERT.LV engages in broad collaboration with other CSIRTs and has signed MoUs with multiple international partners. CERT.LV also frequently participates in joint cybersecurity exercises with Baltic

and European CSIRTs. Latvia plays a leading role in NATO and EU cybersecurity operations, particularly in cyber threat hunting. Since 2022, CERT.LV has conducted joint threat-hunting operations in cooperation with the Cyber Command of the Canadian Armed Forces, the Canadian Centre for Cyber Security, the U.S. Cyber Command, as well as other allies. These threat-hunting operations, led by CERT.LV, focus on identifying cyber threats within Latvian critical infrastructure systems. The process involves onboarding selected information systems, conducting systematic threat-hunting operations to detect attackers, anomalous activities, and malicious behaviour, as well as identifying long-term attack patterns, which can reveal significant security vulnerabilities in endpoint software, hardware, and network infrastructure. These operations have played a critical role in strengthening Latvia's cybersecurity resilience and enhancing NATO and EU-wide threat intelligence efforts. In 2025, CERT.LV in cooperation with the Canadian Armed Forces Cyber Command published a "Threat Hunt Playbook" to further promote this valuable experience and expertise (Teivans & Smith, 2025).

Results and Discussion

Over the past decade, CERT.LV has undergone significant advancements in its cyber incident response maturity. The comparison between the 2015 evaluation and the current evaluation using the SIM3 v2 interim CSIRT maturity framework highlights major improvements across all four quadrants. The previous evaluation identified several areas requiring development, particularly in resource constraints, formalised processes, and incident detection capabilities (ENISA, 2015). This study demonstrates notable progress in these areas, with CERT.LV now operating within a more structured national cybersecurity framework and integrating best practices at both the national and EU levels.

Organisational Maturity: Strengthened Governance and Authority

In 2015, CERT.LV's mandate, authority, and responsibilities were legally established but lacked strategic alignment with national cybersecurity priorities (ENISA, 2015). The 2024 evaluation indicates a significant enhancement in governance mechanisms:

- CERT.LV's mandate is now enshrined in the National Cybersecurity Law (2024), providing a clear legal foundation for its activities and role as Latvia's national CSIRT.
- Annual delegation agreements between CERT.LV and the Ministry of Defence ensure continuity of operations and funding, addressing earlier concerns about resource stability.
- CERT.LV has been fully integrated into the NCSC-LV, ensuring better coordination with other national cybersecurity entities.
- Participation in EU-wide cyber cooperation mechanisms, such as the EU CSIRTs Network and ENISA's peer review processes, has expanded CERT.LV's international influence and operational reach.

Despite these advancements, challenges remain in terms of ensuring long-term sustainability of CERT.LV's expanded responsibilities. Given the increasing cyber threat landscape, further strategic investments in organisational growth and resilience are necessary.

Human Maturity: Workforce Expansion and Capability Development

A major limitation highlighted in the 2015 evaluation was insufficient staffing and expertise, particularly in incident response and threat intelligence analysis (ENISA, 2015). In response, CERT.LV has undergone significant workforce expansion and restructuring:

- Staff size has doubled, allowing for the creation of specialised units/subteams.
- A structured onboarding and training programme has been introduced, incorporating mandatory courses such as TRANSITS I and ENISA-led cybersecurity workshops.
- CERT.LV has developed stronger collaborations with international cyber defence entities, including NATO CCDCOE and allied military cyber commands, facilitating knowledge exchange and joint training initiatives.
- The introduction of remote working procedures and interoperability testing with Latvia's National Guard has improved staff resilience in crisis scenarios.

However, soft skills training and structured communication protocols for public engagement remain areas for improvement. While media and public relations capabilities have developed informally, formal communication training for CERT.LV personnel should be prioritised.

Tools Maturity: Enhanced Detection, Prevention, and Response Capabilities

Technological advancements represent one of the most notable improvements since the 2015 evaluation, particularly in the areas of incident detection and prevention. Key developments include:

- Deployment of a national early warning sensor network, allowing CERT.LV to detect cyber threats in real time and provide targeted alerts to critical infrastructure operators.
- Expansion of CERT.LV's SOC, which now offers proactive threat monitoring, anomaly detection, and automated response mechanisms.
- Development of a DNS RPZ (DNS firewall) service, which has become a widely used cybersecurity tool for both public and private sector entities.
- Integration of automated threat intelligence feeds from sources such as MISP, Shadowserver, and international cybersecurity partners.

Compared to 2015, CERT.LV has moved from a largely reactive incident response model to a more proactive approach, incorporating threat hunting, penetration testing, and cyber resilience initiatives. However, challenges remain in ensuring

continuous funding for the development and maintenance of advanced cybersecurity infrastructure.

Process Maturity: From Ad-Hoc to Standardised Workflows

CERT.LV's incident response processes have evolved significantly, transitioning from a semi-structured model in 2015 to a fully documented and standardised approach in 2024. Key improvements include:

- Adoption of a cyber incident classification matrix, based on the UK model, to prioritise incident response efforts based on impact and victim importance.
- Formalisation of the escalation process for cyber incidents, ensuring that major national security threats are communicated to senior government officials in a timely and coordinated manner.
- Establishment of a 24/7 emergency helpdesk, with predefined escalation pathways to CERT.LV leadership, the Ministry of Defence, and other key stakeholders.
- Implementation of audit and feedback mechanisms, including quarterly and annual reporting to the Ministry of Defence, public accountability reports, and external audits by the State Audit Office.

Despite these improvements, CERT.LV still does not operate on a full 24/7 basis, relying instead on on-call response mechanisms. As cyber incidents increasingly require immediate intervention, transitioning to a fully operational 24/7 model should be a medium-term priority.

Conclusion and Policy Recommendations

The 2024 evaluation of CERT.LV's maturity shows clear improvements in governance, workforce capabilities, technological advancements, and incident response processes when compared to the 2015 evaluation. Over the past decade, CERT.LV has transformed from a developing CSIRT into a mature, strategically integrated national cybersecurity entity. This progress is particularly evident in the formalisation of its mandate, the expansion of its staff and expertise, the adoption of advanced cyber threat detection tools, and the establishment of structured incident response procedures.

A key factor contributing to this growth has been the integration of CERT.LV into Latvia's broader cybersecurity governance framework. By becoming part of the NCSC-LV and maintaining annual delegation agreements with the Ministry of Defence, CERT.LV has secured a stronger legal and operational foundation. In addition, its role within EU-wide cybersecurity cooperation mechanisms has enhanced its international engagement and capacity to respond to cross-border cyber threats.

CERT.LV has positioned itself as a proactive cybersecurity authority, not only by strengthening Latvia's cyber resilience but also by taking on a leadership

role in regional and international initiatives. One of the most notable developments has been its threat-hunting operations, which have been conducted in collaboration with EU and NATO allies and other partners. By leading these initiatives, CERT.LV has demonstrated its ability to operate at the forefront of cybersecurity defence, contributing to the security of Latvia and the broader European cybersecurity ecosystem. Moving forward, sustaining this leadership role will require ongoing investment in technical capabilities, human resources, and cross-border cooperation to keep pace with an increasingly complex cyber threat landscape.

To further enhance the resilience and effectiveness of CERT.LV, the following policy recommendations should be considered:

- 1 **Secure sustained funding for cybersecurity infrastructure.** Continued investment in cybersecurity capabilities is essential to ensure that CERT.LV can maintain and expand its early warning systems, SOC, and automated threat detection tools. Long-term financial planning should prioritise funding for infrastructure improvements and the development of new cybersecurity services.
- 2 **Enhance structured media and public communication training.** Cyber incidents increasingly require clear and timely public communication, especially within the current hybrid threat landscape. CERT.LV should implement structured media training for its personnel to ensure that public statements are accurate, transparent, and effective. Regular crisis communication exercises should be conducted in collaboration with the Ministry of Defence, State Chancellery, and other key stakeholders.
- 3 **Transition to a fully operational 24/7 incident response model.** The increasing frequency and impact of cyber threats make it necessary to provide continuous monitoring and incident response services. A phased approach to 24/7 operations should be considered, beginning with extended operational hours and eventually transitioning to full-time coverage.
- 4 **Strengthen talent retention and workforce development.** The cybersecurity sector faces a shortage of skilled professionals. CERT.LV should focus on talent retention strategies, such as career development programmes, competitive salaries, and continuous training opportunities, to ensure that it can attract and retain top cybersecurity experts.
- 5 **Improve cross-sector collaboration and international partnerships.** Strengthening partnerships with the private sector, academia, and international cybersecurity organisations can enhance Latvia's overall cyber resilience. Increased collaboration on cyber threat intelligence sharing and joint exercises will improve CERT.LV's ability to anticipate and respond to emerging threats.

Note

- 1 As of 2 March 2025.

Bibliography

- Brownlee, N., & Guttman, E. (1998). *RFC 2350 Expectations for Computer Security Incident Response*. <https://datatracker.ietf.org/doc/html/rfc2350>
- CERT.LV. (2024a). *Kas ir DNS uguns mūris*. <https://dnsmuris.lv>
- CERT.LV. (2024b). *Latvijas un NATO apvienotā komanda izcīnā pirmo vietu kiberaizsardzības mācībās "Locked Shields 2024"*. <https://cert.lv/lv/2024/05/latvijas-un-nato-apvienota-komanda-izcina-pirmo-vietu-kiberaizsardzibas-macibas-locked-shields-2024>
- CERT.LV. (2025). *Pieejama statistika par 2024. gadu*. <https://www.cert.lv/lv/2025/01/pieejama-statistika-par-2024-gadu>
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). <https://data.europa.eu/eli/dir/2016/1148/oj>
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). <https://data.europa.eu/eli/dir/2022/2555/oj>
- Duijnhoven, H., van Schie, T., & Stikvoort, D. (2019). *Global CSIRT Maturity Framework: Stimulating the Development and Maturity Enhancement of National CSIRTs*. Global Forum on Cyber Expertise. https://thegfce.org/wp-content/uploads/MaturityFramework-formationalCSIRTsv1.0_GFCE.pdf
- ENISA. (2015). *CSIRT Capabilities: How to Assess Maturity? Guidelines for National and Governmental CSIRTs*. <https://doi.org/10.2824/214073>
- ENISA. (2019). *ENISA CSIRT Maturity Assessment Model*. <https://doi.org/10.2824/860039>
- ENISA. (2024). *CSIRTs by Country - Interactive Map*. <https://tools.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map>
- FIRST. (2025). *FIRST Members around the World*. <https://www.first.org/members/map>
- Haller, J., Merrell, S. A., Butkovic, M. J., & Willke, B. J. (2011). *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability*. Carnegie Mellon University Software Engineering Institute. <https://doi.org/10.1184/R1/6572093.v1>
- Information Technology Security Law. (2010). <https://likumi.lv/ta/id/220962>
- ITU. (2025). *National CIRT*. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx>
- Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). State of the practice of computer security incident response teams (CSIRTs). *Carnegie Mellon University Software Engineering Institute technical report*. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf
- Morgus, R., Skierka, I., Hohmann, M., & Maurer, T. I. M. (2015). *National CSIRTs and Their Role in Computer Security Incident Response*. New America. <https://www.jstor.org/stable/resrep10504.1>
- National Cyber Security Centre. (2023). *Categorising UK Cyber Incidents: Explaining the NCSC and UK Law Enforcement Categorisation Model for Cyber Incidents*. <https://www.ncsc.gov.uk/information/categorising-uk-cyber-incidents>
- National Cybersecurity Law. (2024). <https://likumi.lv/ta/id/353390>
- Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*, 1(3), 9–19. <https://cyberir.mit.edu/site/elements-national-cybersecurity-strategy-developing-nations/>

- Novak, J., Manley, B., McIntire, D., Mudd, S., Hueca, A., & Bills, T. (2021). *The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities*. Carnegie Mellon University Software Engineering Institute. <https://doi.org/10.1184/R1/13624148>
- Skierka, I., Morgus, R., Hohmann, M., & Maurer, T. (2015). CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams. *Transatlantic Dialogues on Security and Freedom in the Digital Age*. https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT_Basics_for_Policy-Makers.493bfc8eb0ef4caa90869a4db30f47ce.pdf
- Spafford, E. H. (1989). The internet worm incident. In C. Ghezzi & J. A. McDermid (Eds.), *Proceedings of the 1989 European Software Engineering Conference (ESEC '89). Lecture Notes in Computer Science*, Coventry, UK (Vol. 387, pp. 446–468). Springer. https://doi.org/10.1007/3-540-51635-2_54
- Stikvoort, D. (2015). *SIM3: Security Incident Management Maturity Model*. Open CSIRT Foundation. <https://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf>
- Stikvoort, D., Kossakowski, K.-P., & Maj, M. (2023). *SIM3 v2 interim – Security Incident Management Maturity Model*. Open CSIRT Foundation. <https://opencsirt.org/csirt-maturity/sim3-and-references/>
- Teivans, V., & Smith, J. (2025). *Threat Hunt Playbook*. <https://www.cert.lv/en/threat-hunt-playbook>
- West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2nd ed.). Carnegie Mellon Software Engineering Institute. https://insights.sei.cmu.edu/documents/1606/2003_002_001_14102.pdf
- Wiik, J., Gonzalez, J. J., & Kossakowski, K.-P. (2006). Effectiveness of Proactive CSIRT Services. *Proceedings of the IT-Incident Management & IT-Forensics Conference (IMF 2006)*. Stuttgart, Germany. https://www.researchgate.net/publication/221002694_Effectiveness_of_Proactive_CSIRT_Services

5 Societal Resilience in Latvia

The Cybersecurity Perspective

Sigita Struberga and Žaneta Ozoliņa

Introduction

In the digital age, cybersecurity has become a critical component of societal stability and national security at large. As technology integrates deeper into the fabric of daily life, the threats posed by cyberattacks have evolved, affecting individuals, communities, and states. Cybersecurity is one of the newest areas of security policy, both in Latvia and globally. Initially, it primarily concerned the military and political sectors, where the state played a dominant role, taking responsibility for critical infrastructure and national defence.

However, with the growing integration of information and communication technologies (ICT) into everyday life, the frequency and intensity of cyber threats have increasingly put larger segments of the population at risk. National security gradually became interconnected with the ability of individuals to recognize cyber threats, respond appropriately, and mitigate them. This shift in security policy was described by scholars aligned with the Copenhagen School, emphasizing that societal resilience in cyber sector represents a significant departure from the state-centric paradigm of cybersecurity, which is predominantly rooted in the concept of national security. This perspective challenges traditional frameworks by advocating for a broader focus on the societal dimensions of cybersecurity. Burton and Lain (2020) underline the importance of shifting analytical attention towards societal cybersecurity, which emphasizes the protection of critical sectors such as health, energy, transportation, finance, and democratic governance. These sectors, integral to the functioning of modern societies, are increasingly susceptible to direct and indirect cyberattacks. Consequently, a close mutual interaction between the state, which provides conditions for public safety and security, and society, which actively participates in strengthening cybersecurity as a partner, can foster societal resilience.

The increasing frequency and sophistication of cyber threats have necessitated a shift from traditional defensive cybersecurity measures to a more resilient approach. This involves not only preventing attacks but also developing the capacity of individuals, communities, and society to absorb impacts, maintain essential functions, and swiftly recover. Societal resilience from the cyber perspective

encompasses various domains, including technical infrastructure, public awareness, policy frameworks, community capital, and collaborative efforts across different sectors.

The primary aim of this article is to explore the interaction between three fundamental pillars of societal resilience in Latvia: the state, the community, and the individual. The synergy among these elements is pivotal, as the intensity and quality of their collaboration shape the development of capabilities necessary to build a strong foundation for withstanding, adapting to, and recovering from the ever-evolving landscape of cyber threats. Analysing the nature and dynamics of interaction among these pillars will provide valuable insights and data for the creation of a policy framework aimed at strengthening Latvia's cybersecurity posture while fostering a resilient and engaged society.

The article is structured into six main sections to ensure a comprehensive examination of the topic. The first chapter outlines the research methodology, providing a systematic framework for data collection and analysis. This approach is designed to address the core research questions:

- What is the state's attitude towards including society in cybersecurity policy-making and implementation? Does the state perceive society as a passive recipient or as an active participant in cybersecurity efforts?
- What roles do communities play in fostering a resilient society in the cyber domain, and how is community capital utilized?
- How do individuals perceive cyber threats, and how do they define their roles in building societal cyber resilience?

By answering these questions, the research aims to uncover the current dynamics of engagement across all levels of society and identify areas for improvement in Latvia. The second chapter delves into the key definitions of societal resilience and examines their applicability to the cybersecurity domain. It discusses theoretical and practical perspectives, emphasizing the importance of resilience as a framework for addressing contemporary cyber challenges. The third chapter analyses the main policy documents that define cybersecurity in Latvia. It examines how these policies conceptualize the role of society and whether they encourage active societal involvement or primarily focus on top-down approaches. The fourth chapter explores the community pillar, focusing on the concept of "cyber capital" and its manifestation at the local level. It investigates how communities contribute to societal resilience through collaborative initiatives, resource pooling, NGOs, and capacity building. The fifth section examines the individual pillar by analysing how Latvian citizens perceive cyber threats and their roles in enhancing societal cyber resilience. This chapter investigates awareness levels, personal responsibility, and engagement in cybersecurity practices. The concluding chapter synthesizes the findings from the previous sections and provides actionable recommendations for building a roadmap towards societal cyber resilience. These recommendations aim to promote stronger collaboration among the state, community, and individual

pillars, enhancing Latvia's ability to address current and emerging cyber threats effectively.

Research Methodology

The study employs a range of research methods to provide a multifaceted approach to examining societal resilience in the cybersecurity domain in Latvia, ensuring the collection of relevant and valid evidence to address the primary research questions. This comprehensive methodology draws on best practices in interdisciplinary research and evidence-based policy analysis, as outlined by Creswell (2014). The specific methods employed include:

- 1 **Content analysis of legal and policy documents** to identify the primary approaches and interpretations of societal resilience in the context of cybersecurity in Latvia, the study conducts a detailed analysis of key legal and policy documents. The focus is on examining how societal issues are framed at the state level, particularly whether society is treated as a passive actor—requiring information dissemination and education—or as an active partner engaged in building a secure and resilient cyber environment. The scope of the document review encompasses frameworks addressing resilience both at the national and community levels, offering a comprehensive perspective on the integration (or lack thereof) of societal considerations in cybersecurity-related documents. Content analysis will systematically examine three key indices, as guided by Krippendorff's (2018) methodology:
 - **Presence or absence of references to society:** This will determine whether societal considerations are explicitly acknowledged in the documents.
 - **Frequency of references to society:** The frequency of mentions will be assessed to evaluate the relative importance assigned to societal aspects in comparison to technical, organizational, or other considerations.
 - **Qualification of society:** Documents will be scrutinized to determine whether society is depicted as a passive recipient of state-led initiatives or as a participatory actor actively involved in co-creating resilience frameworks.

The analysis will incorporate qualitative and quantitative components, identifying not only the prevalence of specific terms and concepts but also their contextual usage. This dual focus enables a nuanced understanding of whether policy narratives align with inclusive governance approaches, as advocated by scholars like Ostrom (2015).

By evaluating the framing of society within these documents, the study will uncover implicit assumptions about the role of civic engagement in cybersecurity. These insights will inform broader discussions on how policy design can better integrate societal resilience as a foundational element of cybersecurity governance.

- 2 **Focus group discussions with representatives from diverse stakeholder groups** to explore the main challenges, policy gaps, and potential recommendations

for improving societal resilience in the cybersecurity domain. The use of focus groups as a research method is grounded in its ability to capture dynamic interactions and nuanced perspectives, as highlighted by Morgan (1996). Eleven separate focus group discussions were conducted as part of this study in a period from March 2024 to January 2025. Three discussions were conducted in Riga, while eight covered Latvian regions. These sessions were designed to facilitate in-depth qualitative insights from a diverse range of stakeholders with direct expertise and decision-making authority in the fields of digital security and cybersecurity. Participants included subject matter experts, policymakers, and representatives from the business sector, all of whom are actively engaged in the development, implementation, and oversight of cybersecurity strategies and digital security frameworks. The goal is to elicit a deeper understanding of collective viewpoints and stakeholder priorities regarding the state of affairs with societal resilience in cyber domain and summarizing recommendations for the road map to more resilient society in the domain of cybersecurity.

- 3 **Semi-structured Interviews.** A total of 15 semi-structured interviews were conducted with representatives from multiple governance levels, including EU-level policymakers, national decision-makers, and key stakeholders from the business community. This approach facilitated the collection of diverse perspectives on digital security and cybersecurity challenges, contributing to a comprehensive understanding of policy approaches, regulatory frameworks, and industry best practices across various institutional and economic contexts. Additionally, this method enabled both the validation of previously gathered data and the exploration of societal resilience from multiple dimensions. As noted by Kvale and Brinkmann (2015), semi-structured interviews as data gathering method empowers to effectively balance structured inquiry with flexibility, making them particularly suitable for exploratory studies such as this one.
- 4 **Analysis of public opinion polls.** Recent public opinion surveys conducted in Latvia that address societal resilience and cybersecurity issues were analysed. The data has been collected from multiple Eurobarometer waves, along with opinion polls conducted by the BDA and the State Chancellery of the Republic of Latvia. This analysis aims to assess public perceptions of threats and risks and gauge attitudes towards cybersecurity at the national, community, and individual levels. This step will enhance the study's empirical base by integrating quantitative data reflective of broader societal trends.

By combining these research methods, the study seeks to integrate qualitative and quantitative insights, thereby enriching the understanding of societal resilience in the cybersecurity context. This mixed-research methods approach not only ensures a comprehensive exploration of the topic but also aligns with established research standards for multidisciplinary studies in political science.

The study aims to assess whether the initiatives undertaken by the government at both national and community levels, as outlined in legal frameworks, policy documents, and organizational structures, effectively contribute to fostering societal resilience. Additionally, the research seeks to determine whether

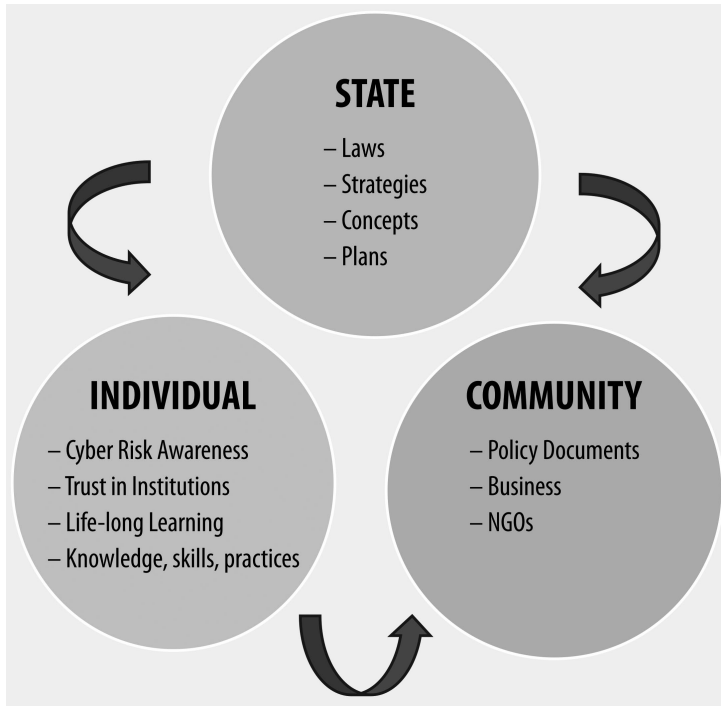


Figure 5.1 Research methodology overview.

these governmental efforts are grounded in participatory practices that actively engage society in enhancing the nation's cybersecurity. By evaluating the alignment between governmental measures and societal involvement, the study intends to identify gaps and opportunities for strengthening collaboration in this critical domain. The findings of this study will be reflected in recommendations for designing a comprehensive roadmap to achieve societal cyber resilience. The methodology employed in conducting this research is systematically structured and is depicted in Figure 5.1, which outlines the overall framework used to compose this article.

Defining Societal Resilience: What Relevance for Cybersecurity?

Most studies and research projects on resilience begin with a widely accepted definition that frames resilience as the capacity of systems to resist, absorb, and recover from shocks or crises (Folke, 2006). The concept originated within systems theory, which underscores the significance of interconnections and feedback loops within social, economic, and environmental systems. Walker et al. (2004) further articulated resilience as the ability of a system to absorb disturbances while maintaining its essential functions. Over time, this conceptualization was extended to encompass societal and social processes, providing a framework for understanding how

human beings, as integral components of social systems, restore equilibrium following shocks or disruptions (Burges, 2022).

Dante and Les (2016) highlighted that a key determinant of crisis-resistant and resilient societies is the prepared people in prepared households. This perspective points at the multi-scalar nature of resilience, as it is tested at all levels during emergencies—ranging from state institutions to individual citizens. By emphasizing the importance of preparedness, their work underlines the interconnectedness of systemic resilience and individual readiness, illustrating that resilience is not merely a structural characteristic but a dynamic interplay across state, community, and individual.

Societal resilience is a constantly changing and transforming concept depending on various factors, including such as risk and threat environment, contextual aspects, interpretation of security and safety concepts on national and local levels, as well as participatory level of society in large. Haavik underlines (Haavik, 2020) that introduction of the concept of societal resilience allows “to reach out to a broader public audience and to communicate ... addressing development trends with significance not only for resilient critical infrastructures, but for socio-ecological-political resilience” (Haavik, 2020, p. 2).

The incorporation of societal perspectives into security studies has fostered a growing consensus among scholars that well-prepared civilian populations are better equipped to respond effectively to diverse emergencies, thereby enhancing their overall resilience (Bodas et al., 2022). Bodas et al. (2020, p. 2) articulate a key distinction: “in contrast to national resilience, which deals with national infrastructure capacities to withstand and cope with hardships, societal resilience represents the ability of the members of the public to continue to function despite adversities”. This conceptual differentiation highlights the centrality of individual and collective agency within societal resilience frameworks.

In addition to the roles of the state and the population in fostering societal resilience, other scholars emphasize the importance of various communities as key contributors. These include businesses, local governments, research and development entities, and other stakeholders, all of which serve as essential actors in ensuring the functionality and sustainability of technologies and the systems that support them.

For instance, Elran (2017, p. 301) defines societal resilience as “the capacity of communities to flexibly contain major disruptions and to rapidly bounce back and forward following the unavoidable decline of their core functionalities”. This distinction emphasizes the importance of individual and community preparedness in maintaining societal stability amidst crises. Research (Aldrich & Meyer 2015) has shown that communities with higher levels of social capital, such as trust, networks, and norms, tend to recover more swiftly from disasters. Thus, fostering societal resilience not only involves preparing infrastructure and providing top-down approach for continuity of system function but also strengthening the social fabric and empowering individuals to act effectively in times of crisis. At the same time, Güngör and Elburz (2024) indicate that several dimensions of social capital of relevance for societal resilience and its correlations have been neglected. On the

one hand, relevance of community networks is a commonly accepted pre-condition for strong societal resilience, while place attachment was not sufficiently analysed.

Research further indicates that communities with elevated levels of social capital—characterized by trust, robust networks, and shared norms—tend to recover more swiftly and effectively from disasters. These attributes enhance collective problem-solving, resource mobilization, and emotional support during crises, demonstrating the critical role of social cohesion in mitigating adverse impacts. Consequently, fostering societal resilience requires a multifaceted approach that not only prioritizes the preparedness of physical infrastructure and top-down continuity mechanisms but also strengthens the social fabric and empowers individuals and communities to act decisively. By integrating these dimensions, resilience-building efforts can achieve a more holistic and sustainable impact.

In recent years, as a reaction to the widening of the concept resilience, a new term—cyber resilience is introduced. It approaches resilience as the ability of a system, organization, or society to withstand, adapt to, and recover from cyber-attacks and incidents. Research literature emphasizes that cyber resilience is not just about defence but also about maintaining operational continuity in the face of cyber disruptions. As authors of the comprehensive overview of cyber resilience argue (Björck et al., 2015, p. 312): “Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events. This ability can be considered at different levels”.

Such authors as Linkov (2013) and Chang and Shinozuka (2004) emphasize the necessity to use holistic approach to cyber resilience including also society, which is an integral part of cybersecurity landscape and is exposed to cyber threats and risks caused by humans or nature. Besides, societal cybersecurity includes pro-active aspects of resilience, namely, undertaking actions by individuals and groups aimed at mitigating potential threats. However, including society in security landscape is sufficient argument for introducing new concept, such as societal cyber resilience.

Necessity to introduce societal perspectives in cybersecurity domain is underlined and argued in Joe Burton’s and Clare Lain’s study (2020). They (Burton & Lain, 2020, p. 454) also emphasize the relevance of cognitive perspectives in cyberattacks:

The latest research on societal influences on cybersecurity supplement these theoretical assumptions by elevating the cognitive influence of cyberattacks and the cognitive effects generated within target populations. Fear, uncertainty and the sense of anxiety that cyber intrusions engender may shape responses in irrational ways, including in a national security context.

Acknowledging that the concept of societal cyber resilience is crucial in broadening the scope of actors involved in shaping the cybersecurity landscape, we align with the view that this concept remains insufficiently explored. As Joinson et al. (2023, p. 1) highlight, “There is a distinct lack of research on what would constitute cyber resilience in individual users of technology who may encounter cybersecurity

incidents in a domestic or non-work setting”. This gap in research underlines the need for a more comprehensive understanding of how societal resilience can be applied in the context of cybersecurity.

In response to this, the article builds on the concept of societal resilience, examining it specifically through the lens of cybersecurity. By doing so, we aim to contribute to the studies on how individuals, communities, and institutions can collectively enhance their capacity to anticipate, withstand, and recover from cyber threats. This perspective is essential in recognizing the interconnected nature of cybersecurity, where not only governments and organizations but also everyday technology users play a pivotal role.

The degree of societal resilience is directly influenced by the quality and intensity of the interactions between the state, diverse communities, and individuals, since they are essential contributors to the overall stability and functionality of society during crises. In this context, the more interconnected, collaborative, and inclusive these relationships become, the greater the resilience of the social system to potential risks and threats. This integrated approach fosters a collective capacity to anticipate, mitigate, and recover from disruptions, thereby reinforcing the robustness and adaptability of societal systems in the face of both anticipated and unforeseen challenges.

In the following chapters, applying the research methods described previously, we will analyse how societal resilience in the context of cybersecurity is approached by the state, community, and individual perspectives.

State Perspective

The conceptual framework of this study positions the state as a fundamental pre-condition for societal resilience in the field of cybersecurity. While communities and individuals are pivotal contributors to both cyber and societal resilience, the capacity to withstand, respond to, absorb, and recover from potential risks is contingent upon the level of collaboration among all stakeholders involved. Consequently, the initial step in this research involves examining the government’s attitude towards society and its role in mitigating potential cyber threats, as well as determining whether society is perceived as an active participant in fostering a cyber-resilient ecosystem.

To achieve this, the study employs a content analysis method, focusing on the following documents: (1) the National Cybersecurity Law (Law, 2024), (2) the National Security Concept (Security Concept, 2023), (3) the National Defence Concept (Defence Concept, 2023), (4) the Cybersecurity Strategy of Latvia 2023–2026 (Strategy, 2023), and (5) the State Civil Protection Plan (Plan, 2020).

The analysis specifically investigates the term “society”, examining its presence and frequency within these key legal and policy documents. The findings reveal that the term “society” is most frequently mentioned in the Cybersecurity Strategy (2023)—35 occurrences. In contrast, the National Cybersecurity Law (2024) references society six times, and the National Security Concept (2023) includes it four times. Notably, the State Defence Concept (2023) does not contain any

references to society, and the State Civil Protection Plan (2020) does not address cybersecurity within its scope of responsibility.

On the one hand, the limited focus of the National Cybersecurity Law (2024) on the engagement of society in the policymaking process can be attributed to the fundamental nature of the document itself. This law primarily serves to establish the foundational framework for cybersecurity, outlining basic principles, delineating the roles and responsibilities of key institutions, and defining their respective areas of jurisdiction. The operationalization and contextualization of these principles, including societal engagement, are more comprehensively addressed in the Cybersecurity Strategy (2023), which builds upon this foundational framework.

On the other hand, despite the overarching ambition to enhance societal resilience—a theme explicitly articulated in the majority of security-related policy documents—the State Civil Protection Plan (2020) appears to fall short in addressing the specific implications of cyberattacks on the general population. This omission is particularly notable given that the successful implementation of the plan is inherently dependent on active societal participation and the overall level of societal resilience. By neglecting the potential impact of cyber incidents on the population, the plan risks underestimating the critical interplay between societal engagement, resilience, and cybersecurity preparedness.

A deeper analysis of the aforementioned documents provided insights into whether society is portrayed as a passive recipient of state-driven initiatives or as an active, participatory stakeholder in the cybersecurity policy framework. This analysis was conducted by examining the contexts in which the term “society” appears within the documents.

The National Cybersecurity Law (2024) specifies that activities aimed at enhancing the digital and cybersecurity skills of the population should be further developed and elaborated upon in the National Cybersecurity Strategy (2023). According to the provisions of the law, the institution tasked with overseeing these activities is the National Cybersecurity Centre (NCSC). This body is mandated to collaborate with a range of partners, including governmental agencies, non-governmental organizations (NGOs), and private-sector entities. The explicit mention of partnerships within the law signals an initial ambition to foster a collaborative approach to building societal resilience to cyber threats. As an initial step in fostering partnerships, the NCSC has convened a group of 53 experts on cybersecurity from governmental, non-governmental, and business sectors. This group was established to disseminate relevant policy initiatives, inform and educate their respective target audiences, provide consultation to governmental institutions on cybersecurity matters, and coordinate related activities. Notably, the expert group convenes quarterly, ensuring a consistent consultation process with partners. The perspectives and insights shared during these meetings are systematically collected and subsequently integrated into various cybersecurity programmes.

However, among the activities referenced in the law, there is a marked emphasis on education and the dissemination of information. This focus suggests that the envisioned role of society, as articulated in the law, may be more aligned with passive forms of engagement, such as receiving knowledge and guidance

from institutional actors, rather than active participation in the formulation and implementation of cybersecurity measures. Consequently, while the inclusion of partnerships underlines an intent to involve a broader spectrum of stakeholders, the practical mechanisms for empowering society as an active contributor to cybersecurity resilience remain underdeveloped in the law's provisions.

Societal resilience is addressed in a more comprehensive manner in the Strategy (2023). It outlines that by 2026, the goal is to enhance public awareness, education, and research on cybersecurity issues. Public involvement in managing and mitigating cyber threats is envisioned alongside the activities of other institutions. At the same time, the document identifies several challenges, including overlapping institutional responsibilities and competencies, as well as potential issues that may arise in the future.

The Strategy (2023) assigns the task of educating the public on cybersecurity issues to the NCSC. However, it also notes that the Ministry of Education and Science is responsible for promoting public knowledge and understanding of cyberspace, conducting research, and advancing the capacity of higher education institutions. A lack of clarity regarding the coordination of educational programmes development and implementation between the Ministry and the NCSC further complicates the situation. Additionally, the involvement of another partner, the Latvian Safer Internet Centre "Net-Safe Latvia", in public education efforts raises further concerns about coordination and the ability to achieve national-level objectives effectively.

Concerns about insufficient institutional coordination on cyber issues were consistently raised by participants across all focus groups and interviewed respondents, who pointed to a lack of clear leadership in cybersecurity matters in Latvia. While the Ministry of Smart Administration and Regional Development is formally responsible for this area, cybersecurity falls under the portfolio of the Ministry of Defence, while public education and research are within the competence of the Ministry of Education and Science. Respondents broadly indicated that this fragmented governance structure, marked by a lack of coordination and ineffective oversight, represents a significant challenge. Such shortcomings not only weaken institutional responses to cyber threats but also hinder broader societal engagement in cybersecurity efforts.

At the same time, interviewees recognized the importance of government initiatives aimed at strengthening societal cyber resilience. However, concerns persist regarding the effectiveness of their implementation and the translation of cybersecurity knowledge into actionable capacity during risks and crises.

Community Perspective

The framework for the analysis of community resilience is presented in the study by Norris et al. (2008). This framework defines resilience through four interconnected domains: economic development, social capital, information and communication, and community competence. By utilizing this model, we assess how societies respond to crises and apply it as a structured approach to evaluating

Latvia's cybersecurity preparedness through the lens of societal resilience. At the community level, the assessment of societal resilience in cybersecurity is analysed across four key dimensions: a content analysis of local Civil Protection Plans, the involvement of NGOs and business groups, the role of social capital, and the level of trust in institutions.

Civil Protection Plans serve as critical indicators of how localities perceive and prioritize threats, while also reflecting the extent of engagement by individuals, organizations, and communities in mitigating risks. This study examines five strategically significant municipalities: Riga, Liepāja, the Dienvidkurzeme region, Alūksne, Daugavpils, and Rēzekne. Riga, as the capital, hosts critical infrastructure essential for state functions, while Liepāja, Latvia's third-largest city, holds strategic importance due to its NATO military base and major port. Alūksne, Rēzekne, and Daugavpils—situated on NATO's Eastern Flank and bordering Belarus and Russia—are particularly vulnerable to hybrid threats. Among them, Daugavpils, Latvia's second-largest city, serves as a key urban centre near the eastern border, further reinforcing its geopolitical significance.

Given that societal resilience, including in the cyber domain, is strongly influenced by the participation of NGOs, private sector entities, community groups, and specialists, semi-structured interviews were conducted. These interviews involved representatives from municipalities, the police, the State Fire and Rescue Service, NGOs, and the media. Their input was critical in understanding the extent of collaboration, awareness-building, and implementation of proactive defence measures against cyber threats.

As outlined in the previous chapter, the Civil Protection Plan of Latvia (Plan, 2020) serves as the national-level framework for disaster management and societal resilience. Local Civil Protection Plans are expected to align with this overarching document, adapting its guidelines to address region-specific risks and challenges. These plans are essential benchmarks for assessing societal resilience. However, the absence of cybersecurity as a component in the National Civil Protection Plan raises significant concerns about how risks will be identified, mitigated, and managed at the regional level. Furthermore, questions arise regarding the recovery process and the roles and responsibilities of key stakeholders in these efforts.

The analysis of the five Civil Protection Plans revealed significant disparities in their treatment of societal resilience and cybersecurity. For instance, the Liepāja and Dienvidkurzemes region's Civil Protection Plan (Liepāja, 2023) explicitly mentions "society" in the context of cybersecurity three times, signalling an awareness of critical risks facing local communities. The plan identifies three primary cyber risks and provides a detailed description of their potential impacts on the local population:

- 1 Fraud and theft perpetrated in cyberspace.
- 2 Cybercrimes as components of hybrid threats, including the use of ICT for disinformation campaigns.
- 3 Cyberattacks targeting private companies and public administration systems.

Despite acknowledging key cyber risks in the Liepāja and Dienvidkurzemes region's Civil Protection Plan (Liepāja 2023), the document does not incorporate specific initiatives aimed at educating, informing, or engaging the community to enhance resilience. However, this omission does not necessarily reflect a critical lack of public awareness integration. Insights gathered from semi-structured interviews indicate that the region benefits from a well-established level of cooperation among municipalities, the police, the State Fire and Rescue Service, NGOs, and local business representatives. Respondents highlighted that participatory practices in risk management are robust at the regional level and have been successfully tested through specialized training programs, but cybersecurity was not prioritized. The focus group interview similarly highlighted the resilience of NGOs and other entities in responding to various crises, such as power outages and other disruptions that communities have previously experienced and learned from. However, cybersecurity concerns did not emerge in discussions about secure everyday practices or crisis management.

Nevertheless, respondents expressed concerns regarding the effectiveness of communication during crises. While routine communication with local communities is reportedly functioning well, and residents are generally aware of risks and corresponding mitigation plans, critical gaps remain in crisis-specific communication capabilities. Specifically, respondents noted the absence of trained communication specialists equipped to manage information dissemination during emergencies. Additionally, a lack of basic psychological training among communication personnel poses challenges in addressing the psychosocial dimensions of resilience. This reflects broader issues identified by Windle et al. (2011), who emphasize the importance of psychosocial resilience in enhancing societal coping mechanisms, providing mental health support, and facilitating recovery and adaptation processes.

The Riga City Council's Civil Protection Plan (Riga, 2024), which governs the city and its territories, includes only a single mention of "society" in the context of cybersecurity, identifying CERT.LV as the responsible institution. During semi-structured interviews, representatives from the business sector and NGOs raised several critical issues regarding societal resilience in Riga. A significant challenge is the lack of trained cybersecurity governance specialists within the Riga City Council and other municipal administrations. This skills gap limits the ability to develop and implement effective societal resilience strategies related to cybersecurity.

Moreover, respondents noted a significant information deficit for the general population concerning cybersecurity at the local level. For most residents, accessing relevant information on cyber threats and protective measures is almost impossible. One potential solution to bridge this gap could be the establishment of "one-stop cyber agencies", which would serve as centralized hubs for disseminating information, providing guidance, and supporting community efforts to enhance resilience.

Additionally, focus group interviews demonstrated a growing interest not only from NGOs, private businesses, and other entities but also from active citizens

who wish to be more engaged in crisis preparedness and resilience-building efforts. There was a clear interest in strengthening resilience against various threats, including cyber risks. However, stakeholders agreed that in the case of Riga, Latvia's capital, preparedness mechanisms operate differently due to the concentration of national-level critical infrastructure. The same applies to national-level NGOs focused on cybersecurity and cyber-related issues.

At the same time, an open question remains regarding how to effectively inform and actively involve the private sector and citizens in building societal resilience in the cyber domain. Respondents noted a significant information deficit for the general population concerning cybersecurity at the local level. For most residents, accessing relevant information on cyber threats and protective measures is not an issue of interest and there are no extended guidelines on importance of it or potential measures to be done. One possible solution to bridge this gap is leveraging existing "one-stop cyber agencies" or so-called "Riga Neighbourhood residents' centres" for cybersecurity awareness. Since these centres are already operational, they could serve as centralized hubs for disseminating information, offering guidance, and supporting community efforts to strengthen resilience.

Notably, the Riga City Council website provides information summaries in various formats, including videos, covering a range of threats and crisis management mechanisms, as well as guidelines for residents on how to respond in different situations. Additionally, resources on cybersecurity and digital safety are also available.

At the same time, in general, municipal websites were identified as an underutilized resource. Respondents observed that these platforms rarely include information or links to resources related to cybersecurity, further exacerbating the information gap. Optimizing these online platforms by integrating user-friendly, accessible, and regularly updated cybersecurity resources could significantly contribute to enhancing societal resilience at the local level.

The Alūksne Civil Protection Plan (Alūksne, 2021) references the term "society" only once in relation to cybersecurity. Adopted in 2021 and updated in a single annex in 2024, the plan does not identify cybersecurity as one of the most probable threats. Instead, it situates cybersecurity within the broader context of terrorism. This categorization suggests a limited recognition of the distinct and pervasive risks posed by cyber threats, which may reflect the evolving nature of cybersecurity challenges since the plan's initial drafting.

The municipality's approach to societal resilience emphasizes the dissemination of information rather than fostering participatory practices. From Alūksne's perspective, the primary responsibility for cybersecurity lies with CERT.LV, the national cybersecurity authority. This includes tasks such as public information dissemination and the organization of awareness campaigns to address cyber risks. While these efforts are crucial, the absence of a localized participatory framework limits the ability to engage community members, NGOs, and private stakeholders directly in the mitigation of cyber risks and the enhancement of societal resilience. Shift from an information-driven approach to a more participatory model of resilience, would empower its community to actively contribute to the mitigation of cybersecurity risks.

It is worth highlighting that community resilience in Alūksne benefits significantly from the presence of the National Armed Forces, which actively collaborate with the municipal administration and other partners. This collaboration strengthens the municipality's capacity to address broader security challenges, including disaster response and crisis management. However, the synergy between the National Armed Forces and local efforts in the specific domain of cybersecurity remains underexplored in the plan.

Focus group interview reflected similar trends observed in the semi-structured interviews. On the one hand, respondents expressed a strong interest in measures to enhance their own resilience, as well as that of municipalities and local communities. On the other hand, they acknowledged a lack of broader knowledge on the subject, including and especially related to the cyber dimension.

The two cities in the eastern part of Latvia—Daugavpils (Daugavpils, 2022) and Rēzekne (Rēzeknes, 2024) in their respective Civil Protection Plans do not mention “society” in the context of cybersecurity. Diverse forms of cyber threats are not defined in the plans, as well as participatory frameworks of public engagement in case of crisis and emergencies are missing.

Focus group interviews in Daugavpils and Rēzekne municipalities highlighted that none of the examined municipalities have systematically developed comprehensive crisis preparedness strategies for the population in the context of cybersecurity. Data from focus group discussions and semi-structured interviews reveal that municipal crisis management predominantly adheres to a top-down governance model. This approach is characterized by the oversight of national-level institutions, centralized coordination, and collaboration with municipal authorities in crisis resolution. Although mechanisms have been established to facilitate private sector involvement in crisis management, their scope is largely confined to conventional crisis scenarios, such as military conflict, natural disasters, or infrastructure failures. Notably, cybersecurity remains an underexplored area within municipal crisis management frameworks, as evidenced by its absence from the strategic priorities of local governments.

Moreover, cybersecurity is often overlooked in broader municipal resilience-building efforts. The prevailing institutional framework positions cybersecurity as a national-level responsibility, thereby marginalizing the role of local governments and communities in fostering cyber resilience. This perspective not only limits proactive risk mitigation strategies but also hinders the integration of cybersecurity awareness at the local level.

Nevertheless, several notable steps have been taken. For instance, the 2024 Namejs military exercise (Ministry of Defence, 2024) incorporated elements of Latvia's cybersecurity preparedness, underscoring the need for adaptive economic structures, cohesive social networks, efficient information dissemination, and capable local governance. While primarily focused on national defence, the Namejs highlights the importance of a multi-level resilience strategy, encouraging active engagement from municipalities, private sector actors, civil society, and individuals in safeguarding national security.

Thus, it might be concluded that while Latvia has made progress in strengthening institutional and national mechanisms for the effective crisis management and

strengthening societal resilience, significant gaps remain at the community level, particularly in fostering a culture of shared responsibility among municipalities, businesses, and civil society actors.

Economic resilience and development constitute a fundamental pillar of community stability and resilience. This article primarily examines business perspectives on societal resilience within the cyber domain, with a focus on the ongoing processes that enable communities to withstand and recover effectively from cyber crises. Accordingly, this section analyses the attitudes of the business sector towards enhancing their own cybersecurity measures.

Findings from stakeholder interviews highlight that despite growing awareness of cyber threats, businesses in Latvia face major barriers to effective cybersecurity investment, often adopting reactive rather than preventive approaches. A key obstacle is the lack of financial support and governmental incentives, unlike in Germany or the Netherlands, where corporate social responsibility models encourage cybersecurity contributions through tax breaks and co-funding. A Luminor Bank (2024) survey found that 20% of Latvian small and medium enterprises do not prioritize cybersecurity investments. While 80% implement basic cybersecurity measures, only 42% take additional steps, and 38% allocate minimal financial resources, mainly investing in antivirus and firewalls. Meanwhile, 42% prioritize cybersecurity, with 14% developing strategies, 15% upgrading systems, and 13% using certified IT providers. According to Eurobarometer (2021), only 14% of Latvian businesses consider cybersecurity a very high priority, compared to 32% in Europe. While 51% of Latvians rate cybersecurity as a high priority (vs. 71% in Europe), 39% perceive it as a low priority (vs. 26% in Europe). Cybersecurity training remains low, with only 14% of Latvian small and medium enterprises offering training in 2021 (vs. 19% EU average), and 85% of Latvian businesses seeing no need for it. Furthermore, 69% of Latvians acknowledge that cybersecurity management within their companies is not delegated to external specialists or organizations (Eurobarometer, 2024). This suggests a widespread underestimation of cybersecurity risks, particularly in the private sector, where businesses often prioritize other operational concerns over cybersecurity preparedness.

Latvia's cybersecurity policy remains predominantly top-down, limiting broader stakeholder engagement. While governmental frameworks provide stability, private sector, and civil society participation is minimal. Focus groups indicate that businesses view cybersecurity as a government responsibility rather than a shared effort, resulting in policies that, despite setting high standards, often fail to address industry-specific needs. Interviews with cybersecurity professionals highlight the lack of mechanisms for integrating real-time private sector feedback, leaving many businesses vulnerable due to resource and expertise constraints.

Cybersecurity training should be a standard business practice, integrated into corporate governance like workplace safety rules. Interviews with executives suggest greater investment willingness if supported by government incentives. Alongside this, a cultural shift from reactive to proactive cybersecurity strategies is necessary, with greater involvement from executive leadership in shaping cybersecurity policies within organizations. Many businesses still treat cybersecurity as

a purely technical concern, rather than recognizing it as a core business risk that requires strategic oversight at the executive level.

Social capital, another critical pillar of societal resilience, plays a particularly significant role in the Latvian context, where trust in state institutions remains uneven, and local communities often assume a greater role in crisis response and cybersecurity awareness. In an environment where public confidence in governmental decision-making is low, grassroots initiatives, community networks, and civil society organizations become crucial actors in building cyber resilience. Low trust in government and related institutions weakens national cyber resilience by creating scepticism towards official guidelines, reducing compliance with cybersecurity best practices, and discouraging public participation in resilience-building initiatives.

According to a recent study on societal resilience (Struberga, 2024), only 29% of Latvian residents believe that the government makes the right decisions during crisis situations, including those related to cybersecurity. Additionally, trust in political institutions is alarmingly low, with 70% of Latvians expressing distrust in the Parliament and 66% distrusting the government. This prevailing scepticism may hinder public willingness to embrace state-recommended cybersecurity measures, potentially undermining collective resilience.

Beyond institutional trust, NGOs play a critical role in Latvia's cyber resilience policy by facilitating public engagement, disseminating cybersecurity knowledge, and fostering digital literacy. Their involvement is particularly relevant given Latvia's exposure to cyber threats from neighbouring states, where state-sponsored disinformation campaigns, cyber espionage, and targeted cyberattacks from Russia and Belarus have intensified in recent years (Burton & Lain, 2020). As intermediaries between government-led cybersecurity initiatives and the general public, NGOs contribute by delivering specialized training, enhancing media literacy, and equipping individuals with the skills needed to identify and counteract online manipulation and cyber threats. However, while NGOs such as Women4Cyber and RigaTechGirls have successfully engaged women and underrepresented groups in cybersecurity training and digital skills development, the broader integration of civil society into Latvia's national cybersecurity policy remains limited.

Despite growing awareness of cyber risks, Latvia's cybersecurity framework continues to rely predominantly on a top-down approach, with limited mechanisms for incorporating community-based cybersecurity perspectives into policy development. The development of a societal cyber resilience roadmap by the NCSC under the Ministry of Defence marks a valuable step towards strengthening engagement with cybersecurity stakeholders. However, findings from expert interviews and focus group discussions reveal that while NGOs contribute significantly to cybersecurity awareness, their potential remains underutilized due to insufficient funding, lack of structured partnerships with government institutions, and inadequate opportunities to shape national cybersecurity policies. Many cybersecurity NGOs operate independently, limiting the scalability and long-term impact of their initiatives. Furthermore, the absence of well-defined participatory mechanisms restricts opportunities for businesses and civil society organizations to engage actively in

resilience-building efforts, resulting in an uneven distribution of cybersecurity resources, particularly between urban and rural areas.

The effectiveness of Latvia's cybersecurity policy would be significantly enhanced by a more structured integration of NGOs and local communities into national frameworks. Increased public-private partnerships, targeted funding mechanisms, and improved stakeholder engagement platforms would bridge the gap between state-led initiatives and grassroots cybersecurity efforts. The Latvian Information and Communications Technology Association (LIKTA) has demonstrated the potential for public-private collaboration in cybersecurity awareness, but similar efforts must be expanded across different sectors. Additionally, institutionalizing NGO participation in cybersecurity policymaking would ensure that national strategies reflect the needs and realities of diverse societal groups, fostering more inclusive digital resilience.

Despite a solid basis for potential further development, beyond NGO involvement, Latvia's cybersecurity communication and collaboration remain fragmented. Despite national oversight, no unified framework exists for disseminating cyber risk information to businesses, municipalities, or the public. A limited corporate culture of societal resilience further hinders integration into public discourse. Weak municipal planning and early-stage private sector engagement, coupled with the absence of participatory mechanisms, underscore the need for a more cohesive and cooperative cybersecurity strategy. Latvia's cybersecurity resilience requires a participatory model, integrating businesses, local governments, and civil society. Strengthening public-private partnerships, encouraging corporate investment in cybersecurity, and embedding community-driven initiatives are essential for a cohesive strategy that extends beyond state institutions. Moving forward, embedding community-driven cybersecurity initiatives within Latvia's broader security framework will be crucial to ensuring that resilience-building efforts extend beyond state institutions and are actively supported by an engaged and informed society.

Individual Perspective

Latvia's individual-level cybersecurity resilience is steadily improving, driven by growing cyber risk awareness and public engagement. Strengthening trust in institutions and trust in business is essential for fostering a proactive cybersecurity culture. Expanding lifelong learning opportunities and enhancing the absorption capacity of skills, knowledge, and practice will further empower individuals to navigate cyber threats effectively. Improved communication, education, and outreach remain key to building a digitally resilient society.

A critical indicator of resilience is the extent to which individuals recognize potential cyber threats and understand the necessary mitigation measures. This includes awareness of specific risks, the ability to recognize cyber threats, and knowledge of emergency procedures. By aligning national cybersecurity strategies with public perceptions of risk, policymakers can ensure that security initiatives reflect both institutional priorities and societal concerns, creating a synergy between expert-driven responses and public engagement.

Previous research on Latvians' perceptions of cybersecurity threats suggests that while general awareness exists, concerns primarily centre around personal internet security, particularly regarding personal data, financial information, and online transactions. Findings from 2019 revealed that conspiracy theories—such as fears regarding the impact of 5G technology—were prevalent among certain population groups. However, by 2021, public concerns shifted towards broader security issues, particularly in relation to government responses to the COVID-19 pandemic. This evolution in risk perception highlights a gap between public priorities and national cybersecurity policies, which emphasize the increasing importance of cybersecurity in national defence and societal resilience (Ozoliņa & Struberga, 2023). Bridging this gap requires more targeted awareness campaigns that emphasize the role of cybersecurity not only in protecting personal assets but also in ensuring national security and stability.

Quantitative data further illustrates the evolving landscape of cybersecurity awareness in Latvia. According to the 2021 Eurobarometer survey, 64% of Latvians reported feeling informed about cyber risks, compared to a European average of 71%. Notably, those who considered themselves well-informed about cybercrime were also less concerned about cyber threats, suggesting that awareness can play a role in reducing fear and increasing confidence in digital security practices (Eurobarometer, 2021). More recent data from a 2023 survey conducted by the Baltic Computer Academy (Baltijas Datoru Akadēmija) reinforces these findings, indicating that 28% of Latvian residents feel they have a basic understanding of cybersecurity but recognize the need for updated knowledge. This need is particularly pronounced among individuals over the age of 50 and those between 30 and 39, highlighting key target demographics for future cybersecurity training initiatives. Furthermore, 12% of respondents acknowledged a lack of cybersecurity knowledge but expressed a willingness to learn, while a smaller segment—3%—found cybersecurity information uninteresting (TvNet, 2024). This suggests that tailored approaches are necessary to engage different groups based on their existing knowledge and interest levels.

Eurobarometer data from 2024 provides additional insights into public perceptions of digital security and data privacy. While 61% of Latvians believe they are receiving adequate digital skills education, perceptions of access to secure and privacy-friendly digital technologies remain slightly lower than the European average. 50% of Latvians rate their access to secure digital tools positively, compared to 55% across Europe. Similarly, 44% believe they have sufficient control over their personal data, slightly below the European average of 47%. Notably, 18% of Latvians reported being unsure about their level of data control—twice the European average of 9%—indicating a need for greater public education on digital rights and personal data protection (Eurobarometer, 2024).

Encouragingly, there is evidence that cybersecurity awareness is improving, particularly in relation to protective measures such as antivirus software use. Another survey revealed a positive trend: people are becoming more aware of the importance of antivirus programs. In 2021, 75% of the population reported installing antivirus software on their devices within the past two years, up from 55% in

2019. While it's encouraging that only 13% do not use any security solution, these 13% still represent individuals exposed to cyberattacks ((Labs of Latvia, 2022). This indicates a need for focused initiatives to enhance public confidence in digital security measures and data control practices. These findings highlight the importance of fostering greater confidence in cybersecurity tools and reinforcing public trust in digital safety practices.

Another significant challenge identified in expert interviews pertains to the competency of computer usage among individuals. While the implementation of advanced security programs and protective measures can enhance cyber resilience, their effectiveness is often compromised by user behaviour and insufficient digital literacy. Improper handling of software updates, engagement with unverified links, and the execution of insecure online activities can undermine pre-configured security protocols, rendering even the most sophisticated defence mechanisms ineffective. This issue highlights the critical intersection between technological security measures and human factors.

A fundamental strategy for enhancing cyber resilience lies in the systematic integration of cybersecurity education within lifelong learning frameworks. As the digital landscape undergoes rapid transformation, individuals must continuously develop their competencies in cybersecurity to effectively respond to evolving threats. However, the adoption of robust cybersecurity measures is often hindered by institutional inertia and resistance to change. Overcoming these challenges necessitates the formal incorporation of cybersecurity awareness into educational curricula, workplace training programs, and community outreach initiatives. By embedding cybersecurity as an integral component of digital competence, a culture of continuous learning and adaptive security awareness can be cultivated. Recent advancements in this domain highlight the increasing recognition of the necessity for sustained engagement in cybersecurity education, laying the foundation for a digitally literate and resilient society.

Recognizing the pivotal role of effective communication in cybersecurity education, ongoing initiatives aim to refine the dissemination of cybersecurity knowledge to the general public. A primary obstacle in this regard is the prevalence of technical jargon and complex terminology, which often impede the accessibility and comprehension of essential cybersecurity concepts. Consequently, many individuals face difficulties in adopting best practices, resulting in significant gaps in awareness and preparedness. To address this issue, initiatives have been introduced to train educators, media professionals, and cybersecurity specialists in developing structured, accessible, and audience-specific communication strategies. Findings from expert interviews underscore the importance of collaborative engagement among stakeholders, emphasizing that cybersecurity messaging must not only be technically accurate but also contextually relevant and tailored to diverse demographic groups. Such an approach is essential to bridging the knowledge divide and fostering widespread cybersecurity literacy.

Another area requiring strategic development is the promotion and utilization of existing cybersecurity training platforms. Latvia has already established valuable digital education resources, such as www.stars.gov.lv, yet public engagement

remains suboptimal due to limited awareness and inadequate outreach efforts. Insights from focus group interviews with industry experts and representatives from digital education sectors indicate that the visibility and accessibility of these platforms must be significantly enhanced. Targeted awareness campaigns, strategic partnerships with private enterprises, and the integration of cybersecurity training initiatives within workplaces can contribute to greater adoption across various societal sectors. Interdisciplinary collaboration between the private sector, educational institutions, and government agencies is imperative to ensure that these resources are effectively incorporated into formal training programs and community engagement initiatives, thereby maximizing their impact and reach.

Furthermore, findings from focus group discussions emphasize that an essential aspect of individual cyber resilience is the simplification of cybersecurity guidelines and their alignment with everyday digital practices. While advanced security protocols remain indispensable for critical infrastructure and IT professionals, the broader population benefits most from pragmatic, easily implementable security measures that can be seamlessly incorporated into daily digital interactions. Therefore, the development of clear, user-friendly cybersecurity guidelines tailored to specific groups—such as small business employees, senior citizens, and students—has become a policy priority. Although several initiatives focused on creating and disseminating accessible cybersecurity recommendations are already in place, their visibility and scope require further expansion to reach a broader audience and promote widespread adoption.

Latvia has made significant progress in public cybersecurity awareness, yet challenges remain in ensuring information is accessible, engaging, and effectively targeted. Cybersecurity is often deprioritized in daily life, limiting individuals' willingness to adopt protective measures. Current communication strategies lack demographic customization, reducing their impact. To enhance national cyber resilience, Latvia should refine cybersecurity education by integrating it into lifelong learning systems, tailoring communication to diverse societal groups, and fostering multi-sector collaboration. Strengthening cyber risk awareness and improving the absorption capacity of knowledge and skills will support a more adaptive and resilient digital society.

Conclusion and Recommendations

The concept of societal resilience is continuously evolving, with its conceptual boundaries expanding in response to emerging risks and challenges. Cybersecurity increasingly intersects with traditional notions of national security, influencing threat perception, response strategies, and recovery tactics at individual, group, and societal levels. Therefore, the conceptualization of societal cyber resilience requires multidisciplinary theoretical and applied studies. This concept is deeply embedded within the broader frameworks of national security, cybersecurity governance, and social capital theory. It encompasses not only the technical capabilities needed to counter cyber threats but also the institutional structures, public engagement mechanisms, and trust in governance that collectively shape a society's ability to anticipate, withstand, and recover from cyber incidents.

Contemporary research emphasizes that a comprehensive analysis of societal resilience in cyber domain urges to be extended beyond technical preparedness to encompass the broader structural factors that influence its effectiveness. This includes examining the role of institutional legitimacy, which underpins the successful implementation of cybersecurity policies, the adaptability of governance frameworks in addressing emerging threats, and the active involvement of civil society in protecting digital ecosystems. From this perspective, cybersecurity should not be understood merely as a technological challenge but rather as a multifaceted issue that necessitates coordinated action across multiple governance levels, active engagement from the private sector, and widespread digital education initiatives aimed at fostering societal cyber resilience.

This study has highlighted that while Latvia has established a strong institutional foundation for cybersecurity governance, the sustainability of these efforts is contingent on fostering greater societal involvement, strengthening trust in institutions, and embedding cybersecurity within everyday governance and business operations. One of the key research findings is that the state largely perceives society as a passive recipient rather than an active participant in cybersecurity policymaking and implementation. National cybersecurity strategies and regulatory frameworks provide structural safeguards, but their effectiveness is constrained by a limited inclusion of businesses, local governments, and civil society actors in resilience-building initiatives. The absence of structured participatory mechanisms prevents stakeholders from engaging in cybersecurity decision-making, reinforcing the perception that digital security is a state responsibility rather than a shared commitment.

The study also finds that communities play a crucial yet underutilized role in fostering societal cyber resilience. While certain local initiatives exist, cybersecurity remains an underdeveloped component of municipal governance, with many municipalities failing to incorporate digital threat management into their Civil Protection Plans. This discrepancy reflects a broader challenge: national cybersecurity policies do not sufficiently translate into localized preparedness, creating disparities in cybersecurity awareness and response capabilities between urban and rural areas. As a result, community engagement in cybersecurity remains sporadic, with limited coordination between local governments, businesses, and civil society organizations.

The role of businesses emerges as a critical factor in enhancing societal resilience, particularly in addressing the question of how economic stakeholders can contribute to national cybersecurity efforts. The private sector is not only responsible for protecting its own digital infrastructure but also plays a pivotal role in strengthening supply chain security, advancing workforce cybersecurity skills, and fostering public-private collaboration. However, cybersecurity in Latvia is often perceived as an operational expense rather than a long-term investment in business continuity, consumer trust, and national stability. Unlike in countries where corporate engagement is incentivized through tax benefits, subsidies, and regulatory advantages, Latvian businesses remain largely autonomous in managing cyber risks, leading to a predominantly reactive approach rather than proactive risk mitigation strategies.

Interviews with corporate executives indicate that many companies would be more inclined to invest in cybersecurity awareness and infrastructure if financial incentives or government recognition programs were introduced. Businesses that integrate cybersecurity into their governance frameworks not only protect their own digital assets but also contribute to the broader cybersecurity ecosystem through innovation, information-sharing, and workforce training. Additionally, public-private partnerships could help bridge the gap between state-led cybersecurity initiatives and private-sector capabilities, ensuring that businesses actively participate in resilience-building.

At the individual level, cyber risk awareness is increasing, but digital literacy and trust in cybersecurity measures remain uneven. While individuals recognize cyber threats, many lack the necessary skills, knowledge, and practical experience to implement effective security measures. National cybersecurity education platforms, such as www.stars.gov.lv, have been introduced to address this gap, yet their impact remains limited due to low public engagement, insufficient visibility, and a lack of systematic integration into formal education and workplace training structures. Moreover, cybersecurity awareness campaigns often fail to reach key demographic groups. This highlights the need for a differentiated and targeted approach to cybersecurity education, aligning training programs with the specific digital competencies of different societal groups.

Strengthening societal resilience in the cyber domain requires a shift towards a participatory and multi-stakeholder model. Businesses, local governments, and civil society actors must be systematically incorporated into resilience-building efforts to bridge existing gaps in cybersecurity awareness, preparedness, and response capacity. A more decentralized approach would enable cybersecurity to become an integrated component of municipal governance, with local governments mandated to incorporate digital threat management into crisis response planning. Additionally, introducing financial support programs for private sector cybersecurity investment would incentivize businesses to adopt stronger security measures, training initiatives, and risk mitigation strategies.

Box 5.1 Key Policy Recommendations for Strengthening Societal Cyber Resilience

- A valuable step towards strengthening cybersecurity resilience is fostering participatory cybersecurity building by encouraging businesses, local governments, and civil society organizations to actively contribute to national cybersecurity decision-making and crisis response planning.
- Incorporating cybersecurity into municipal crisis management can enhance local preparedness by integrating digital risk management strategies into Civil Protection Plans.
- Expanding community-based cybersecurity resilience by supporting NGOs and grassroots initiatives can foster greater public awareness and engagement in risk mitigation efforts.

- Embedding cybersecurity education into lifelong learning ensures that individuals across different societal groups have continuous access to updated digital literacy and security skills.
- Enhancing communication strategies through targeted and accessible awareness campaigns can help build public trust in institutions and digital safety practices. Increasing transparency and stakeholder engagement in cybersecurity governance fosters stronger collaboration between society and the state.

Rebuilding public trust in cybersecurity governance is essential to ensuring greater compliance with cybersecurity policies and fostering a more engaged and security-conscious society. This requires greater transparency in cybersecurity policymaking, the institutionalization of public consultations, and the development of inclusive digital governance mechanisms that empower citizens and businesses to take an active role in cybersecurity awareness and best practices. Furthermore, cybersecurity communication strategies must be re-evaluated to ensure that information is accessible, practical, and tailored to diverse societal groups. Focus group discussions indicate that targeted and easy-to-understand public awareness campaigns can enhance public engagement, moving beyond technical jargon to resonate with specific digital behaviours and risk profiles.

Latvia has made significant progress in institutionalizing cybersecurity resilience, but its long-term sustainability depends on expanding stakeholder participation, strengthening cross-sector collaboration, and fostering a culture of proactive digital security (see Box 5.1). A balanced approach that integrates regulatory oversight with participatory governance will be key to ensuring that cybersecurity is not merely a policy priority but a shared societal commitment. If these structural adjustments are effectively implemented, Latvia has the potential to serve as a model for small-state cybersecurity resilience.

References

- Aldrich, D. P., & Meyer, M. A. (2015). Social capital and community resilience. *American Behavioral Scientist*, 59(2), 254–269.
- Alūksnes sadarbības teritoriju civilās aizsardzības plāns. (2021). (Alūksne and its territories' Civil Protection Plan). aluksne.lv/09_03/ASTCAP.pdf
- Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience – Fundamentals for a definition. *Advances in Intelligent Systems and Computing*, January 2015, 353, 1–7. https://doi.org/10.1007/978-3-319-16486-1_31
- Bodas, M., Peleg, K., Stolerio, N., & Adini, B. (2022). Understanding societal resilience—Cross-sectional study in eight countries. *Disaster and Emergency Medicine*, 10, 1–14. <https://doi.org/10.3389/fpubh.2022.883281>
- Burges, J. P. (2022). *What Is Societal Resilience? Building Societal Resilience. The Role of Inclusion in a Fragmented World*. AXA Research Fund.
- Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy*, 5(3), 449–470.

- Cabinet of Ministers of the Republic of Latvia. (2020). The State Civil Protection Plan. <https://likumi.lv/ta/id/317006>
- Cabinet of Ministers of the Republic of Latvia. (2023). The Cyber Security Strategy of Latvia 2023–2026. <https://likumi.lv/ta/id/340633>
- Cabinet of Ministers of the Republic of Latvia. (2023). National Security Concept 2023. Par Nacionālās drošības koncepcijas apstiprināšanu
- Chang, S. E., & Shinozuka, M. (2004). Measuring improvements in the disaster resilience of communities. *Earthquake Spectra*, 20(3), 739–755.
- Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage.
- Dante, A. D., & Les, W. (2016). The Unbroken Chain in a Resilient Society. International Policy Digest, September.
- Daugavpils pilsētas un Augšdaugavas novada sadarbības teritorijas civilās aizsardzības plāns. (2022). (The Daugavpils city and Augšdaugavas region's Civil Protection Plan). CAP_aktualizets_2022_03_gala_Novads_01.docx
- Elran, M. (2017). Societal resilience: from theory to policy and practice. In I. Linkov & JM. Palma-Oliveira (Eds.), *Resilience and Risk* (pp. 301–311). Springer.
- Eurobarometer. (2021). Flash Eurobarometer 496. SMEs and Cybercrime. <https://europa.eu/eurobarometer/surveys/detail/2280>
- Eurobarometer. (2024). Special Eurobarometer 551. The Digital Decade. <https://europa.eu/eurobarometer/surveys/detail/3174>
- Folke, C. (2006). Resilience: the emergence of a perspective for social-ecological systems analyses. *Global Environmental Change*, 16(3), 253–267.
- Güngör, M., & Elburz, Z. (2024). Beyond boundaries: what makes a community resilient? A systematic review. *International Journal of Disaster Risk Reduction*, 108, 1–15.
- Haavik, T. K. (2020). Societal resilience – Clarifying the concept and upscaling the scope. *Safety Science*, 132, 1–8.
- Joinson, A. N., Dixon, M., Coventry, L., & Briggs, P. (2023). Development of a new ‘human cyber-resilience scale’. *Journal of Cybersecurity*, 9(1), 1–10. <https://doi.org/10.1093/cybsec/tyad007>
- Krippendorff, K. (2018). *Content Analysis: An Introduction to Its Methodology*. Sage Publications.
- Kvale, S., & Brinkmann, S. (2015). *InterViews: Learning the Craft of Qualitative Research Interviewing*. Sage Publications.
- Labs of Latvia. (2022). Pētījums: kiberuzbrukumi Latvijā saglabājas augstā skaitā. <https://labsoflatvia.com/aktuali/kiberuzbrukumi-saglabajas-augsta-skaita>
- Liepājas valstspilsētas un Dienvidkurzemes novada Civilās aizsardzības plans. (2023). (The Liepāja and Dienvidkurzemes region's Civil Protection Plan) https://faili.liepaja.lv/CAP/Liepajas-DKN-ST-CAP_2023ATJ.pdf
- Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4), 471–476.
- Luminor Bank. (2024). <https://www.financelatvia.eu/news/latvijas-uznemumi-apzinigakie-kiberdrosiba-baltija/>
- Ministry of Defence. (2024, August 26). Comprehensive national defense exercises “Namejs 2024” are underway in Latvia. <https://www.mod.gov.lv/lv/zinas/latvija-norisinas-visaptverosas-valsts-aizsardzibas-macibas-namejs-2024>
- Morgan, D. L. (1996). Focus groups. *Annual Review of Sociology*, 22, 129–152.
- National Cybersecurity Law. (2024). <https://likumi.lv/ta/id/353390>
- National Security Concept. (2023). <https://likumi.lv/ta/id/345911>

- Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American Journal of Community Psychology*, 41(1–2), 127–150.
- Ostrom, E. (2015). *Governing the Commons: The Evolution of Institutions for Collective Action*. Oxford University Press.
- Ozoliņa, Ž., & Struberga, S. (2023). Subjective perception of hybrid threats in Latvia. *Lithuanian Annual Strategic Review*, 20, 133–135. <https://doi.org/10.47459/lasr.2023.20.6>.
- Rēzeknes valsts pilsētas un Rēzeknes sadarbības teritoriju civilās aizsardzības plāns (2024). (Rezekne city and Rezeknes cooperation territories' Civil Protection Plan). <https://rezekne.lv/wp-content/uploads/2024/03/Rezeknes-valstspilsetas-un-Rezeknes-novada-sadarbibas-teritorijas-Civilas-aizsardzibas-plans.pdf>
- Rīgas sadarbības teritorijas civilās aizsardzības plans (2024). (Riga and its territories' Civil Protection Plan). <https://www.riga.lv/lv/media/56912/download?attachment>
- State Defence Concept (2023). https://www.mod.gov.lv/sites/mod/files/document/AM_VAK-2023_0.pdf
- Struberga, S. (2024). Latvia. In S. Struberga, D. Bankauskaite & D. Teperik *Examining Societal Resilience in the Baltics: A Public Outlook 2024* (pp. 13–21). Latvian Transatlantic Organisation. <https://www.securebaltics.eu/examining-societal-resilience-in-the-baltics-a-public-outlook/>
- TvNet. (2024). Aptauja: 49% Latvijas iedzīvotāju trūkst zināšanu par riskiem digitālajā vidē. 28 March. <https://www.tvnet.lv/7989125/aptauja-49-latvijas-iedzivotaju-trukst-zinasanu-par-riskiem-digitalaja-vide>
- Walker, B., Holling, C. S., Carpenter, S. R., & Kinzig, A. (2004). Resilience, adaptability and transformability in social-ecological systems. *Ecology and Society*, 9(2), 5.
- Windle, G., Bennet, K. M., Noyes, J. P. (2011). A methodological review of resilience measurement scales. *Health and Quality of Life Outcomes*, 9(1), 8. 2–18.

6 Latvian Approach to Fighting Cybercrime

Criminal Liability, Problems, and Solutions

Uldis Ķinis

Introduction

Legally, cybersecurity can be analysed from both broad and restricted perspectives. More broadly, it refers to safeguarding the entirety of the legal principles that humanity has established within a digital context. The Internet was utilized by 91.4% of Latvia's population in 2022 (Official Statistics Portal, 2022). There are around 1.4 million individuals who possess distinct Internet addresses. The Eurobarometer survey for 2020 revealed that 43% of Latvian respondents expressed a lack of confidence in their protection against cyber threats, while 68% stated that the likelihood of falling victim to cybercrimes was increasing (Eurobarometer, 2020). Furthermore, when comparing the data from 2012 onwards (Eurobarometer, 2012), specifically the Eurobarometer's initial report on cyber security, it is evident that the trend has remained consistent. The criteria used to evaluate cybersecurity of Latvian respondents has not undergone any significant changes over the years. Moreover, within the realm of cybersecurity, the Eurobarometer has conducted an extensive analysis of various threats, encompassing areas such as child protection and hate speech. This demonstrates that cybersecurity, within a broader framework, encompasses various measures aimed at safeguarding the lawful interests of the nation's citizens.

However, in a more specific sense, cybersecurity can be narrowed to two components: the protection of information systems, which involves a combination of legal, organizational, and technical measures to safeguard the integrity, confidentiality, and availability of automated data processing system (ADPS) resources, and the handling of security incidents (Kinis, 2022). In this study, we will conduct a thorough analysis of the legal aspects surrounding the terms "information system security" (ISS) and "security incident". A security incident refers to a deliberate harmful act committed by a person that has the potential to compromise the integrity, availability, and confidentiality of system resources. These acts have been officially recognized as cybercrimes for the first time in history by the Convention on Cybercrime (referred as CC) (Council of Europe, 2001).

The definition of cybercrime is a subject that every diligent cybercrime researcher endeavour to establish, as it lacks a universally acknowledged definition. The Committee of Experts on Cybercrime of the Council of Europe was unable to

reach a consensus on defining a criminal offence and to include it in the text of CC and the Explanatory Report to the Convention on Cybercrime (referred as ER CC) (Council of Europe, 2001). All current definitions are constructed according to the specifics of the national legal systems. Hence, the aim of this chapter is not to extensively examine the substance of the Treaty against Cybercrime, but to underscore the thesis mentioned in paragraph 22 of the ER CC, which states that parties are not required to directly replicate the definitions outlined in the treaty within their own domestic legislation. For this reason, this chapter will examine the distinctive features of Latvia's criminal legislation and criminal procedural regulation, as well as the challenges encountered in its implementation within the Latvian judiciary.

The first section will provide an overview of the legislative framework pertaining to criminal offences related to the security of information systems and fraudulent activities within ADPS. The second section addresses issues pertaining to the implementation of cybercrime jurisdiction and the criminal procedural framework in relation to the collection, analysis, and application of electronic evidence. The third section will focus on the most recent advancements, challenges, and potential remedies in case law. It will rely on Latvian legal sources, scholarly research, and court rulings as these are essential for achieving this chapter's objective of showcasing the efficacy of Latvian criminal law and the obstacles it faces in the realm of cybercrime.

The study uses a scientific research method that focuses on epistemology, along with text analysis, comparison, and methods of logical induction and deduction. Since legal documents are heavily featured in the study, methods like legal, historical, comparative, systemic, grammatical, and teleological approaches are employed to analyse these sources. The aim of the research is to analyse national problems in combating cybercrime. This chapter is based on the laws and regulations of the Republic of Latvia, court case law, and the findings of local researchers on the problems of combating cybercrime.

The Concept and the Legal Framework of Cybercrime

The Concept of Cybercrime

Latvia regained its independence in 1991 and completely reinstated the operation of its Constitution of Latvia from 1922 (*Latvijas Republikas Satversme*, 1922). Section 1 provides: "Latvia is an independent democratic republic". However, until 1998, the Latvian Criminal Code (*Latvijas Kriminālkodekss*, 1961) was in effect, with some modifications, which partially facilitated the adoption of fundamental principles of criminal law from the Western European criminal law doctrine. Implementing change was a challenging endeavour due to the fundamental differences between the criminal justice system of the USSR and the legal doctrine of the Western Europe. The difficulties primarily arose from the application rather than the creation of a new legal framework, as it required a shift in the underlying paradigms of legal thinking. The Constitutional Court has acknowledged in its

jurisprudence that Article 1 of the Constitution establishes a democratic legal system in Latvia that upholds the ideals of democracy and the rule of law. These principles include legality, justice, proportionality, and the protection of human rights (Latvijas Satversmes Tiesa, 2014).

The legal system of the USSR did not acknowledge the notion of human rights. Therefore, when formulating the new Criminal Law, it was crucial to emphasize that criminal responsibility is invariably associated with the restriction of fundamental rights of persons. The primary objective of this restriction is to safeguard the rights and lawful interests of other individuals. Australian researchers Majid Yar and Kevin F. Steinmetz (2024) wrote: “Crime is a notoriously difficult subject to study”. This quote perfectly illustrates that crime will always exist irrespective of state political order. According to Lindsay Farmer (2016), modern criminal law has the objective of safeguarding both private and public legitimate interests by imposing penalties for the harm inflicted upon them. This theory was extensively integrated into the Criminal Law due to reason that the Criminal Law’s framework was established by categorizing offences based on the threatened lawful interests. In addition, essential elements of universal law derived from the notion of the rule of law, such as legality, proportionality, fairness, and so on, were integrated into the Criminal Law.

Section 1 of the Criminal Law (1998) enshrines the principle of legality – *nulla poena sine lege*, which means that no punishment can be imposed unless it is prescribed by law. Meanwhile, Section 6 of the Criminal Law defines “a criminal offense as a harmful act or failure to act that is committed either intentionally or through negligence”. This offence must be specified in the law and carried out as a prescribed criminal punishment. It is crucial to highlight that criminal culpability only occurs when all the essential components of the offence (including the object, objective side, subject, and subjective side) can be proven. An object refers to the lawful interest that requires protection, while an objective aspect refers to an action or omission, the causal connection, and the resulting harm. A subject refers to an individual who is considered responsible and has attained the age of 14. They are suspected of committing the claimed offence. However, the subjective aspect pertains to the guilt and intention of the person. If any of the constituent elements are absent, there is no justification for imposing criminal liability on an individual.

To discuss cybercrime, it is essential to recognize that cybercrime must encompass all the essential aspects of a criminal act. Indeed, the definitions of crimes, such as fraud, theft, robbery, extortion, counterfeiting, and damage to property, have been widely recognized and enforced for thousands of years. Nevertheless, these categories were exclusively used to describe offences that took place within a specific geographical region and in an actual location. The occurrence of cybercrime is rooted in the fact that it occurs in cyberspace, which is essentially an ideal and intangible realm “created by users connecting communication devices to information services” (Council of Europe, 2001). This space consists of a continuous movement of electrons that traverse unrestrictedly at the velocity of light. Furthermore, this field lacks a globally enforceable and standardized structure. What is the importance of safeguarding cyberspace? Individuals utilize

the movement of electrons to establish, alter, and conclude legal relationships. The essence of any legal relationship lies in certain lawful interests, which are the state's responsibility to safeguard. The Cybercrimes Committee experts acknowledged that conventional definitions of crimes often prove inadequate in combating online offences and safeguarding the lawful interests of individuals. Consequently, the development of new definitions of criminal offences was deemed necessary and subsequently incorporated into the CC.

The rampant development of information technology, particularly artificial intelligence, will significantly impact the current global legal landscape. In 2011, Rosen J. and B. Whites highlighted the potential challenges that the rapid technological advancements in the 21st century would pose to society's legal and constitutional values. They argued that "this would necessitate a re-evaluation of various issues, such as the right to information, privacy, the concept of personality, and the state's responsibility to ensure security" (Rosen & Whites, 2011). It is difficult to dispute this prediction. This point was also emphasized during the 2018 International Conference of the Constitutional Court by prominent constitutional law experts from several European countries. Claire-Bazy Malaurie, a member of the Constitutional Council of France, highlighted that in "the governance of the global information space, national states are no longer the dominant force but rather one of many participants". She emphasized the importance of courts in developing a consistent solution to safeguard the fundamental rights and freedoms of individuals (Claire-Bazy, 2019). Undoubtedly, this poses a significant challenge as the European Convention on Human Rights mandates that parties take decisive measures to safeguard the human rights and liberties of persons, irrespective of the circumstances (European Convention on human rights, 1950). The necessity to govern the substance and safeguard the security of digital data and services provided and accessible, as well as to defend the interests of consumers and the fundamental rights of users, arises as a result. The General Data Protection Regulation (European Union, 2016) and the Digital Services Act (DSA) (Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), 2022) have been adopted in the European Union (EU). The Regulations establish the premise that the law should be applicable regardless of whether connections are established online or in the physical environment. Hence, the state should not simply watch the processes unfold but rather actively implement steps to guarantee the efficient safeguarding of fundamental rights as stated in the Constitution, irrespective of the means and methods of the crimes committed.

Upon examining the criminal liability regulations of over 20 Member States of the CC regarding offences related to automatic data processing, the author discovered that there are no two identical definitions of these offences. This finding aligns with various international studies, such as the Comprehensive study on cybercrime (UNODC, 2013), which state that the definitions of cybercrime "may vary depending on the national legal system's purpose of application". It is important to highlight that until nowadays scholars face the same problems with definition and qualification of cybercrime (Yar & Steinmetz, 2024). However, all these offences

share a common characteristic: they are all connected to the device utilized for automated data processing. In different countries, the term used to refer to this object that might be implemented for threatening or criminal purposes varies. It is referred to as a computer system in one country, an information system in another, and information technology in still another. Article 2(a) of the EU Cybercrime Directive defines an information system (Directive 2013/40/EU):

‘information system’ means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.

In Latvia, ADPS is acknowledged as both a target of cybercrime and a technology used to carry out illicit activities. When formulating this legislation, it was crucial to ensure technological neutrality and sustainability, enabling it to operate effectively under any future circumstances. Regardless of whether it is quantum or another technology, its fundamental purpose will always involve an automated data processing procedure. Therefore, the legislator aims to safeguard a device, or a collection of devices linked to a computer network, which allows user access and offers a service always related with use of ADPS. Theoretically, two-thirds of the offences outlined in the Special Part of the Criminal Law can be committed by using ADPS functions. This approach encompasses a comprehensive view of the concept of cybercrime, wherein cybercrime is acknowledged as any illicit action that utilizes automated data processing technologies to accomplish a criminal objective. For this study, we will adopt the most specific definition of cybercrime provided by M. Gercke in 2012 (Gercke, 2012). This definition focuses solely on “crimes committed online that target the integrity, accessibility, and confidentiality of computer systems and data”. When delineating these transgressions in the realm of Criminal Law, it is crucial to uphold the tenets of universal jurisprudence. We shall underscore two of these principles:

- 1 Principle of technological neutrality.** The idea of technological neutrality mandates that lawmakers must formulate definitions of cybercrime in a manner that is impartial to specific technologies. The Constitutional Court has recognized that “Legal norms developed and adopted in accordance with the principle of technological neutrality contain general concepts describing the regulated technologies in question according to their **purpose**, impact, function and other general characteristics” (Judgment case no. 2018-10-0103, para 18.1, 2019).
- 2 Principle of legal certainty.** The idea of legal certainty necessitates that the rule be made accessible to the public, comprehensible, and foreseeable. When examining this principle within the realm of criminal law, the Constitutional Court has acknowledged that “it does not follow from the requirements of the quality of legal norms (...) that it should be formulated as an absolutely precise instruction” (Judgment case no. 2018-10-0103, para 18.1, 2019). These two

court conclusions are crucial because criminal law cannot anticipate all potential forms of threats or the corresponding technologies. Hence, the legislator has designated the term “ADPS” as the most suitable Latvian term for a computer system that encompasses any device whose primary function is data processing and occurs online. In this study, we will examine the many components of criminal offences outlined in Sections 144, 177,¹ and 241, 243, 244 of the Criminal Law (1998). These correspond to Articles 2, 3, 4, 5, 6, and 7 of the CC.

Offences Against the Security of Information Systems

Articles 2–7 of Section 1 of the substantive law of the Convention provides that “Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally illegal access, illegal interception, data interference, system interference and misuse of devices” (Council of Europe, 2001). These crimes are aimed at compromising the confidentiality, integrity, and availability of ADPS. The construction of the criminal offences to be incorporated into the Special Part of Latvian Criminal Law is established according to the group’s objective. Specifically, the lawmaker incorporated criminal offences that are grouped together under a unified object of danger in the corresponding section. Consequently, the Criminal Law does not include a unified section that encompasses the offences outlined in Articles 2–7 of the CC. The provisions are distributed throughout various chapters in accordance with the structure of the Criminal Law. As previously stated, an individual can only be held legally responsible for a crime if all the necessary characters of the offence have been explicitly defined. The study will thoroughly analyse the nature and purpose of a criminal offence within the framework of each Article.

Object of criminal offence. Main task of criminal law is to protect public safety, order, and the legitimate interests of people. According to the doctrine of Latvian criminal law, the object is the interests protected by law, for the protection of which the specific article is elaborated in the criminal law. In relation to cybercrimes – everyone has a common interest to protect – the availability, integrity, and confidentiality of ADPS assets. These interests derive from the fundamental rights of individuals defined in the Constitution, such as the right to privacy, freedom of information, property, etc. Section 7 of the Criminal Law (1998) “Classification of Criminal Offences” classifies criminal delinquencies into: (1) criminal violations; (2) less serious crimes – intentional offences punishable by imprisonment of three months to three years; (3) serious crimes – intentional offences punishable by imprisonment of three to eight years; and (4) especially serious crimes – intentional offences punishable by imprisonment of more than eight years or life imprisonment. It is important to mention that criminal offences related to information security, which are the main crimes, are considered less serious. On the other hand, aggravated crimes committed by the intention to obtain property, or by an organized group, or directed toward specific targets, or resulting in serious consequences, as outlined in Section 241(3) and Section 243(5) of the Criminal Law, are classified as serious or especially serious crimes.

The subject of crime. According to the Criminal Law, individuals who are at least 14 years old and are mentally capable, are subject to criminal responsibility. Hence, this state is indistinguishable from all criminal offences and there is no necessity to delineate it explicitly. The study also includes offences that can be perpetrated by a specific category of criminal law, namely a “public official”. To qualify as a special subject of a crime as a public official, one must satisfy the requirements specified in Section 316 of the Criminal Law (1998). This includes individuals employed by state and local government institutions, as well as officials of state capital companies. Such individuals “must possess the authority to carry out functions related to supervision, control, investigation, punishment, or management of the assets and financial resources of a public entity or its capital company”.

Illegal Interception – Section 144

The criminal offence of “illegal interception” as stated in Article 3 of the Convention is described in Section 144 of the Criminal Law, which pertains to the violation of confidentiality in correspondence and information intended for transmission over telecommunications networks. This section is part of Chapter XIV of the Criminal Law, specifically focusing on criminal offences against fundamental rights and freedoms of an individual. It is grouped together with offences such as the violation of inventors and designers’ rights (Criminal law 147) and infringement of copyright and neighbouring rights (Criminal law 148), which are further defined in Article 10 of the CC. The offences outlined in this chapter pertain to the infringement of fundamental rights such as privacy, information, copyright, and freedom of creative expression, as established in Chapter VIII of the Constitution (Latvijas Satversme, 1922). We shall examine the precise legal definition of interception as outlined in Section 144 of the Criminal Law (Box 6.1).

Object of offence. The ER CC (Council of Europe, 2001) states that “This provision aims to protect the right of privacy of data communication. [...] [It] is enshrined in Article 8 of the European Convention on Human Rights” and such

Box 6.1 Excerpt from Section 144 of the Criminal Law (1998)

Section 144. Violation the Confidentiality of Correspondence and Information to be Transmitted over Telecommunications Networks

(2) For a person who commits unlawful interception of publicly unavailable data transmissions or signals in telecommunications networks, as well as unlawful acquisition of publicly unavailable electromagnetic data from a telecommunications network in which such data is present, the applicable punishment is the deprivation of liberty for a period of up to three years or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

rights are also protected by Section 96 of the Constitution. The offence in question must focus on protecting the legitimate interests of persons' right to privacy. Nevertheless, paragraph 59 of the ER CC states that in certain nations, this violation may be intricately linked to the offence of unauthorized interception of ADPS. When assessing the target of an interception offence, Marčiinauskaite (2013) argues that "it is important to differentiate between the right to privacy and the interest in confidentiality". The former should apply to data that is stored in the system, sometimes known as "data at rest", while the latter should apply to data that is being sent. This is comprehensible since in Lithuania, this violation is categorized under the section "Crimes against information system security" in the Criminal Code and requires a pertinent justification. But it is important to emphasize that the article protects only the transmission of information that is not publicly available, and a transmission whose content the participants do not want to reveal to third parties is not publicly available.

In Latvian legal doctrine, "confidentiality is an integral part of the rights to privacy" established by Article 96 of the Constitution (Latvijas Republikas Satversme, 1922). Thus, the violation of privacy in the case of illegal interception cannot be assessed without assessing the content of privacy rights and interests. The German Constitutional Court has also recognized this in its doctrine. In the *Bundestrojan* case, the German Constitutional Court assessed the legality of the actions carried out by the German special services, who installed a spy program on an individual's computer (Judgment in case No 1 BvR 370/07, BvR 595/07, 2007), and Court concluded (in para 197) "that it is essential to establish a new fundamental right for information users and owners in Germany, which guarantees the protection of information confidentiality and integrity, derived from the fundamental right to personal integrity". In paragraphs 204 to 206 of the judgment, the court determined:

What is first of all protected by the fundamental right to the guarantee of the confidentiality and integrity of information technology systems is the interest of the user in ensuring that the data which is created, processed and stored by the information technology systems, that is by its scope of protection remain confidential. (...) The fundamental right related protection of the expectations of confidentiality and integrity exists regardless of whether access of information systems can be achieved easily or only with considerable effort.

However, this right is not absolute and can be limited in cases of prevention or criminal prosecution, but only if such limitations are established by law. The *Budendestrojan* case's verdict significantly contributed to the establishment and advancement of a comprehensive legislative framework across Europe, ensuring the integrity, confidentiality, and accessibility of information systems' security.

Subject matter. While the legal definition of the violation does not explicitly mention "content", it is still important to briefly discuss the legal framework surrounding data transmitted online when determining if the actions described in the section breach the confidentiality of data or signals. This is because not all data necessarily contain confidential information. According to Article 1(b) of the CC, "computer

data” refers to information that can be electronically processed. According to Article 1(d) of the CC, traffic data refers to the data produced by computers involved in the communication process, which is used to direct a communication from its starting point to its endpoint. It is thus supplementary to the communication itself. This data is subject to a specific regime because, in the event of an investigation into a criminal offence involving a computer system, “traffic data is necessary to track the origin of a communication, serving as a basis for gathering additional evidence or as evidence of the offense” (Council of Europe, 2001) para 28. Nevertheless, CC notes that parties are not obligated to replicate this definition.

The Electronic Communications Law (2022) provides the following classification of data: Section 1.3) location data – data, which is processed in an electronic communications network and indicates the location of the terminal equipment of an electronic communications service user. (...) and Section 1.54) stored data – the traffic data referred to in Sections 100 and 101 of this law, location data and data related thereto, which the operator needs to identify the end-user when providing an electronic communication service. Consequently, content data is considered data in the context of interception, because all the above types of data provide information on the content of the information to be transmitted, which can be passwords, codes, electromagnetic signals, and metadata (Kīnis, 2015) p. 91. They must therefore be regarded as a secret of transmission.

Objective side of the offence. The objective side of a criminal offence consists of three factors – an act, a causal link, and a set of harmful consequences. Interception can solely be committed through an active action intercepting ADPS. Given the limitations of this study, it is improbable to provide an exhaustive list of all the methods that can be employed in the interception process. Consequently, any action that involves the utilization of technical devices should be regarded as an unlawful interception if its intention is to unlawfully obtain data, signals, or other information outlined in the section. The causal link of this offence refers to the direct relationship between the suspect’s actions and the detrimental repercussions that result from the illegal gathering of data. The repercussions of the offence occur as soon as the accused individual unlawfully acquires data, signals, etc. According to the topic of this chapter, it would be worth to include the following conclusion of the Senate regarding evaluation of objective and subjective side of interception. The Senate of the Supreme Court (Latvijas Republikas Augstākā tiesa, 2022) in case SKK-[B]/2022 concluded, that in order to hold the suspect – journalist criminally liable pursuant to Section 144 of the Criminal Law, court must take into consideration the findings of the European Court of Human Rights on the application of Articles 8 and 10 of the Convention in the context of Sections 96 and 100 of the Constitution, which have not been assessed extensively by the court of appeal, as the victim about whom the information was obtained and partially made public by the accused journalist is a politician known to the public, who “must have a higher tolerance for interference in their private life which also includes correspondence”. The Senate recognized that the court of appeal failed to conduct a balancing analysis of those rights in the judgment and revoke the judgment in its entirety because the objective side of the offence that the act was unlawful was not proved.

The Analysis of the Offences Encompassed in Sections 241–244 of the Criminal Law

The definitions of these offences are derived from the definitions outlined in Articles 2, 4, 5, and 6 of the CC. However, due to delays in the ratification of the Cybercrime Convention by some Member States of the EU, the European Union Cybercrime Directive (Directive 2013/40/EU) was adopted to harmonize the regulatory framework for combating cybercrime within the EU. Article 7 of the Directive 2013/40/EU mandates Member States to criminalize offences related to the integrity, confidentiality, and availability of ADPS.

Latvia has successfully met this requirement. These offences are included under Chapter 20, titled “Criminal Offences against General Safety and Public Order”, in the Special Part of the Criminal Law (1998). They are grouped together with offences such as Gangsterism, Mass riot, Cruel treatment of animals, torture of animals, and others. All of them are consolidated inside the collective threat entity known as General Safety and Public Order. The ISS is a crucial component of a nation’s security domain. Therefore, it can be inferred that the inclusion of these offences in Chapter XX of the Criminal Law underscores the legislator’s recognition that the protection of information systems is an essential component of public safety. We will do a more comprehensive analysis of the individual components of each offence.

The unauthorized access, both in theory and in practice, is regarded as the core offence of the ISS. The section’s language, in complete accordance with the stipulations of Article 2 of the CC, outlines three prerequisites for its implementation:

Box 6.2 Excerpts from Section 241 of the Criminal Law (1998)**Section 241. Arbitrary Accessing Automated Data Processing Systems**

(1) For a person who commits arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused thereby, the applicable punishment is the deprivation of liberty for a period of up to two years or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

(3) For a person who commits the acts provided for in Paragraph one of this Section, (...) if they are directed against an automated data processing system that processes information related to State political, economic, military, social or other security, the applicable punishment is the deprivation of liberty for a period of up to five years or temporary deprivation of liberty, or probationary supervision, or community service, or fine, with or without confiscation of property.

(1) access is deemed arbitrary solely when the individual lacks entitlement to it; (2) if the action pertains to evading security measures of a system; and (3) if the individual utilizes the privileges assigned upon another person (see Box 6.2). Conversely, the general phrase (substantial harm) pertains to the minimum threshold of consequences established by the legislator that would result in criminal culpability.

Regarding arbitrary access, availability ensures that authorized users of ADPS have the right to access ADPS resources. It also creates the rightful concern of the system owner that only individuals who have been authorized by the lawful owner or legal possessor can access the resources of ADPS. The article protects a person's right to determine access procedures to ADAS resources owned or held by him. Not every access is criminally punishable, if, for example, the system does not have safeguards, the owner does not treat his property with due diligence, then the state does not apply criminal remedies. Also, there is no crime if the victim is not substantially harmed by the arbitrary access.

The third paragraph of that section stipulates enhanced liability for the offence described in the first paragraph, namely when it targets an ADPS that handles information pertaining to the political, economic, military, social, or other security of the State. If the offence is committed against an ADPS that provides a service of public significance, the crime is fully accomplished by the illegal act itself. The legislator introduced revisions to hold individuals accountable for their actions after a person dubbed NEO (IR, 2013) exploited vulnerabilities in the system's security measures in 2010. NEO gained unauthorized access to the Declaration system of the State Revenue Service and illegally downloaded over a million documents. The individual was charged, but law enforcement and the prosecution were unable to substantiate that this action resulted in significant harm to any individual, thereby leading to the termination of the case.

To avoid such situations, the Criminal Law was amended to specify that if an individual engages in the actions described in the initial section of the article against systems associated with the execution of state security functions, they will be held accountable solely for the act of unauthorized access. Nevertheless, it is important to acknowledge that the language used in this statute lacks clarity, leading to a dispute over jurisdiction between the State Security Service and the State Police. The State Security Service has the authority to investigate crimes committed against critical information infrastructure. The section in question includes a clause that specifies its application to cases involving military, economic, environmental, ISS, and other security matters. Therefore, the State Police does not consider it within their jurisdiction to investigate offences falling under this section.

In 2010, the Information Technology Security Law (2010) was adopted. Section 1(1) of the law provides: "The purpose of this Law is to improve the security of information technologies, laying down the most important requirements in order to guarantee the receipt of such essential services, in the supply of which such technologies are used". This essential service is provided both by the critical information technology infrastructure defined in Section 3 of the law, and by service providers listed in Section 3.1 – Operators of Essential Services, Digital

Service Providers, and Representatives of the Digital Service Providers. The list covers a wide range of ADPS subjects, including government and local authorities, private individuals providing financial, supply, and delivery services, information technology, digital services, and other services. The regulation of this law applies to any subject of private law or representatives thereof, which performs economic activity in the territory of the Republic of Latvia.

For all subjects referred to in Section 3.1 of the Information Technology Security Law (2010) the state also set minimum ADPS security requirements (Cabinet Regulation No. 442, 2015).

The Regulation prescribes: the minimum security requirements for the information and communication technologies of the State and local government authorities, general security requirements for the State information systems; and minimum security requirements for ADPS who provided essential services for society.

However, it is likely that the number of ADPS covered under Section 241(3) of the Criminal Law will expand following the transposition of the NIS 2 Directive (Directive 2022/2555). Para 15 of Preamble of NIS 2 Directive says:

Entities falling within the scope of this Directive for the purpose of compliance with cybersecurity risk-management measures and reporting obligations should be classified into two categories, essential entities, and important entities. This classification is based on their level of criticality within their sector or the type of service they offer, as well as their size.

The Latvian government has approved a new National Cybersecurity Law (2024) to implement the provisions of the NIS2 Directive. Section 3 of the law specifies that it will be applicable to providers of essential and important services as well as critical infrastructure. Implementing legislation, it is probable that the scope of endangered ADPS outlined in Section 241(3) of the Criminal Law will be modified and clarified. Consequently, any debates regarding competition in the jurisdiction will be eliminated, as the police will assume authority over all offences against ADPS pertaining to essential and important services. However, offences against ADPS in relation to the critical infrastructure within the State Security Service's jurisdiction will remain under their purview.

The objective aspect falls under Section 241(1) of the Criminal Law. In this section, an act refers to a deliberate activity that involves unauthorized access to ADAS resources by bypassing the system's security safeguards. Within the NEO case, a TV debate took place in 2010 between legal professionals and ICT specialists about the question of whether exploiting a security flaw to gain system access may be deemed as arbitrary access. Regrettably, the prevailing viewpoint in the meeting was that such behaviour did not qualify as arbitrary access and therefore not to be subject to criminalization. The expression of gratitude contradicted the guidelines established by the UN and ITU (2010), as the "circumventing security measures"

Box 6.3 Excerpt from Section 243 of the Criminal Law (1998)

Section 243. Interference in the Operation of Automated Data Processing Systems and Illegal Actions with the Information Included in Such Systems

(1) For a person who commits unauthorized modifying, damaging, destroying, impairing or hiding of information stored in an ADPS, or knowingly entering false information into an ADPS, if substantial harm has been caused thereby, the applicable punishment is the deprivation of liberty for a period of up to three years or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

clause includes any action that mitigates, bypasses, neutralizes or exploits the security holes of the system, and program gaps but achieves the target and accesses the protected ADAS resources. The NEO case also revealed a deficiency in the expertise and comprehension of police officers, prosecutors, judges, and attorneys regarding the investigation and legal resolution of such crimes. Consequently, the professional training curriculum at all levels now includes prerequisites for acquiring the essential knowledge to prevent cybercrime.

Object of offence. That section contains two criminal offences consistent with Article 4 of the CC – data interference and Article 5 of the CC – system interference. The first paragraph of this section (Box 6.3) provides for liability for damage to information contained in the system. Criminal activities are directed against the ISS feature named integrity. The analysis of the *Bundestrojan* case demonstrates that the German Constitutional Court has acknowledged the constitutional protection of the right to data integrity. In addition, the court stated that “this principle applies not only to data stored in the ADPS but also to any stage of the data processing procedure”. This is because the integrity of information resources cannot be compromised without also compromising the integrity of the infrastructure and equipment. The ADPS is a complex system in which every alteration to one of its components results in a corresponding modification to the overall integrity of the entire system.

Objective side of offence. This offence can only be perpetrated through an action. The section presents two options: unauthorized manipulation (modification, destruction, removal, or editing) of existing information in the ADPS or intentionally inputting false information into the system with the intention of impacting the resources inside the system (Box 6.4). To establish the objective element of the offence, it is imperative to demonstrate that the victim has suffered significant harm. This offence can be committed through remote means or by physically inputting fraudulent data into a computer. For instance, the Prosecution Office reported a case where a customs officer was found responsible for entering information into the computer with the intention of deleting identifiers for a car undergoing customs inspection. Consequently, the driver brought in commodities that were on the EU’s list of sanctions against Russia, bypassing customs inspection. Any method capable

Box 6.4 Excerpts from Section 243 of the Criminal Law (1998)

Section 243. part two – System interference

(2) For a person who knowingly commits interference in the operation of an automated data processing system by entering, transferring, damaging, extinguishing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused, the applicable punishment is the deprivation of liberty for a period of up to three years or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

(5) For a person who commits the acts provided for in Paragraph one or two of this section, if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to the political, economic, military, social or other security of the State, or for the criminal offence provided for in Paragraph one or two of this section, if it has been committed by an organized group, the applicable punishment is the deprivation of liberty for a period of up to seven years, with or without confiscation of property and with or without probationary supervision for a period of up to three years.

of accomplishing the outcomes of the section shall be considered an action within the definition of that section.

Object of crime. According to paragraph 65 of the ER CC (Council of Europe, 2001) this crime in the physical world can be classified as sabotage. Unlike the criminal offences described in Articles 3 and 4 of the Convention, this crime object is all aspects of the ISS (integrity, confidentiality, availability) collectively. Section 89 of the Criminal Law (1998) establishes the responsibility for acts of sabotage, which are classified as crimes against the state under Title X. The objective of this section is to penalize actions that would cause harm to the Republic of Latvia. Furthermore, according to Section 89, sabotage is regarded as a grave or particularly grave offence due to the penalty of imprisonment ranging from 5 to 12 years. Theoretically, this could be implemented in cases of system interference, but only if the target of the offence was limited to critical information infrastructure. Nevertheless, according to the definition provided in Article 5 of the CC, any system that becomes the target of the activities specified in the Article is deemed to be an object of threat. As a result, the lawmaker made the decision to create a new structure for carrying out the regulation specified in Article 5 of the Convention. The objective of this offence is to safeguard owners or lawful possessors of ADPS against system disruption or obstructive attacks perpetrated via botnets. These acts are referred to as denial-of-service attacks or distributed denial-of-service (DDoS) attacks. In the context of criminal law, these attacks are specifically targeted on

ADPS with the intention of hindering its operations or causing its destruction. The intended target of this crime will consistently be the designated ADPS. Section 5 assigns accountability for acts conducted in the first and second part of the section, if those actions are aimed at the ADPS, which handles information pertaining to public security functions. We conducted a thorough examination of this object by analysing the provisions outlined in Section 241(3) of the Criminal Law.

Objective side. This offence can only be committed by an intentional act. A frequently employed method of attack involves inundating ADPS with spam or an overwhelming volume of requests that surpasses the system's processing capabilities. Furthermore, these requests or floods of "spam" might be accompanied by the infiltration of various viruses into the system. This malware is specifically designed to either gather certain information or to cause harm and destruction to ADPS resources. In this section, culpability is only established if the conduct described in the section directly result in significant harm to the victim. In the fifth section, the offence is deemed complete solely by the action itself, without requiring any harmful effect. Consequently, these offences are referred to as formal criminal offences. On the other hand, material criminal offences are those for which the occurrence of harmful consequences is an essential condition for criminal liability.

Object of crime. This offence corresponds to the criminal offence *illegal device* defined in Article 6 of the CC. This section defines a distinct and autonomous criminal offence against the confidentiality, integrity, and availability of ADPS or data (Council of Europe, 2001), para 71. Tools such as devices, computer programs, computer passwords, access codes, etc., that are specifically meant to unlawfully disrupt the resources of ADPS owned by another individual are considered instruments for perpetrating this offence. The target of the offence is the assets of ADPS, or a portion thereof.

Objective side. The activities outlined in this section pertain to the advancement, dissemination, and preservation of the devices and programs (see Box 6.5).

Box 6.5 Excerpt from Section 244 of the Criminal Law (1998)

Section 244. Illegal operations with automated data processing system resource influencing devices.

(1) For a person who commits the illegal manufacture, adaptation for utilization, disposal, distribution, obtaining, movement, or storage of such tool (device, software, computer password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for the purpose of committing a criminal offence, the applicable punishment is the deprivation of liberty for a period of up to two years or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

In Latvia, the distribution of these malicious devices is strictly forbidden, and legal responsibility is incurred for engaging in the mentioned activities, regardless of whether they have resulted in any specific harm to the victim. The section's list of hazardous devices is unquestionably incomplete. Therefore, when adopting this section, the Committee of Cybercrime Experts of the Council of Europe discussed the content of objects that are prohibited from being circulated. Human rights organizations argued that the broad term "misuse of devices", referred to as "hacker tools" in the ER CC, contradicts the principle of clarity of norms, as analysed in Chapter 1 of the study and in Paragraph 18.1 of the judgment of the Constitutional Court in Case No. 2018-10-0103. In this case, the court concluded that "The legislator may use a general term for a specific type of device, rather than listing the specific names and models of devices". Therefore, the term "device" used in the Article assesses the clarity of the law and should be interpreted in the context of the Criminal Law provision being contested. The section does not hold accountability for the dissemination of any device, software, or data that may impact ADPS resources. However, it does hold culpability for the dissemination of devices that are specifically developed or altered with the intention of illegally influencing ADPS resources.

The second part of the section already provides for liability for causing serious consequences. According to Section 24 of the Law on the Procedures for the Coming into Force and Application of the Criminal Law (1998)

Liability for a criminal offence provided for in the Criminal Law that has caused serious consequences shall apply if the criminal offence has resulted in death of a person, serious bodily injuries to at least one person, moderate bodily injuries to a number of persons have been caused, or property loss which was not less than the total of fifty minimum monthly wages specified in the Republic of Latvia at that time has been inflicted, or other serious harm has been caused to the interests protected by law.

An equivalent criterion of aggravated liability is also provided by the regulation of Sections 241, 243 of the Criminal Law (1998).

Computer-Related Fraud

This offence is commonly known as a quasi-cybercrime, as it involves the use of ADPS. However, it is important to note that similar activities can also be directed towards an individual. Paragraph 86 of the ER CC emphasizes that "these crimes primarily involve input manipulations, where incorrect data is intentionally entered into the computer, or program manipulations and other interferences during data processing". Fraud has traditionally been defined as the act of deceitfully appropriating another person's property (Smith, Wayte & Marindin, 1980). Fraud encompasses a diverse array of forms and techniques, all with the objective of deceiving an individual or ADPS to get financial benefit.

The Convention mandates parties to enact laws that classify conduct as criminal if they result in the outcomes specified in Article 7 of the CC. Nevertheless,

computer fraud has not been explicitly outlawed in all nations. For example, Article 182 “Swindling” of the Republic of Lithuania Criminal Code (2000) states that “A person who, by deceit, acquires another’s property for own benefit or for the benefit of other persons or acquires a property right, avoids a property obligation or annuls it shall be punished”. In its practice, the Lithuanian court applied the precedent doctrine, which gave them the opportunity to broadly interpret the concept of fraud, to apply it both to the fraud of a person and ADPS, thus fulfilling the provisions of Article 7 of the Convention.

The court acted contrary in Latvia, in a case where the alleged perpetrators damaged the cable, “which gave them the opportunity to use paid services, such as phone sex, on their behalf by connecting through the damaged cable to the telephone lines of legitimate users”. As a result, Latt telecom suffered losses in the amount of more than 70,000 lats (equivalent to approximately 100,000 EUR), however, the court acquitted the suspects of fraud, stating that the Criminal Law provides for liability only for defrauding a natural person. The Senate Department of Criminal Cases in case SKK-3 of 2004b upheld this ruling, concluding that “fraud primarily involves manipulating the intentions of a human being, rather than a technological device” (Kinis, 2015).

The Supreme Court also noted that this was not in line with the intention of the legislator, as Section 177 of the Criminal Law imposes liability on individuals who acquire another person’s property or rights to such property through the deliberate use of trust or fraudulent means (see Box 6.6). When comparing the definition of fraud in the Lithuanian Criminal Code with the Criminal Law, there are minimal differences. The Supreme Court of Lithuania has acknowledged that fraud can be committed against a technical device, whereas the Latvian court has taken a more conservative stance, stating that only the legislator has the authority to do so. On 1 July 2005, amendments to the Criminal Law providing for computer fraud entered into force.

Object of offence. This offence is included in Chapter XVIII “Criminal offences against property” of the Criminal Law. This Chapter encompasses all criminal offences specifically aimed at personal property. Consequently, this Chapter encompasses crimes such as theft, robbery, fraud, and so on. Paragraph 88 of the

Box 6.6 Excerpt from Section 177 of the Criminal Law (1998)

Section 177.1 Fraud in an Automated Data Processing System

1) For a person who commits the knowingly entering of false data into an automated data processing system for the acquisition of the property of another person or the rights to such property, or the acquisition of other material benefits, in order to influence the operation of the resources thereof (computer fraud), the applicable punishment is the deprivation of liberty for a period of up to three years or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

ER CC states that individuals will be held accountable for computer fraud manipulations if they cause financial harm to someone else's belongings. The term "loss of property" encompasses the loss of money, material assets, and intangible assets with economic value. Consequently, the scope of safeguarding legitimate interests encompasses any legal relationship pertaining to the pursuit of the victim's economic interests. The target of the offence is ADPS, which primarily serves the purpose of processing data.

Objective side. When assessing the nature of the offence, it is crucial to accurately comprehend the phrase "the intentional insertion of inaccurate information into a computerized data processing system". Articles 8(a) and 8(b) of the CC enumerate many forms of manipulation, including alteration, suppression, and deletion. However, this list is not comprehensive, meaning that computer fraud can employ any method intended to carry out the activities and consequences outlined in the section. The crucial aspect is that the fraudulent act relies on automated data processing and can alone be executed remotely. Hence, actions such as prevalent telephone fraud, investment fraud, and others cannot be classified as computer fraud. If a someone is intentionally deceiving someone by bodily actions, those actions would be considered fraudulent according to Section 177 of the Criminal Law. ADPS fraud encompasses several forms, including as phishing employing diverse techniques, malware, device misuse (including viruses and ransomware), and DDoS attacks. The offence necessitates the presence of tangible outcomes, specifically economic damages. As previously stated, all economic advantages, regardless of their kind or substance, must be encompassed under unlawful economic gain.

Jurisdiction and Criminal Procedure Law

Jurisdiction

Article 22 CC provides that Parties shall establish jurisdiction over any offence established in accordance with the Convention: (1) if they were committed in its territory, (2) on board a ship or an aircraft sailing under or flying the flag of that country, and (4) its national committed the offence outside the territorial jurisdiction of any State. "Criminal legal jurisdiction traditionally refers to jurisdiction to prescribe, jurisdiction to enforce and jurisdiction to adjudicate the territory of the state" (Brenner & Koops, 2004). Nevertheless, most cybercrimes are inherently supranational in nature, meaning they transcend national boundaries and jurisdictions. The Harvard Research Draft Convention on jurisdiction with respect to the crime of 1935 originally incorporated the ideas of territorial, personal, universal, consequence, and defence jurisdiction to enable countries to exercise their legal authority outside their borders (Capps, Evans & Konstadinidis, 2003).

The proposed Convention established five fundamental principles for the establishment of jurisdiction:

- 1 **The territorial principle** refers to the legal concept that a country has jurisdiction over actions and events that occur inside its territory. The notion of geographical jurisdiction is widely regarded as the fundamental basis for criminal

jurisdiction, both in theory and in practice. Parties predominantly adhere to the subjective territorial concept, which pertains to crimes committed inside the borders of a sovereign state. This principle applies to all individuals and entities, whether they are natural or legal persons, as well as to any objects situated within the territory. The principle is encompassed within Section 2 of the Criminal Law (1998), specifically titled “Application of Criminal Law in the territory of Latvia”. This principle is intricately connected to the party’s sovereignty, as emphasized by the ER CC: “Each Party is required to punish the commission of crimes established in this Convention that are committed in its territory” (para 23). Cyber sovereignty pertains to the jurisdiction over the digital realm inside a nation’s geographical boundaries and the underlying infrastructure that constitutes it. Despite the current heated geopolitical environment, international law is primarily based on the principles of state sovereignty and territorial jurisdiction. The territorial principle encompasses the officially recognized territorial boundaries of Latvia, as well as its airspace and marine borders.

- 2 **Objective (expanded) territorial jurisdiction.** If subjective jurisdiction is determined by the connection between the individual and the territory, extended jurisdiction acknowledges a state’s authority to exercise criminal jurisdiction in the following cases: (a) for offences committed by nationals, citizens, non-citizens of the Republic of Latvia, and individuals with a permanent residence permit, outside the state’s territory, and (b) against foreigners for a crime committed within the territory of another state, if significant consequences have taken place within the territory of Latvia.
- 3 **Active personal (nationality) jurisdiction** – nationality is a universally acknowledged standard. In Latvia, the term “Latvian residents” encompasses those who are Latvian citizens, non-citizens, and foreigners with a permanent residency permit in the Republic of Latvia. The principle is applied in cases where the persons have committed a criminal offence provided for in the Special Part of the Criminal Law while being in the territory of another country or in the territory outside of any jurisdiction.
- 4 **Principle of defence or consequences.** The principle is outlined in the third paragraph of Section 4 of the Criminal Law (1998). It pertains to foreigners without permanent residence permits in Latvia who have committed serious or particularly severe crimes in another country, specifically those directed against Latvia. This principle is also referred to as the doctrine of consequences. Parties are entitled to apply it, unless another party, in whose jurisdiction the cybercrime occurred, has already commenced criminal procedures for the specific offence. The principle of the doctrine of consequences is limited to offences that are officially classified as either serious or especially serious according to the Criminal Law. According to Mathias for this jurisdictional basis to be applicable, the implications must be both main and direct (Mathias, 1996). Nevertheless, it is important to acknowledge that there is presently no universally accepted approach for determining the consequences.

- 5 **Passive personal (victims) jurisdiction** – According to Section 4(3) of the Criminal Law (1998), foreigners who do not have permanent residence permits in Latvia and who committed serious or especially serious crimes in the territory of another state which have been directed against the interests of Latvian residents shall be criminally liable in accordance with this law. Therefore, applying this principle, the victim's legal connection with the Latvian state must be determined (citizenship, non-citizen status, or independent resident status). Latvian criminal law mandates the application of protective jurisdiction and jurisdiction of consequences, as stipulated in the Criminal Law, irrespective of whether the activity is criminalized by another Party. We shall further examine the issue of jurisdiction by exploring the regulation of Criminal Procedure Law (2005).

Procedural Law

Article 14 CC provides that “Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings”, this covers procedural matters for obtaining evidence in the cases, when ADPS was used to commit a criminal offence. The procedures encompass “Expedited preservation of stored computer data”, “Expedited preservation and partial disclosure of traffic data”, “Real time collection on traffic data”, “Interception of content data”, and “Search and seizure of stored computer data”. The parties are not restricted by these measures when it comes to deciding on additional procedural steps that are required for the gathering and handling of electronic evidence. As part of the study, we will examine Sections 136, 192, 193, and 219 of the Criminal Procedure Law (2005), which specifically pertain to the obtaining and application of electronic evidence in criminal cases.

According to Section 136 of the Criminal Procedure Law (*Kriminālprocesa likuma komentāri A daļa*, 2019), the term “electronic evidence” includes: “any information regarding facts in the form of electronic information that has been processed, stored, or broadcast with automated data processing devices or systems”. The commentary to the section analyses terms such as ADPS, a complex of computer systems, electronic networks, technical and information resources that have a user access and data storage function. Unlike ADPS within the meaning of the Criminal Law, the scope here is more extensive, encompassing any technical device that performs data processing and storing functions, even if data processing is not its primary function. For instance, the automobile's central computer system, as well as gadgets linked to the Internet of Things, among others. Section 180 of the Criminal Procedure Law regulates the process of search and seizure. However, this section does not specifically highlight the aspects of search related to obtaining electronic evidence, as those have been thoroughly examined in Section 219 of the Criminal Procedure Law.

Box 6.7 Excerpt from Section 191 of the Criminal Procedure Law (2005)

Section 191. Storage of Data located in an Electronic Information System

(1) The person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system.

This section contains the provisions of Article 16 CC, which pertains to the prompt preservation of stored computer data. The primary purpose of this instrument is to facilitate the expeditious storing of specific categories of data, such as traffic data. Section 191 (Box 6.7) governs the preservation of two types of data: (1) data stored in the system pertaining to a particular criminal investigation, which must be retained for a maximum of 30 days and can only be prolonged with the authorization of the investigating judge and (2) storage of traffic and location data. In the first scenario, the responsibility for maintaining the accuracy of data lies with the owner or legal possessor of the system where the data is stored. If requested by law enforcement or a prosecutor, they must ensure the integrity of the data. However, in the second scenario, the obligation to ensure data integrity falls upon public electronic communications service providers, as mandated by the Law.

Section 1(54) of the Electronic Communications Law (2022) defines stored data as “the traffic data referred to in Sections 100 and 101 of this law, means – any information or data which is processed in order to transmit information by an electronic communications network or to prepare accounts and register payments, except the content of transmitted information”. According to Section 99 of the Electronic Communications Law, data that is stored must be kept for a period of 18 months and shared with pre-trial investigation institutions, operational activity subjects, state security institutions, the prosecution office, and the court. This is done to ensure the security of the state and the society, as well as to facilitate the prevention, detection, and investigation of criminal offences, criminal prosecution, and the trial of criminal cases. The Law mandates the service provider to guarantee the preservation of data and forbids the divulgence of any information pertaining to the transmission of said data. On the other hand, Article 192 of the Criminal Procedure Law (2005) determines the procedure by which the stored data can be disclosed and used in criminal proceedings. It can be done upon the request of the investigator who has sanction of a prosecutor or data subject, but in the court investigation – upon the request of a judge.

The Criminal Procedure Law encompasses not only conventional procedural mechanisms like search and seizure or witness questioning, confrontation, etc., but also encompasses activities performed as Special Investigative Actions. According to Section 210(1) of the Criminal Procedure Law (2005), the special investigative actions outlined in this Chapter will be conducted when it is necessary to gather information about facts relevant to the criminal proceedings without notifying the individuals involved in the proceedings or those who may have the information. These activities are authorized for the investigation of crimes of varying severity, including less serious, serious, and especially serious offences. Evidence derived from specialized investigative operations is deemed acceptable in a particular criminal case. A tool commonly used for covertly gathering electronic evidence is described in Section 219 “Control of Data Located in an Automated Data Processing System”:

(1) The search of an automated data processing system (a part thereof), the data accumulated therein, the data environment, and the access thereto, as well as the its removal without the knowledge of the owner, possessor, or maintainer of such system or data shall be performed, on the basis of a decision of an investigating judge, if there are grounds to believe that the information in the specific system may contain information regarding facts included in circumstances to be proven.

This section defines the objectives of the activities outlined in Article 19 of the CC, specifically related to “Search and seizure”. The Annotation to draft to Section 219 of the Criminal Law (Anotācija Nr. 21-TA-1730, 2022) explains that the control of data stored in an automatic data processing system is essentially the same as conducting a search, with the only distinction being the setting in which it occurs. Law enforcement with authorization have the right to carry out certain investigative operations throughout the whole area of the Republic of Latvia, regardless of the number and location of the systems under surveillance, based on a single decision made by the investigating judge. Nevertheless, with the advancement of technology, it is a reality that most criminal offences include the processing of ADPS situated beyond the borders of the country, either directly or indirectly. In 2020, the State Police requested the Ministry of Justice to prepare amendments to the part one of the section to remove from the text the clause stating that “control is only possible in the territory of the Republic of Latvia”. This proposal aimed to eliminate the provision of subjective territorial jurisdiction from the Criminal Procedure Law (2005). “Consequently, the police would gain the legal authority to access, control, and copy information from and on ADPS located globally” (Kīnis & Sinkevičs, 2021). Nevertheless, such approach would contradict with Article 19 CC, which stipulates that searches are permissible only within systems located within the national area.

The Tallinn Manual (Smitt, 2017) acknowledges that parties possess the right to conduct operations in cyberspace beyond their borders, provided they adhere to international law. Within the realm of cyber operations, any action carried out by one state against individuals or entities situated within the borders of another state

without their consent shall be considered a breach of territorial sovereignty. Moreover, Article 31 of the Convention explicitly states that if parties need to obtain computer data stored in another country, they must follow the procedures for international cooperation in criminal cases. This includes providing a justification for the need and specifying which instruments of international cooperation they are requesting to use.

For purpose to access this proposal, the Ministry of Justice carried out a survey of EU Member States (Legicoop, 2020) on whether such amendments could be made to the law. Responses were obtained from 15 EU Member States. The majority argued that procedural regulations did not encompass the right to conduct searches of ADPS located within the jurisdiction of a foreign country. Nevertheless, Spain, Romania, Portugal, the Netherlands, and Estonia expressed that the data may be retrieved if the ADPS were situated beyond any specific jurisdiction. The experts of the drafting group therefore agreed on the need to draft a new paragraph 2.¹ and implementing the measures outlined in the initial portion of Section 219 of the Criminal Procedure Law (2005) to systems that exist beyond the jurisdiction of any other nation. This refers specifically to systems that employ encrypted resources, making it impossible to ascertain their national origin and location through conventional means. So, legislator amended this law with the following wording:

where data are stored in an information system located outside the jurisdiction of any state which may be accessed with authorisation using the system referred to in the decision of the investigating judge, no new decision shall be required. If the jurisdiction of the information system is ascertained during criminal proceedings, the process officer shall contact the state in whose jurisdiction the information system is located in accordance with the procedures laid down in Chapters 83 and 83.1 of the Criminal Procedure Law.

In the ex-ante assessment of the law (Anotācija Nr. 21-TA-1730, 2022), the Ministry of Justice indicated that this instrument would be applicable in cases where encrypted ADPS resources operating, for example, in the dark net, and the location of which cannot be determined by using the internet domain name system or ordinary internet browsers. Moreover, the regulation establishes an obligation,

if the territorial affiliation of ADPS to another state is determined during the investigation, then the process officer must contact the officials of the relevant state and act with accordance to the procedures laid down in Chapters 83 and 83.¹ of the Criminal Procedure Law.

The third paragraph of that section mandates the owner of the ADPS under investigation to uphold the integrity of the system's resources and to provide a caution against the concealment of the inquiry's confidential information. Consequently, the lawmaker has achieved a certain equilibrium between the provisions of the Cybercrime Convention and the interests of the State to enhance the effectiveness of combating cybercrime.

Problems with the Application of Criminal Legal Regulation

The Eurobarometer survey conducted in 2020 (Eurobarometer, 2020) revealed that 26% of Latvian internet users experienced fraudulent e-mails and phone messages requesting sensitive banking and personal information. Additionally, 25% of computers were infected with harmful devices, 11% fell victim to online fraud, 13% had their social media accounts hacked, and data stolen or deleted, 8% encountered cyberattacks that denied access to banking or public administration services, 4% made payments in connection with a ransomware attack, and 6% reported incidents of identity theft. It is important to note that the Criminal Law does not specifically address digital identity theft, as such offences are classified as computer fraud.

According to pool conducted by Norstat 2021 on behalf of Cyber Incident Response Institution (CERT.LV), 28% of respondents in Latvia acknowledged experiencing cyberattacks on at least one occasion. Considering the quantity of internet users in Latvia, surpassing 1.5 million IP addresses, it can be inferred that, on average, 420,000 IP addresses were vulnerable to potential dangers in 2021. The report published by CERT.LV in 2023 (CERT.LV, 2023) reveals that a staggering number of over 350,000 incidents were recorded during the fourth quarter of that year. Among these, 2,321 incidents were classified as significant threats with a moderate impact on the commercial or state and local government sectors, while 96 incidents were deemed significant threats, and two cases were classified as high-level threats. The other instances are deemed insignificant.

Based on these numbers, it may be presumed that almost 2,000 criminal processes should have been launched. According to statistics provided by Information Centre of the Ministry of the Interior (2024) during the 2021–2023 period, cases of computer fraud (Article 177-1 of the Criminal Law) and offences related to hindering of systems and data (Article 243 of the Criminal Law) have been registered. On the other hand, no cases have been initiated for arbitrary access (Article 241), and only a few cases have been registered for illegal interception (Article 144, Part 2), and use of illegal devices (Article 244) (see Table 6.1).

However, it must be noted that the number of victims who file a complaint with the police does not result in a fair and lawful resolution, as court data reveal (Court administration, 2023), from 2020 to the fourth quarter of 2023, a total of five criminal cases, including those in the appeals courts, were successfully adjudicated. These include one case of arbitrary access (as defined in Article 241 of the Criminal Law), one case of data damage (as defined in Article 243), one case of illegal use of equipment (as defined in Article 244), and one case related to Article 5. There are, of course, both objective reasons, such as the inability to discover the location of the guilty person, to obtain evidence, but there are still many subjective factors that prevent a fair and legal solution in criminal proceedings. As court statistics show, a stable jurisprudence on cybercrimes has not yet been established in Latvian courts. Several reasons can be cited as the cause, both the above-mentioned discussion on the jurisdiction of the investigation of the crime, as well as the very conservative approach to the interpretation of the norms of the Criminal Law in connection with the clarification of the content of substantial damage as a prerequisite for liability.

Table 6.1 Registered criminal cases from 2021 to 2023 (Ministry of the Interior, 2024)

| <i>Criminal Law Sections</i> | <i>2021</i> | <i>2022</i> | <i>2023</i> |
|------------------------------|-------------|-------------|-------------|
| 177-1 | 47 | 0 | 73 |
| 241 | 3 | 0 | 0 |
| 243 | 6 | 34 | 3 |
| 244 | 0 | 0 | 4 |
| 144 | 0 | 1 | 1 |

In respect of Section 177.1 of the Criminal Law (1998) “Computer Fraud”, an average of 40 applications per year were registered from 2010 to 2014, but most offences were related to fraud used in slot machines by throwing into them either tokens or Hungarian forints instead of 1 lats coin, as their weight was the same as the weight of 1 lats coin and thus the person had the opportunity to receive services. Such juridical practice started from 2009 and lasted until 2014. Cybercrime experts strongly criticized this practice in scientific publications and conferences, as well as when providing trainings for judges on the nature of CC. As a result, it bore fruit as the Senate of the Supreme Court reversed the ruling and changed the case law. Namely, the Senate in the case SKK-349/2014, concluded that the act of a person throwing tokens or a coin that does not correspond to the value of the currency into a gaming machine does not create the objective side of computer fraud, since this act can only be performed by processing automated data, therefore the person’s actions were reclassified as theft (Senāts, 2014). This demonstrates how subjective barriers to a just and lawful outcome in criminal processes can be eliminated when legal scientists collaborate with judges, prosecutors, and police officers at all levels.

However, Latvia hasn’t had much success in prosecuting people for offences against ISS. There are a few obstacles, including the difficulties in locating the offender and the restrictions placed on foreign legal assistance mechanisms in criminal law, which make it impossible to obtain data from systems situated abroad. However, this is a unique feature of Latvia’s criminal justice system, and we shall explore this further. It has already been stated above that one of the reasons why we are not successful in investigating cybercrimes is the problem of application and estimation of mandatory feature – substantial harm in cybercrimes. The matter was extensively discussed upon during the International Conference organized by the Faculty of Law at Riga Stradiņš University, focusing on “Substantial Harm in Latvian Criminal Law and its Implications on the Right to a Fair Trial” (2022). The conference was attended by various entities, including the Ombudsman’s Office, the Data State Inspectorate, the Environmental State Inspectorate, responsible officials, judges, prosecutors, lawyers, police officers, and specialists who regularly encounter the issue of determining significant harm, particularly in the realm of cybercrime. The State Police or the Prosecution Office cease proceedings due to the inability to establish the causal effects of the objective aspect of the criminal offence – significant harm. The legal definition of substantial harm is outlined in Section 23 of the Law on the Procedures for the Coming into Force and Application of the Criminal Law (1998).

Box 6.8 Excerpt from Section 23(1) of the Law on the Procedures for Coming into Force and Application of the Criminal Law (1998)

Section 23(1) Liability for a criminal offence provided for in the Criminal Law causing substantial harm shall apply if due to the criminal offence any of the following consequences have set in:

- 1 property loss has been suffered which at the time of committing the criminal offence has not been less than the total of five minimum monthly wages specified in the Republic of Latvia at that time, and other interests protected by law have been threatened.
- 2 property loss has been suffered which at the time of committing the criminal offence has not been less than the total of ten minimum monthly wages specified in the Republic of Latvia at that time.
- 3 other interests protected by law have been significantly threatened.

The participants of the conference acknowledged that there are problems in the application of points 1 and 3 of the first paragraph of that section (Box 6.8). This is because, in order to meet the requirement of substantial harm, it is necessary to provide evidence that the interests of the individual in question have been violated. During a conference, Dr. D. Hamkova, who was leading expert on the Supreme Court's "Report on Generalization of juridical practice in criminal cases related with estimation of substantial harm" (Hamkova, Latvijas Republikas Augstākās tiesas Senāts, 2017), mentioned that despite the passage of over five years since the compilation and conclusions of the Senate, the interpretation of the term "other interests" still varies in practical application. The author identifies the problem as originating from the Senate's conclusion in paragraph 11, which states that "to define substantial harm, it is crucial to specify the specific legally protected interests that have been endangered and how the threat to other legally protected interests has been specifically demonstrated". Furthermore, paragraph 11.1 of the Senate's conclusion states that

if a provision in the Special Part of the Criminal Law suggests that significant harm may be inflicted upon the interests of a legally protected individual, it is necessary to specify the particular person whose interests have been severely harmed, identify the legal enactment that safeguards that interest, and describe the precise manner in which the harm to that interest has occurred.

When evaluating these findings in relation to Sections 241–243 of the Criminal Law, it is important to acknowledge that practical enforcement is not always feasible, as the lawful interest of an individual is not consistently explicitly defined. In contrast, the civil law domain in which most ADPS function permits any action

that is not explicitly forbidden by law. Each of these actions is associated with the lawful interest of an individual, which may not always be justified by a particular statute. Cyber threats can result in both financial and non-financial effects, including reputational risks and potential commercial concerns that might impact an entrepreneur's profitability. Nevertheless, the Latvian courts do not acknowledge unearned profit as a form of financial loss.

The author suggests that the criteria for evaluating significant damage should be clarified, considering the practices of other States like Germany, Estonia, and Lithuania. This entails specifying in the relevant sections of the Criminal Law that the threshold for substantial harm is met when the damage exceeds EUR 4,000. Alternatively, there could be a shift toward using an algorithmic method to assess significant damage, which is already partly covered in the Cabinet Regulation No.15 (2019). In order to determine substantial harm in criminal proceedings, a proposed algorithm based on four criteria has been suggested (Kīnis & Sinkevičs, 2022). These criteria include: (1) the time criterion, which considers the duration of service within a specific time frame; (2) criteria for assessing financial loss, which considers verifiable losses supported by accounting records, such as downtime and lost profits; and (3) evaluation of non-financial losses, based on the social role fulfilled by the relevant ADPS. In addition, when evaluating the factor of social significance, it is crucial to consider the subjective viewpoint of the victim, as they alone possess the genuine worth of their data. Lastly, the criterion of the intent behind the offence should be considered, specifically whether the offence was aimed at causing harm to other lawful interests, such as the commission of another offence. Therefore, it is worth to evaluate if the motive behind the offence is connected to safeguarding other essential rights established in the Constitution, which are unrelated to the specific nature of the criminal act.

Conclusion

To summarize this chapter, it should be noted that the Latvian doctrine and practice of criminal law are constantly developing, and the problems described above are closely examined by criminal law experts, law policymakers, and legislators. There is continuous training of staff at all levels. However, the effectiveness of the police will mostly rely on their level of technical proficiency and legal knowledge. While investigating cybercrime, it is important to note that simply being able to identify the prohibited activity and the alleged perpetrator does not automatically guarantee holding that person criminally liable. Section 92 of the Constitution states that "everyone is considered innocent until his guilt is recognized in accordance with the law". An integral part of this right is the basis of criminal prosecution, which ensures a person's fundamental right to a fair trial. Because the fundamental principle of Latvian criminal law underlines that person can only be held criminally liable if all the necessary elements of the criminal offence have been established. However, the above-mentioned also proves that the legislator, by defining substantial damage as the minimum threshold for criminal liability, did not find a correct balance between the rights of the victim and the suspect to fair trial in criminal law.

Consequently, how well Latvia can defend its citizens' legal interests in cyberspace will depend on how high this criminal responsibility threshold is set in the future.

References

- Anotācija Nr. 21-TA-1730. (2022, 01 28). Saeima. Retrieved from <https://titania.saeima.lv/LIVS13/SaeimaLIVS13.nsf/0/1493B4CCDCBD851EC22587DB0029DF4D?OpenDocumentB>
- Brenner, S., & Kooops, B. (2004). Approaches to cybercrime jurisdiction. *Suffolk University Journal of High Technology Law*. Retrieved 12 3, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507#
- Cabinet Regulation No. 15. (2019, 01 15). *Regulations Regarding the Security Incident Relevance Criteria, Reporting Procedures, and Content of Reporta*. Retrieved from <https://likumi.lv/ta/en/en/id/304284>
- Cabinet Regulation No. 442. (2015, 07 28). *Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements*. Retrieved from <https://likumi.lv/ta/en/en/id/275671-procedures-for-the-ensuring-conformity-of-information-and-communication-technologies-systems-to-minimum-security-requirements>
- Capps, P., Evans, M., & Konstadinidis, S. (2003). *Asserting Jurisdiction: International and European Approaches*. xix. Hart Publishing.
- CERT.LV. (2023). *CERT.LV darbības pārskats par 2023. gada 3. ceturksni*. Rīga: CERT. LV. Retrieved 12 5, 2023, from <https://cert.lv/lv/2023/11/cert-lv-darbibas-parskats-par-2023-gada-3-ceturksni>
- Claire-Bazy, M. (2019). *The Role of the Constitutional Courts in the Global World* (pp. 59–67). Rīga: The Constitutional court of the Republic of Latvia. Retrieved from <https://www.satv.tiesa.gov.lv/other/2019-ST-Referati-2018-atverumos.pdf>
- Council of Europe. (2001). Convention on cybercrime. Retrieved from <https://rm.coe.int/1680081561>
- Council of Europe. (2001). *Explanatory report Convention on cybercrime*. Council of Europe. Retrieved from <https://m.coe.int>
- Court Administration. (2023). *Criminalcases related to cybercrimes*. Rīga: unpublished.
- Criminal Law. (1998). <https://likumi.lv/ta/en/en/id/88966>
- Criminal Procedure Law. (2005). <https://likumi.lv/ta/en/en/id/107820>
- Directive 2013/40/EU of the European Parliament and the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. <http://data.europa.eu/eli/dir/2013/40/oj>
- Directive (EU) 2022/2555 of the European Parliament and the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2) <https://eur-lex.europa.eu/eli/dir/2022/2555>
- Electronic Communications Law. (2022). <https://likumi.lv/ta/id/334345>
- Eurobarometer. (2012). *Special Eurobarometer 390: Cybersecurity*. Eurobarometer. Retrieved 12 5, 2023, from https://data.europa.eu/data/datasets/s1058_77_2_ebs390?locale=en
- Eurobarometer. (2020). *Special Eurobarometer 499. Report European's attitudes towards cyber security*. Publication office of European Union. Retrieved 12 4, 2023, from https://data.europa.eu/data/datasets/s2249_92_2_499_eng
- European Convention on human rights. (1950). Council of Europe. Retrieved from https://www.echr.coe.int/documents/d/echr/convention_ENG

- Farmer, L. (2016). *Making the modern criminal law. Criminalization and civil order*. Oxford university Press.
- Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response, pp. 11–33. <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>
- Hamkova, D. (2017). Tiesu prakse lietās, kurās noziedzīga nodarījuma sastāva pazīme ir būtisks kaitējums. Latvijas Republikas Augstākās tiesas Senāts. <https://www.at.gov.lv/lv/tiesu-prakse/tiesu-prakses-apkopojumi/kriminaltiesibas>
- Information Centre of the Ministry of the Interior. (2024). *Crime Statistics 2021–2023*. Riga. Retrieved 02 10, 2024, from <https://www.ic.iem.gov.lv/lv/kriminala-statistika>
- IR. (2013, 09 16). *Prokuratūra Neo uzrāda apsūdzību*. Retrieved 12 06, 2023 from <https://ir.lv/2013/05/08/prokuratūra-neo-uzrada-apsudzibu/>
- ITU. (2010). *ITU Toolkit for Cybercrime Legislation*. ITU. Retrieved 11 29, 2023, from <https://www.combattingcybercrime.org/files/virtual-library/assessment-tool/itu-toolkit-for-cybercrime-legislation-%28draft%29.pdf>
- Judgment case no. 2018-10-0103, para 18.1 (Constitutional Court of the Republic of Latvia 02 12, 2019). Retrieved from https://www.satv.tiesa.gov.lv/en/wp-content/uploads/sites/2/2019/03/2018-10-0103_PR_par_spriedumu_ENG.pdf
- Judgment in case No 1 BvR 370/07, BvR 595/07 (Bundesfassungsgericht 10 10, 2007). Retrieved 11 30, 2023, from <https://data.guardint.org/en/entity/yulli73nwx?page=2>
- Ķinis, U. (2015). *Kibernoziedzība, kibernoziegumi un jurisdikcija*. Riga: Jumava.
- Ķinis, U. (Ed.) (2022). *Introduction to Information Society Law*. Riga: Rīga Stradiņš University.
- Ķinis, U., & Sinkevičs, Ņ. (2021). Automatizētās datu apstrādes sistēmā esošu datu kontrole. *Socrates*, 1(9), 90–106. <https://www.researchgate.net/publication/351639688>
- Ķinis, U., & Sinkevičs, Ņ. (2022). Algoritms kā būtiska kaitējuma noteikšanas metode noziedzīgos nodarījumos, kas saistīti ar automatizētu datu apstrādes sistēmu (ADAS). *Socrates*, Nr 2(23), 61–80. <https://www.researchgate.net/publication/364510089>
- Kriminālprocesa likuma komentāri A daļa. (2019). 459–460. Latvijas Vēstnesis.
- Latvijas Kriminālkodekss. (1961). Retrieved from <https://likumi.lv/ta/id/318953-latvijas-kriminalkodekss>
- Latvijas Republikas Augstākā tiesa, SKK-B/2022; ECLI:LV:AT2022[...] (Latvijas Republikas Augstākā tiesa Senāts 2022). Retrieved 12 05, 2023, from <https://www.at.gov.lv/lv/tiesu-prakse/judikaturas-nolemumu-arhivs/kriminallietu-departaments/hronologiska-seciiba?lawfilter=0&year=2022>
- Latvijas Republikas Satversme. (1922). Latvijas Vēstnesis. <https://likumi.lv/ta/en/en/id/57980>
- Latvijas Satversmes Tiesa. (2014). The Constitutional Court of the Republic of Latvia Judgment in case No. 2013–05–01, para 15. Retrieved from https://www.satv.tiesa.gov.lv/wp-content/uploads/2013/03/2013-05-01_Spriedums_ENG.pdf
- Information Technology Security Law. (2010). Retrieved from <https://likumi.lv/ta/en/en/id/220962>.
- Legicoop. (2020). *The network for legislative cooperation between the ministries of Justice of the European Union*. Retrieved from <https://intra.legicoop.eu/lv/user/login>
- Marčinauskaite, R. (2013). Doctoral dissertation. *Criminal offences against the confidentiality of electronic data and information systems (Criminal code of the Republic of Lithuania Articles 198 and 198(1))*, 208–213. Vilnius.
- Mathias, E. b. (Ed.). (1996). *External jurisdiction in theory and practice*. Kluwer law international.
- National Cybersecurity Law. (2024). <https://likumi.lv/ta/id/353390>

- Official Statistics Portal. (2022, November 4). *The share of regular internet users has reached 90%*. <https://stat.gov.lv/en/statistics-themes/information-technologies/ict-households/press-releases/8195-internet-usage>
- On the Procedures for the Coming into Force and Application of the Criminal Law. (1998, 10 15). *Law*. Retrieved from <https://likumi.lv/ta/en/en/id/50539>
- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). (2022). Retrieved from <https://eur-lex.europa.eu/EN/legal-content/summary/digital-services-act.html>
- Republic of Lithuania Criminal Code. (2000, 09 26). Retrieved 12 20 2023, from <https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=rivwzvvpvg&documentId=a84fa232877611e5bca4ce385a9b7048&category=TAD>
- Rosen, J., & Wittes, B. (2011). *Constitution 3.0 Freedom and technology challenge*. The Brookings Institution.
- Senāts (2014). Krimināllikuma 177.1 pantā paredzētā noziedzīgā nodarījuma sastāva objektīvā puse, SKK -349/2014 (Latvijas Republikas Augstākā tiesa Senāts 08 27, 2014). Retrieved 12 05, 2023, from <https://www.at.gov.lv/lv/tiesu-prakse/judikaturas-nolemumu-arhivs/kriminallietu-departaments/hronologiska-seciba?lawfilter=0&year=2014>
- Smith, W., Wayte, W., & Marindin, G. E. (Eds). (1980). *A dictionary of Greek and Roman Antiquities*. Retrieved from <https://www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.04.0063:entry=falsum-cn>
- Smitt, N. (Ed.). (2017). *Tallinn Manual 2.0*. Cambridge University Press.
- Substantial harm in criminal right to fair trial. (2022, 09 23). *Conference video*. Riga, Latvia. Retrieved 12 5, 2023, from <https://www.rsu.lv/aktualitates/aizvadita-konference-butiskais-kaitejums-kriminallikuma-v-tiesibas-uz-taisnigu-tiesu>
- UNODC. (2013). *Comprehensive study on cybercrime, p. ix*. Retrieved 11 20, 2023, from UNODC: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- Yar, M., & Steinmetz, K. F. (2024). *Cybercrime and Society*. (4th ed.). Sage.

7 Latvia in the European Cybersecurity Ecosystem

Mihails Potapovs and Stella Blumfelde

Introduction

Cybersecurity governance in the European Union (EU) reflects the complex interplay between national sovereignty and supranational integration. While all EU Member States are obligated to align their national policies with EU cybersecurity legislation, the degree and manner of implementation vary based on national priorities and security contexts. Latvia's approach to cybersecurity governance is shaped not only by its legal obligations under the EU framework but also by its geopolitical position and evolving threat landscape.

As a relatively small yet distinctly pro-European nation, Latvia has been a vocal advocate for deeper integration in security and defence policy. Public sentiment strongly supports this direction, with 83% of Latvians endorsing a common defence and security policy among EU Member States (Eurostat, 2024). However, Latvia's security environment is uniquely complex. Even before Russia's full-scale war of aggression against Ukraine, Latvia faced significant hybrid threats, particularly in the cyber domain, where the risk of foreign interference has remained persistently high. This volatile landscape has reinforced the Baltic country's commitment to strengthening its cybersecurity posture through collaboration with allies and international partners.

The EU plays a pivotal role in facilitating Latvia's cybersecurity efforts, particularly through legislative harmonisation, cross-border information sharing, and collective capacity-building initiatives. Latvia prioritises swift and efficient information exchange, joint training exercises, and operational coordination as core elements of its cybersecurity strategy. These priorities align closely with EU-wide initiatives, where regulatory and policy frameworks serve as the foundation for a more resilient European digital space.

This chapter examines Latvia's engagement within the EU cybersecurity ecosystem by integrating international relations (IR) perspectives with empirical analysis of legislative and policy developments. The discussion situates Latvia's cybersecurity approach within the broader tension between national sovereignty and European integration, exploring how regulatory compliance, strategic cooperation, and digital sovereignty coexist within the EU framework. The analysis proceeds with an overview of key stakeholders and institutional mechanisms

within the EU cybersecurity landscape. It then evaluates Latvia's contributions and alignments across the core cyber policy dimensions. Through this lens, this chapter highlights Latvia's role in the European cybersecurity ecosystem.

National and Collective Security in the Digital Age

IR studies have traditionally emphasised state sovereignty, framing states as the primary actors responsible for maintaining national security within their borders and in their international engagements. Sovereignty entails a state's authority to govern itself independently – managing its territory, population, and resources, as well as enforcing laws, regulations, and foreign policy without external interference (Kennedy, 1989; Mearsheimer, 2001; Waltz, 1979). However, the emergence of the digital domain challenges these traditional notions of sovereignty due to its inherently borderless nature and complex regulatory landscape (Deibert & Rohozinski, 2010; Kello, 2013). In cybersecurity, while governments remain central to policy formulation and regulation, the decentralised nature of cyberspace prevents any single actor from exerting complete control over the digital ecosystem (Clarke & Knake, 2011).

Although Article 4(2) of the Maastricht Treaty states that “national security remains the sole responsibility of each Member State” (Consolidated Version of the Treaty on European Union, 2012), the cyber domain has increasingly become regulated at the EU level due to the “spillover” effect from common market regulations. Initially, the EU's focus was on regulating specific services to facilitate their inclusion in the common market. However, as cyberattacks demonstrated vulnerabilities in the shared market infrastructure, the EU shifted towards a more integrated regulatory approach. This transition, driven by deeper European integration and the pursuit of a closer Union, has positioned cybersecurity as a key area of EU governance.

From a collective security perspective, IR literature suggests that states can enhance their security by cooperating with others to address common threats (Deutsch, 2006; Walt, 1991). The EU has embraced this principle, implementing collective security measures that require Member States to align with EU regulations and collaborate on cybersecurity initiatives to mitigate shared risks (Haas, 2004; Keohane, 1984). The EU's cybersecurity approach acknowledges that no Member State can fully address cyber threats alone, thus advocating for collective action (Carrapico & Barrinha, 2017).

Furthermore, digital sovereignty – the control over digital resources and data privacy – has become increasingly significant for national security and economic interests (Budnitsky & Jia, 2018; Couture & Toupin, 2019; European External Action Service, 2022; Klossa, 2019; Timmers, 2018). This reflects a broader trend in collective security, where national efforts to regulate the digital environment underscore the necessity of European-level cooperation to protect EU values, critical infrastructure, and the digital market (Council of the European Union, 2020; Floridi, 2020; Pohle & Thiel, 2020; von der Leyen, 2020).

To ensure a secure and resilient digital environment, the EU has implemented various regulations aimed at enhancing the resilience and incident response

capabilities of essential services and digital service providers (ENISA, 2017; Juncker, 2018; Li et al., 2019; Madiaga, 2020). These regulations form part of a broader collective security strategy, framing cybersecurity as essential for European sovereignty and the integrity of the EU integration project (Baldini et al., 2020; Bellanova et al., 2022; von der Leyen, 2019). This collective approach aligns with the EU's integration process, characterised by the pooling or sharing of sovereignty to address challenges more effectively through common institutions and regulations (Howorth, 2014; MacCormick, 1999; Moravcsik, 1998; Sandholtz & Stone Sweet, 1998; Wallace, 1999).

The balance between national sovereignty and collective security within the EU's cybersecurity framework remains a critical issue. While integration strengthens the EU's global role, it also raises concerns about the erosion of national control over defence matters. Differences in strategic culture, cybersecurity capabilities, and resources among Member States further complicate efforts to harmonise security and defence initiatives across the EU (Biscop, 2016; Christou, 2016; European Defence Agency, 2021; Menon, 2011). Latvia's alignment with the EU's cybersecurity framework illustrates this dynamic balance, demonstrating how national and supranational interests interact within the evolving European cybersecurity ecosystem.

The EU Cybersecurity Ecosystem

The EU cybersecurity ecosystem is complex, involving numerous stakeholders and cooperation formats. It is a robust framework essential for enhancing the resilience of the EU and its Member States against an increasingly sophisticated array of cyber threats. This ecosystem is defined by a collaborative approach, with various EU institutions, agencies, and networks working together to strengthen the cybersecurity capabilities of both individual Member States and the EU as a whole.

While the roles of core EU institutions – namely the European Parliament, the Council of the EU, and the European Commission – are well established, particularly in the context of the legislative process through mechanisms such as the ordinary legislative procedure, trialogues, and comitology, the cybersecurity ecosystem extends well beyond legislation. It encompasses such dimensions as policy and legislation, capacity-building, cyber incident response, cyber diplomacy, cyber defence, and law enforcement (see Figure 7.1). Moreover, EU cybersecurity policy intersects with sectoral legislation in areas such as banking, electronic communications, and critical infrastructure protection, which, while relevant, fall outside the scope of this study, which focuses on core cybersecurity policy domains.

The European Union Agency for Cybersecurity (ENISA) plays a central role in developing and implementing EU cybersecurity policies (Bederna & Rajnai, 2022). It provides expert advice to the European Commission and Member States, supporting the formulation and enforcement of key legislative frameworks such as the Network and Information Security (NIS) Directive (2016/1148) and the Cybersecurity Act, which are fundamental to the EU's cybersecurity strategy (Christou, 2016). Beyond policy development, ENISA engages in capacity-building activities,

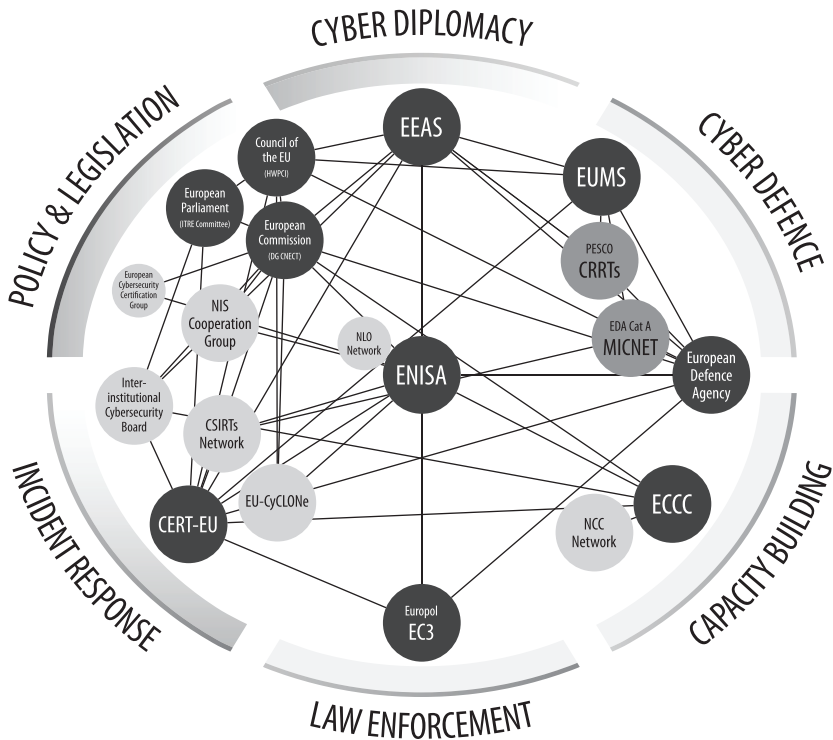


Figure 7.1 A conceptual model of a fragment of the EU cybersecurity ecosystem. Darker nodes represent structures, lighter nodes represent networks, and medium nodes represent projects.

offering training programs, workshops, and exercises to enhance Member States’ incident response mechanisms and crisis management capabilities (ENISA, 2024).

Additionally, ENISA manages the EU-wide cybersecurity certification framework, ensuring high security standards for ICT products and services (European Parliament & Council of the EU, 2019). It also monitors emerging cyber threats and facilitates information sharing through collaborative formats such as the European Cybersecurity Certification Group (ECCG) and the Computer Security Incident Response Teams (CSIRTs) Network (ENISA, 2023). ENISA further coordinates the National Liaison Officers (NLO) Network, which ensures the synchronisation of cybersecurity policies across Member States. The NIS Cooperation Group, established under the NIS Directive and supported by ENISA and the European Commission, fosters coordination among Member States on legislative implementation issues.

The European Commission, particularly its Directorate-General for Communications Networks, Content and Technology (DG CNECT), complements ENISA’s efforts by proposing and enforcing cybersecurity legislation, ensuring its consistent implementation across Member States (Carrapico & Barrinha, 2017;

European Commission, 2020). The Commission also funds cybersecurity research and innovation through initiatives such as Horizon Europe and the Digital Europe Programme, which are crucial for developing new cybersecurity technologies and solutions. Additionally, the Commission facilitates collaboration between Member States and EU institutions through expert working groups that address cybersecurity challenges.

The recently established European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and its associated National Coordination Centres (NCCs) play a critical role in strengthening the EU's cybersecurity capabilities. The ECCC is responsible for implementing the EU's cybersecurity research agenda and managing investments in cybersecurity innovations, ensuring that the EU remains at the forefront of technological advancements. Following its transition to financial autonomy, the ECCC has assumed the management of funding programs previously overseen by the European Commission. The ECCC also collaborates with NCCs in each Member State to facilitate resource allocation and knowledge dissemination, ensuring broad participation in EU-wide cybersecurity initiatives. The NCC network serves as a bridge between the ECCC and national cybersecurity efforts, aligning local and regional strategies with broader EU goals, fostering cross-border cooperation, and ensuring a cohesive cybersecurity approach across the Union.

The Computer Security Incident Response Teams (CSIRTs) Network, established under the NIS Directive and supported by ENISA, enhances cooperation and information sharing among national CSIRTs. It facilitates the exchange of threat intelligence, such as indicators of compromise, and improves Member States' ability to respond to cross-border cyber incidents. A more recent initiative designed to coordinate responses to large-scale incidents and crises at the executive level is the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe). This format enhances crisis management by ensuring rapid coordination and mutual assistance among Member States.

CERT-EU, the CSIRT for EU institutions, bodies, and agencies, is responsible for cyber incident response within the EU structures. It works closely with ENISA and national CSIRTs to strengthen cybersecurity across the EU's institutional framework. In 2024, an Interinstitutional Cybersecurity Board was established to oversee CERT-EU's operations and ensure the cybersecurity of EU institutions. Currently chaired by the European Parliament, this board provides a framework for structured coordination and oversight.

Cyber diplomacy and cyber defence fall within the EU's Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP). The European External Action Service (EEAS) plays a pivotal role in cyber diplomacy, coordinating Member States' efforts and implementing initiatives such as the Strategic Compass for Security and Defence, which includes measures for confidence-building and collective cybersecurity resilience. The Horizontal Working Party on Cyber Issues (HWPCI) within the Council of the EU is an important forum for both legislative discussions and broader cyber diplomacy coordination.

The European Defence Agency (EDA) supports cyber defence capacity-building within the EU, notably by facilitating defence-oriented projects such as

the MICNET Category A project, which establishes a cooperation network for Member States' military CSIRTs. Additionally, the EDA supports the implementation of PESCO projects, including the Cyber Rapid Reaction Teams and Mutual Assistance in Cyberspace (CRRTs) initiative. This project enables Member States to provide mutual support in the event of a large-scale cybersecurity incident or crisis, as well as contribute cybersecurity capabilities to EU missions and operations.

The European Cybercrime Centre (EC3) at Europol plays a key role in combating cybercrime across the EU by assisting national law enforcement agencies in investigating and dismantling cybercriminal networks. EC3 also facilitates intelligence sharing among Member States and international partners, enhancing collective responses to transnational cyber threats. Additionally, EC3 provides specialised training to law enforcement officers across the EU, equipping them with the skills necessary to effectively combat cybercrime. The EU Agency for Law Enforcement Training (CEPOL) supports these efforts by offering advanced training in cybersecurity and cybercrime investigations, ensuring a high level of expertise within national law enforcement agencies.

Stakeholders in the EU cybersecurity ecosystem actively engage with the private sector through collaborative platforms such as the European Cybersecurity Organisation (ECSO). ECSO is a leading non-governmental organisation (NGO) that brings together industry, academia, and public sector representatives to foster cybersecurity innovation and technological advancement. ECSO also plays a key role in establishing the European cybersecurity competence community in partnership with the ECCC. At the national level, cybersecurity authorities within each Member State implement EU cybersecurity legislation, oversee incident management, and collaborate to ensure effective responses to cyber threats. The authorities also conduct public awareness campaigns to educate citizens and businesses about cybersecurity risks, thereby enhancing overall resilience.

The EU cybersecurity ecosystem is a complex and dynamic network of institutions, agencies, and collaborative platforms, each playing a crucial role in safeguarding Member States against cyber threats. Through legislation, capacity-building, operational support, and public-private partnerships (PPPs), these stakeholders collectively create a cybersecurity resilience framework essential for protecting the EU's digital infrastructure.

Methods and Approach

The study employs a descriptive, qualitative case study research design to examine Latvia's role within the EU cybersecurity ecosystem. The research is structured around a practitioner-centric approach, leveraging the co-author's professional expertise in cybersecurity policymaking within the Latvian Ministry of Defence. This methodological choice allows for an in-depth, contextually rich analysis of Latvia's involvement in EU cybersecurity frameworks, legislative implementation processes, and strategic alignment with EU cybersecurity policies.

Descriptive research aims to systematically document and interpret existing phenomena without introducing external manipulation (Bickman & Rog, 2009).

In public policy studies, descriptive methodologies are particularly valuable for mapping governance structures, policy implementation dynamics, and institutional participation. Given that cybersecurity governance is an evolving and institutionally complex field, descriptive case studies provide clarity regarding the mechanisms through which EU policies shape national cybersecurity frameworks. Qualitative descriptive research involving decision-makers, public servants, and local researchers enables international comparative studies to leverage participants' context-specific knowledge, providing a nuanced understanding of diverse public policy environments (Seixas et al., 2018).

This research focuses on Latvia's engagement within EU cybersecurity governance, analysing its participation in key institutional formats, legislative adaptation, and strategic cybersecurity initiatives. The study draws upon first-hand institutional knowledge, policy documents, and official EU legislative texts. This approach aligns with expert knowledge methodologies, wherein policymakers and practitioners provide unique insights that may not be readily available in published literature. The study is primarily based on public and non-public, policy-relevant knowledge acquired through the author's role within the Ministry of Defence. This is complemented by:

- **Legislative and policy documents:** Analysis of key EU cybersecurity legislation (e.g., NIS2 Directive, Cybersecurity Act) and Latvia's national legislation (e.g., National Cybersecurity Law, secondary legislation).
- **Institutional reports and official communications:** Review of Latvian governmental cybersecurity frameworks (e.g., National Cybersecurity Strategy) and participation records in EU cybersecurity structures such as ENISA, the NIS Cooperation Group, and the European Cybersecurity Competence Centre (ECCC).
- **Comparative internal assessments:** Evaluation of Latvia's progress in implementing EU cybersecurity legislation relative to other Member States, based on informal expert discussions and working group exchanges.

Additionally, institutional theories of European integration (Haas, 2004; Moravcsik, 1998) provide a useful lens to interpret Latvia's role in EU cybersecurity policy-making, highlighting how regulatory compliance, policy convergence, and security cooperation evolve within a multilevel governance system. The study is limited by the reliance on non-public sources and insider knowledge, which may restrict replicability. The authors acknowledge the potential for bias and have taken measures to maintain objectivity by cross-referencing findings with publicly available sources. The practitioner-oriented approach employed in the study ensures a high degree of empirical validity, offering a first-hand perspective on cybersecurity governance.

Latvia in the EU Cybersecurity Ecosystem

While six thematic dimensions of the EU cybersecurity ecosystem were established in the previous sections, the complexity of the ecosystem necessitates a more

focused approach. Therefore, the present analysis concentrates on Latvia's engagement in three key dimensions: (1) policy and legislation, (2) capacity-building, and (3) cyber defence. Additionally, this focus is informed by the structure of the book, as the related domains of cyber incident response, law enforcement, and cyber diplomacy are addressed in Chapters 4, 6, and 8, respectively.

Policy and Legislation

One of the key components of Latvia's National Cybersecurity Strategy (Cabinet of Ministers, 2023) is the transposition of EU cybersecurity legislation into national law, with over three-quarters of the national cyber legislation domain being directly impacted by EU policies. The NIS Directive (2016/1148) has significantly impacted Latvia's institutional framework, which has existed in its current form since 2013 but was reviewed to adapt to the new realities introduced by the Directive. It established baseline cybersecurity requirements and reporting obligations for essential service providers and operators of digital services. The Directive also redefined the roles and responsibilities of CERT.LV and reinforced the role of the Ministry of Defence as the national competent authority overseeing cybersecurity policy and serving as the single point of contact for cybersecurity (Information Technology Security Law, 2010).

The impact of the NIS Directive became even more profound with its revision, initiated by the European Commission in 2021. Recognising that the revised legislation would significantly affect the existing institutional framework and require additional resources, Latvia began reorganising its internal processes in late 2021 and early 2022. In June 2022, the Latvian government adopted a policy paper prepared by the Ministry of Defence (2022), which proposed introducing a semi-centralised cybersecurity governance model, discussed in more detail in Chapter 3 of this book. This model included establishing the National Cybersecurity Centre (NCSC-LV), powered by the Cybersecurity Policy Department of the Ministry of Defence in cooperation with CERT.LV. The NCSC-LV was designated as the single point of contact and the competent national authority for essential and important entities, aligning with the requirements of the revised legislation, the NIS2 Directive (2022/2555), thereby consolidating and strengthening the efforts of CERT.LV and the Ministry of Defence. Additionally, the review of the NIS Directive prompted Latvia to take a more active role in expert discussions, particularly within the HWPCI, as well as in other multilateral formats.

The NIS2 Directive came into force on 16 January 2023. Latvia emerged as one of the pioneers in transposing this legislation, submitting the draft National Cybersecurity Law for public consultation as early as October 2022. Despite facing a complex inter-institutional negotiation process, the Latvian Parliament successfully adopted the National Cybersecurity Law on 20 June 2024. The law came into force on 1 September 2024, more than a month ahead of the NIS2 Directive's transposition deadline, placing Latvia among the forerunners. However, the adoption of related secondary legislation has been lagging due to the large volume of objections and feedback on the draft baseline cybersecurity requirements received

from different public institutions and NGOs. Nonetheless, Latvia's progress in implementing the NIS2 Directive remains significant.

Latvia's proactive approach to cybersecurity is further demonstrated by the inclusion of provisions in the National Cybersecurity Law (2024) that extend beyond the scope of the NIS2 Directive. For instance, the law mandates reporting of even non-significant cyber incidents, reflecting a rigorous approach to incident monitoring. Additionally, Latvia interprets the NIS2 provisions concerning covered entities as broadly as possible, to the extent of practicality. This interpretation includes all public administration entities at the central government level, such as the Parliament, the central bank, courts, universities, and other independent bodies, as well as all municipal councils and local government entities. Furthermore, the law extends its reach to private sector entities not covered by the NIS2 Directive, including operators of education information systems and providers of security services.

Despite Latvia's proactive approach vis-à-vis NIS2, the country falls behind in applying the Cybersecurity Act (2019/881), which came into force in 2019 and while it is true that the Cybersecurity Act makes cybersecurity certification voluntary for the Member States, the certification is becoming mandatory with the Cyber Resilience Act (2024/2847) adopted in 2024. Latvia has yet to establish a national framework for the certification of ICT products, services, and processes in accordance with EU cybersecurity certification schemes. Although experts from the Ministry of Defence and CERT.LV are working on developing the national cybersecurity certification framework, with support from the ECCG, no certification schemes have been implemented as of the time of writing.

While many steps remain in establishing a national cybersecurity certification model, exploring opportunities for PPPs remains crucial, particularly concerning the potential establishment of conformity assessment bodies (CABs). Latvia already has experience with PPPs in regulated ICT areas connected to cybersecurity, such as the qualified electronic identification and trust services, regulated by the Digital Security Supervisory Committee under the eIDAS regulation (910/2014). While the Committee formally supervises the providers of these services, it outsources compliance audits to private experts who are certified and listed by the Committee. Given this existing framework, it is feasible that CABs under the Cyber Resilience Act could operate similarly, utilising PPPs and outsourcing conformity assessments to certified private experts.

In addition to the legislation and policy implementation-related issues, Latvia has been an active participant in multiple EU cybersecurity policy coordination and cooperation formats, including the NIS Cooperation Group, the ENISA Management Board, and the NLO Network, where the Ministry of Defence represents the country. Through these platforms, Latvia has contributed to shaping EU-wide cybersecurity policies, exchanging best practices with other Member States, and ensuring the effective implementation of European cybersecurity initiatives at the national level. These efforts reinforce Latvia's commitment to strengthening its cybersecurity posture and ensuring resilience against an ever-evolving threat landscape.

Capacity-Building

CERT.LV has been the central institution for cybersecurity capacity-building in Latvia. Initially focused on enhancing its own personnel's expertise through external training, it has since expanded its efforts to provide a broad range of capacity-building initiatives for experts across various sectors. CERT.LV operates as a non-punitive institution, ensuring that any information it receives regarding vulnerabilities, compliance issues, or security flaws is never used for fines or sanctions. Instead, it provides free guidance to help entities improve their cybersecurity, fostering a collaborative and trust-based environment. As a research laboratory under the Institute of Mathematics and Computer Science at the University of Latvia, CERT.LV's neutrality has been crucial in cultivating open communication and information sharing. This approach has encouraged cybersecurity professionals to reciprocate, creating a culture of mutual exchange both with CERT.LV and among themselves.

Over time, this collaborative model has led to the development of a strong cybersecurity community spanning various sectors. To facilitate communication, CERT.LV established a secure online platform using *Mattermost*, an open-source solution. Currently, with over 800 members, this platform serves as a forum for discussing industry topics, coordinating activities, sharing news and cyber threat intelligence in real time, and receiving expert advice. CERT.LV ensures that only trusted individuals gain access, mitigating insider threats. Another key initiative is the Security Experts Group (DEG), which unites cybersecurity professionals to enhance cooperation and knowledge-sharing. Initially informal in 2007 and formalised in 2012, DEG provides a platform for cybersecurity discussions, policy input, and exploring emerging challenges. Members are often consulted in the drafting of major cybersecurity policy documents, making DEG a vital forum for advancing Latvia's cybersecurity ecosystem.

Beyond training and networking, CERT.LV has developed a comprehensive suite of technical assistance services. In addition to its core function in cyber incident response, it offers free services such as a DNS firewall to filter out malicious content, phishing simulations, penetration testing, an early warning sensor network, and security operations centre services. Some services, like penetration testing, receive support from ENISA's Cybersecurity Support Action initiative, while others, such as DDoS protection provided by the Latvia State Radio and Television Centre (LVRTC), are funded by the Ministry of Defence.

CERT.LV is also a leading force in public cybersecurity awareness campaigns. These efforts include lectures on cybersecurity and cyber hygiene, as well as the development of informational materials like presentations and factsheets. Its website *cert.lv* provides practical cybersecurity resources for institutions and businesses, while the dedicated *esidrošs.lv* platform offers guidance on best practices, cyber hygiene, and responses to cyber incidents. Though its content is not necessarily unique, CERT.LV's communications align with ENISA's efforts at the EU level. One of CERT.LV's most prominent initiatives is the "Esi drošs" (*Be Safe*) workshops, designed for IT professionals and reaching a wider audience than similar training programs offered by other organisations in Latvia.

A flagship event in CERT.LV's awareness-raising efforts is *CyberChess*, the largest cybersecurity conference in Latvia, organised annually as part of European Cybersecurity Month. Supported by ENISA and the European Commission, *CyberChess* attracts over 500 in-person attendees and 3,000 online participants, drawing representatives from EU Member States, agencies, and international partners. Its growing significance has positioned *CyberChess* as a key cybersecurity event in the region, setting an example for other Member States. In 2025, the conference will be held for the twelfth time, continuing to cover a broad range of cybersecurity topics, from technical innovations to policy and strategy discussions.

With the establishment of the National Coordination Centre in Latvia (NCC-LV) under the ECCC Regulation (2021/887), Latvia has added another institution dedicated to cybersecurity capacity-building, facilitating the distribution of EU resources and knowledge. NCC-LV not only helps define strategic priorities for the ECCC but also oversees national cybersecurity research and development (R&D) activities. While its full impact is still unfolding, it has already allocated €1 million in financial support through third-party (FSTP) grants to support cybersecurity transformation in small and medium-sized enterprises. To implement EU funding policies, Latvia adopted the Law on Management of the ECCC Funding for the 2021–2027 Programming Period (2022).

Although NCC-LV provides FSTP funding, it is not the sole financial resource for cybersecurity-related projects. Other significant funding includes the €37.5 million digital transformation program managed by the Investment and Development Agency of Latvia (LIAA), co-funded by the Recovery and Resilience Facility. Additionally, businesses can access EU-level funding through Digital Europe and Horizon Europe programs, with NCC-LV playing a key role in guiding applicants.

In line with the ECCC Regulation, NCC-LV established a national cybersecurity competence community in 2022 as a central networking platform for innovation and cybersecurity. Community members undergo national-level assessment and security vetting. As of February 2025, the community includes 53 organisations, surpassing the projected milestone of 50 members by mid-2025. Latvia was also the first EU Member State to formally notify the ECCC of its assessed national cybersecurity competence community members, despite the ECCC not yet launching a registration system.

Community representatives meet quarterly for plenary discussions on cybersecurity topics, with open participation and topic proposals. Two working groups focus on organising the National Cybersecurity Challenge and enhancing cybersecurity education. Future groups may address cybersecurity legislation (including NIS2 implementation) and certification. Communication channels include a Mattermost platform and a mailing list managed by NCC-LV, used for newsletters, event announcements, funding opportunities, and policy consultations. The community has provided input on key legislative proposals, such as the National Cybersecurity Law, its implementing regulations, and the EU Cyber Solidarity Act. NCC-LV also serves as the main hub for cybersecurity R&D information exchange and promotion.

NCC-LV has launched multiple initiatives, particularly in education and training. The National Cybersecurity Challenge, aimed at students aged 14–24,

attracted 469 participants from 100 educational institutions in 2024. Future plans include educator training to enhance youth cybersecurity education and the development of a national Cybersecurity Education Roadmap. Additionally, NCC-LV provides training sessions for cybersecurity experts and essential and important entities under NIS2, alongside information events on legislative changes and funding opportunities.

A landmark event was *CyberBazaar*, the Baltic Cybersecurity Innovation Forum, organised for the first time in December 2024 by NCC-LV and its Estonian and Lithuanian counterparts, with support from the ECCC and ENISA. As the largest cybersecurity forum in the Baltic states, it attracted over 600 participants and featured an exhibition of cybersecurity projects, a business and technology conference, the first cybersecurity research conference in the Baltics, and a pan-Baltic student hackathon. European Parliament President Roberta Metsola (2024) called *CyberBazaar* a “groundbreaking event” and an “important step” for strengthening EU cyber resilience.

Latvia also utilises external training opportunities from the European Security and Defence College (ESDC) and EU law enforcement programs. The European Cybercrime Centre (EC3) supports Latvia’s law enforcement agencies in exchanging best practices. Additionally, the EU Agency for Law Enforcement Training (CEPOL) provides specialised training, while networks such as the European Judicial Training Network, the International Organization for Judicial Training, and the Academy of European Law (ERA) contribute to building cybersecurity expertise.

Cyber Defence

Due to its secretive nature, cyber defence is a challenging domain to explore publicly. This section focuses on cyber defence-related initiatives, including information exchange and capacity-building projects where information is available. At the EU level, it remains a complex area to study, as defence and national security fall under the exclusive competence of Member States. Nevertheless, general observations provide insights into Latvia’s approach.

In Latvia, both cyber defence and broader cybersecurity policy are coordinated by the Ministry of Defence, ensuring alignment between civilian and military efforts and fostering a comprehensive cyber resilience approach. Within the military, cyber defence activities are managed by the J-6 Department of the Joint Headquarters of the National Armed Forces. Established in 2016 under the Defence Intelligence and Security Agency (MIDD), MilCERT serves as the military CSIRT, handling cyber incident response for defence sector ICT infrastructure in close cooperation with CERT.LV.

Latvia has also established a Cyber Defence Unit, reorganised in 2024 into the Cyber Defence and Electromagnetic Warfare Battalion within the National Guard. Comprising both career military personnel and civilian cybersecurity experts from public and private sectors, this well-equipped and trained unit is fully operational.

It can assist civilian authorities during major cyber incidents, support MilCERT or CERT.LV, and leverage its members' expertise to enhance national cyber defence.

Latvia actively participates in national and international cybersecurity and cyber defence exercises. National drills include the cross-sectoral cybersecurity exercise *Medus Pods* and hybrid military exercises with cyber components, such as *AMEX* and *Namejs*. Internationally, Latvia engages in *Cyber Autumn*, ENISA-led *Cyber Europe* and *Blue OLEx*, as well as NATO's *Locked Shields*, *Crossed Swords*, and *Cyber Coalition*. In 2024, Latvia, alongside the NATO Communications and Information (NCI) Agency, won first place in *Locked Shields*, the world's largest live-fire cyber defence exercise, organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). This victory highlighted Latvia's advanced cyber defence capabilities. The team comprised members of the National Guard Cyber Defence Unit, CERT.LV experts, and specialists from government, military, critical infrastructure, academia, and the private sector – demonstrating Latvia's strong interoperability and coordination skills.

Capacity-building is another crucial aspect of Latvia's cyber defence policy, with initiatives under the European Defence Fund (EDF), the European Defence Agency (EDA), and Permanent Structured Cooperation (PESCO). The Ministry of Defence coordinates national participation in these projects, collaborating with the National Armed Forces and other defence institutions. Latvia participates in the EDA's MICNET project, which facilitates military CSIRT cooperation, including MilCERT. Additionally, in May 2024, Latvia joined the PESCO Cyber Rapid Reaction Teams and Mutual Assistance in Cyber Security (CRRTs) project, aimed at supporting Member States during major cyber incidents, conducting joint training, and assisting EU missions. However, Latvia's defence sector has limited capacity to fully engage in all cross-border projects due to personnel constraints, necessitating a focus on priority initiatives.

For cyber defence crisis response, Latvia is actively involved in the EU-CyCLONE network, represented by the Ministry of Defence. Procedures for requesting support via EU-CyCLONE are integrated into Latvia's national cyber crisis management framework, aligning with the EU Strategic Compass for defence and security. Furthermore, these procedures have been tested in national-level cybersecurity exercise *AMEX*. Overall, Latvia's cyber defence efforts are well-coordinated within the European ecosystem, both benefiting from and contributing to EU-wide cyber resilience initiatives. While personnel limitations currently restrict Latvia's participation in some cross-border projects, its structured and strategic approach ensures effective engagement where resources allow.

Results and Discussion

The empirical findings illustrate Latvia's extensive engagement in the EU's cybersecurity ecosystem across three key dimensions: policy and legislation, capacity-building, and cyber defence. To assess the depth of Latvia's involvement, the following analysis applies a structured evaluation based on specific criteria

within each dimension. The degree of involvement is assessed qualitatively, distinguishing between high, moderate, and limited engagement.

Policy and Legislation

Latvia has demonstrated a high level of commitment to aligning its national cybersecurity policies with EU directives and regulations, reinforcing collective security principles through European legal harmonisation. The legal framework governing cybersecurity in Latvia is shaped predominantly by EU legislation, particularly the NIS Directive (and its successor, NIS2 Directive), the Cybersecurity Act, and the eIDAS regulation. The rapid and proactive implementation of these frameworks, in some instances exceeding minimum requirements, underscores Latvia’s dedication to strengthening cybersecurity governance. This process reflects digital sovereignty considerations, as Latvia strategically aligns its domestic policies with EU frameworks to ensure autonomy in securing its digital space while maintaining interoperability within the broader European cybersecurity landscape.

Institutionally, Latvia’s semi-centralised governance model, with the NCSC-LV as the lead institution, facilitates coordination with the EU cybersecurity bodies, including ENISA, the NIS Cooperation Group, and the CSIRT Network. However, while Latvia’s legislative integration with EU frameworks is well established, challenges persist in terms of resource allocation for specialised cybersecurity domains such as ICT certification under the Cyber Resilience Act. Table 7.1 summarises Latvia’s involvement in the EU cybersecurity ecosystem within the policy and legislation domain.

Table 7.1 Assessment of Latvia’s involvement in the EU cybersecurity ecosystem – policy and legislation domain

| <i>Criteria</i> | <i>Assessment</i> | <i>Justification</i> |
|--|-------------------|---|
| Transposition of EU legislation | Moderate | Proactive alignment with NIS2, in some aspect exceeding EU requirements, though the implementation is not yet complete. |
| Participation in EU cyber policy structures | Moderate | Active involvement in HWPCI, ENISA, NIS Cooperation Group, CSIRTs Network, though limited by personnel constraints. |
| Institutional coordination | Moderate | Ongoing centralisation under the NCSC-LV, facilitating horizontal cooperation and coordinated EU policy implementation. |
| European cybersecurity certification | Low | No national cybersecurity certification framework yet in place. |
| Enforcement of cybersecurity requirements | Moderate | Legislative alignment exists, but implementation is still in progress. |

Capacity-Building

Latvia has invested significantly in cybersecurity capacity-building, covering training programs, cybersecurity exercises, and community development. CERT.LV plays a leading role in knowledge transfer and technical support, including organising cybersecurity conferences, training sessions and exercises. Furthermore, Latvia's integration into the ECCC and the emerging role of NCC-LV as a cybersecurity competence-building hub further reinforce its commitment to fostering cybersecurity expertise.

One of Latvia's notable strengths in this dimension is its ability to integrate public and private stakeholders into a cohesive cybersecurity community. Through platforms such as *Mattermost*, Latvia facilitates real-time information exchange among cybersecurity professionals, ensuring that expertise is continuously shared across sectors. Moreover, financial support mechanisms, such as the FSTP grants managed by NCC-LV, provide a solid basis for strengthening cybersecurity innovation at the SME level. These efforts reinforce digital sovereignty by developing local cybersecurity expertise, reducing dependence on external actors, and ensuring that Latvia retains control over its national cyber capabilities.

Despite these achievements, Latvia faces scalability challenges in its educational and training programmes, requiring more detailed roadmapping at the national level, making full use of ENISA's European Cybersecurity Skills Framework (ECSF). Additionally, while Latvia actively engages in funding mechanisms such as Digital Europe and Horizon Europe, administrative constraints limit the full utilisation of these funding opportunities, with relatively low number of entities applying for funding. Addressing these limitations would not only bolster national cybersecurity resilience but also fortify the EU's collective cyber defence posture. Table 7.2 summarises Latvia's involvement in the EU cybersecurity ecosystem within the capacity-building domain.

Cyber Defence

Cyber defence remains a sensitive and complex domain due to national security considerations. Latvia has successfully integrated cyber defence within its broader security architecture, with the Ministry of Defence ensuring centralised coordination. The establishment and recent reorganisation of the Cyber Defence and Electromagnetic Warfare Battalion of the National Guard demonstrates Latvia's proactive stance in enhancing cyber defence capabilities.

At the operational level, Latvia actively participates in cross-border cyber defence exercises, both within the EU and NATO frameworks. The success of the Latvian-led *Locked Shields* team in 2024 is a testament the country's advanced operational capabilities and interoperability. Moreover, Latvia's participation in the PESCO CRRTs and MICNET projects underscores its commitment to collective EU cyber defence efforts. This development is a testament to Latvia's dual commitment to collective security and digital sovereignty, balancing its EU and

Table 7.2 Assessment of Latvia's involvement in the EU cybersecurity ecosystem – capacity-building domain

| <i>Criteria</i> | <i>Assessment</i> | <i>Justification</i> |
|---|-------------------|--|
| Alignment of awareness-raising initiatives | High | Well-coordinated efforts by CERT-LV and NCC-LV involving key stakeholders, in line with the ENISA guidance; European Cybersecurity Month activities. |
| Cross-border cooperation initiatives | Moderate | Cross-border cooperation activities involving the Baltic states (e.g. <i>CyberBazaar</i>), cooperation in the NCC Network and CSIRTs Network, albeit constrained by personnel resources. |
| Community-building | High | Well-coordinated, operational cybersecurity community network with strong information-sharing mechanisms. |
| Investments in R&D | Low | Despite the NCC-LV's efforts, EU funding opportunities (Digital Europe, Horizon Europe) remain underutilised. |
| Education and training | Moderate | Several notable EU-related initiatives, such as the National Cybersecurity Challenge, but no ECSF-aligned, comprehensive education framework in place yet. Limited use of EU trainings due to personnel constraints. |

Table 7.3 Assessment of Latvia's involvement in the EU cybersecurity ecosystem – cyber defence domain

| <i>Criteria</i> | <i>Assessment</i> | <i>Justification</i> |
|---|-------------------|--|
| Integration with civilian cybersecurity structures | High | Ministry of Defence ensures central coordination; cyber defence structures are well-integrated and support CSIRTs in case of a major cyber incident or crisis. |
| Participation in EU-level and other major cross-border exercises | High | Regular engagement in <i>Locked Shields</i> , <i>Cyber Europe</i> , and other cross-border cyber defence exercises. |
| Engagement in EU-funded cyber defence projects | Moderate | Active participation in select initiatives (CRRTs, MICNET), but constrained by resource limitations. |
| Operational readiness to support other EU allies | Moderate | High degree of operational readiness, as evidenced by major exercises, but limited participation in missions due to resource constraints. |
| Alignment with the EU strategic compass | High | Confidence-building measures are well aligned; EU-CyCLONE procedures have been integrated into the national crisis management frameworks and tested. |

NATO engagements while maintaining national cyber autonomy. However, relying on multinational defence initiatives can create dependencies that may conflict with national cybersecurity priorities (Bendiek & Porter, 2013).

However, while Latvia engages in EU defence initiatives, its participation remains constrained by personnel and resource limitations. In particular, while Latvia is a member of key EU and NATO cyber defence formats, its ability to meaningfully contribute to all relevant initiatives is restricted. Prioritisation of engagement in high-impact projects is therefore necessary. Table 7.3 summarises Latvia's involvement in the EU cybersecurity ecosystem within the cyber defence domain.

Conclusion and Policy Recommendations

Latvia occupies a strategic position within the EU cybersecurity ecosystem, successfully balancing regulatory alignment, extensive capacity-building initiatives, and robust engagement in cyber defence efforts. The country exemplifies a smaller EU Member State that effectively leverages collective security frameworks to enhance national resilience, while also safeguarding elements of digital sovereignty.

Despite these strengths, Latvia faces structural and institutional constraints that require strategic intervention. In regulatory matters, challenges persist in implementing ICT product certification and ensuring cybersecurity market regulation keeps pace with technological advancements. In capacity-building, Latvia excels in community-driven initiatives but faces limitations in fully integrating its educational frameworks with the ECSF. In cyber defence, the country demonstrates a high level of operational readiness and interoperability but its involvement in multinational projects is limited by insufficient resources.

Overall, continued investment in institutional capacity, cybersecurity education, and operational cyber defence capabilities will be critical in maintaining and strengthening its role within the European cybersecurity ecosystem. Moving forwards, Latvia should pursue a dual strategy – deepening its integration in the EU cybersecurity frameworks while also fostering national initiatives that reduce external dependencies. Key recommendations include:

- 1 **Implementing cybersecurity certification frameworks** – Latvia should prioritise the development of a national certification framework for ICT products and services, aligning with the EU Cyber Resilience Act, while preserving national flexibility in the implementation of certification standards (notably in terms of institutional setup).
- 2 **Enhancing cybersecurity training and workforce development** – Expanding cybersecurity educational programs in line with ECSF profiles, improving cybersecurity awareness, and integrating cybersecurity into national curricula would mitigate skills shortages and reduce reliance on external cybersecurity expertise.

- 3 **Strengthening cross-border cyber defence cooperation** – Increased engagement in EU cyber defence initiatives (PESCO, EDA) should be pursued strategically, ensuring that participation aligns with Latvia's national cybersecurity objectives.
- 4 **Maximising EU funding utilisation** – Increasing the participation in Digital Europe and Horizon Europe programmes can be instrumental to strengthening cybersecurity in public and private institutions and strengthening national ICT infrastructure through targeted investments in R&D. Latvia must also streamline administrative processes to fully leverage the available financial instruments.

By addressing these key areas, Latvia can further consolidate its role as a regional cybersecurity leader, demonstrating how a small but agile state can successfully navigate the interplay between collective security imperatives and digital sovereignty considerations within the evolving EU cybersecurity landscape.

Bibliography

- Baldini, G., Barrero, J., Chaudron, S., Coisel, I., Draper Gil, G., Duch Brown, N., Eulaerts, O., Geneiatakis, D., Hernandez Ramos, J. L., Joanny, G., Junklewitz, H., Kampourakis, G., Kerckhof, S., Kounelis, I., Lewis, A., Martin, T., Nai Fovino, I., Nativi, S., Neisse, R.,... Tirendi, S. (2020). Cybersecurity at the Heart of Societal Transformation. In I. Nai Fovino, G. Barry, S. Chaudron, I. Coisel, M. Dewar, H. Junklewitz, G. Kampourakis, I. Kounelis, B. Mortara, J. P. Nordvik & J. I. Sanchez Martin (Eds.), *Cybersecurity, Our Digital Anchor: A European Perspective* (pp. 20–31). European Commission. <https://doi.org/10.2760/352218>
- Bederna, Z., & Rajnai, Z. (2022). Analysis of the Cybersecurity Ecosystem in the European Union. *International Cybersecurity Law Review*, 3(1), 35–49. <https://doi.org/10.1365/s43439-022-00048-9>
- Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/Sovereignty and European Security Integration: An Introduction. *European Security*, 31(3), 337–355. <https://doi.org/10.1080/09662839.2022.2101887>
- Bendiek, A., & Porter, A. L. (2013). European Cyber Security Policy Within a Global Multi-stakeholder Structure. *European Foreign Affairs Review*, 18(2). <https://doi.org/10.54648/eerr2013011>
- Bickman, L., & Rog, D. (2009). Applied Research Design: A Practical Approach. In L. Bickman & D. Rog (Eds.), *The SAGE Handbook of Applied Social Research Methods* (2nd ed., pp. 3–43). SAGE Publications. <https://doi.org/10.4135/9781483348858>
- Biscop, S. (2016). All or Nothing? The EU Global Strategy and Defence Policy After the Brexit. *Contemporary Security Policy*, 37(3), 431–445. <https://doi.org/10.1080/13523260.2016.1238120>
- Budnitsky, S., & Jia, L. (2018). Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance. *European Journal of Cultural Studies*, 21(5), 594–613. <https://doi.org/10.1177/1367549417751151>
- Cabinet of Ministers. (2023). *National Cybersecurity Strategy of Latvia 2023–2026*. <https://likumi.lv/ta/id/340633>
- Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, 55(6), 1254–1272. <https://doi.org/10.1111/jcms.12575>

- Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Palgrave Macmillan. <https://doi.org/10.1057/9781137400529>
- Clarke, R. A., & Knake, R. K. (2011). *Cyber War: The Next Threat to National Security and What to Do About It*. Tantor Media.
- Consolidated Version of the Treaty on European Union. (2012). <https://data.europa.eu/eli/treaty/teu/2012/oj>
- Council of the European Union. (2020). *Council conclusions on shaping Europe's digital future*. <https://www.consilium.europa.eu/media/44389/st08711-en20.pdf>
- Couture, S., & Toupin, S. (2019). What Does the Notion of “Sovereignty” Mean When Referring to the Digital? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, 4(1), 15–32. <https://doi.org/10.1111/j.1749-5687.2009.00088.x>
- Deutsch, K. (2006). Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience. In M. Eilstrup-Sangiovanni (Ed.), *Debates on European Integration: A Reader* (1st ed., pp. 68–86). Bloomsbury Academic. https://doi.org/10.1007/978-0-230-20933-6_4
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). <https://data.europa.eu/eli/dir/2016/1148/oj>
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). <https://data.europa.eu/eli/dir/2022/2555/oj>
- ENISA. (2017). *Principles and opportunities for a renewed EU cyber security strategy*. <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-input-to-the-css-review>
- ENISA. (2023). *ENISA Threat Landscape 2023*. <https://doi.org/10.2824/782573>
- ENISA. (2024). *2023 Consolidated Annual Activity Report*. Publications Office of the European Union. <https://doi.org/10.2824/44117>
- European Commission. (2020). *Joint communication to the European Parliament and the Council. The EU's cybersecurity strategy for the digital decade*. <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>
- European Defence Agency. (2021). *Defence Data 2018–2019: Key findings and analysis*. <https://eda.europa.eu/publications-and-data/brochures/defence-data-2018-2019>
- European External Action Service. (2022). *A strategic compass for security and defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security*. (7371/22). <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>
- Eurostat. (2024). *Standard Eurobarometer 100 – Autumn 2023* (Version 1.00) European Commission. https://data.europa.eu/88u/dataset/s3053_100_2_std100_eng
- Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, 33(3), 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
- Haas, E. B. (2004). *Uniting of Europe: Political, Social, and Economic Forces, 1950–1957*. University of Notre Dame Press. <https://doi.org/10.2307/j.ctv19m62zk>
- Howorth, J. (2014). *Security and Defence Policy in the European Union* (2nd ed.). Red Globe Press.

- Information Technology Security Law. (2010). <https://likumi.lv/ta/id/220962>
- Juncker, J.-C. (2018). *State of the European Union Address by President Juncker*. https://ec.europa.eu/info/priorities/state-union-speeches/state-union-2018_en
- Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, 38(2), 7–40. https://doi.org/10.1162/ISEC_a_00138
- Kennedy, P. (1989). *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000*. William Collins.
- Keohane, R. O. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy* (Revised ed.). Princeton University Press. <https://doi.org/10.2307/j.ctt7sq9s>
- Klossa, G. (2019). *Towards European media sovereignty: An industrial media strategy to leverage data, algorithms and artificial intelligence*. https://commission.europa.eu/publications/towards-european-media-sovereignty_en
- Law on Management of the European Cybersecurity Competence Centre Funding for the 2021–2027 Programming Period. (2022). <https://likumi.lv/ta/id/336087>
- Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, 22(1), 1–6. <https://doi.org/10.1080/1097198X.2019.1569186>
- MacCormick, N. (1999). *Questioning Sovereignty: Law, State, and Nation in the European Commonwealth*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780198268765.001.0001>
- Madiega, T. A. (2020). *Digital Sovereignty for Europe* [Briefing]. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2020\)651992](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651992)
- Mearsheimer, J. J. (2001). *The Tragedy of Great Power Politics*. W. W. Norton & Company.
- Menon, A. (2011). European Defence Policy from Lisbon to Libya. *Survival*, 53(3), 75–90. <https://doi.org/10.1080/00396338.2011.586191>
- Metsola, R. (2024, December 5). Keynote Address, Baltic Cybersecurity Innovation Forum “CyberBazaar 2024”. <https://www.youtube.com/watch?v=rw4nrN-T9G0>
- Ministry of Defence. (2022). *On Improving National Cybersecurity Governance (Report)*. https://tapportals.mk.gov.lv/legal_acts/3496512f-0307-4e7a-9951-579b79cc3eb2#
- Moravcsik, A. (1998). *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht*. Cornell University Press.
- National Cybersecurity Law. (2024). <https://likumi.lv/ta/id/353390>
- Pohle, J., & Thiel, T. (2020). Digital Sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>
- Regulation 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. <https://data.europa.eu/eli/reg/2021/887/oj>
- Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS). <https://data.europa.eu/eli/reg/2014/910/oj>
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). <https://data.europa.eu/eli/reg/2019/881/oj>
- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). <https://data.europa.eu/eli/reg/2024/2847/oj>

- Sandholtz, W., & Stone Sweet, A. (1998). Integration, Supranational Governance, and the Institutionalization of the European Polity. In W. Sandholtz & A. Stone Sweet (Eds.), *European Integration and Supranational Governance* (pp. 1–26). Oxford University Press. <https://doi.org/10.1093/0198294646.003.0001>
- Seixas, B. V., Smith, N., & Mitton, C. (2018). The Qualitative Descriptive Approach in International Comparative Studies: Using Online Qualitative Surveys. *International Journal of Health Policy and Management*, 7(9), 778–781. <https://doi.org/10.15171/ijhpm.2017.142>
- Timmers, P. (2018). The European Union's Cybersecurity Industrial Policy. *Journal of Cyber Policy*, 3(3), 363–384. <https://doi.org/10.1080/23738871.2018.1562560>
- von der Leyen, U. (2019). *A Union that strives for more: My agenda for Europe*. https://commission.europa.eu/system/files/2020-04/political-guidelines-next-commission_en_0.pdf
- von der Leyen, U. (2020). *State of the European Union Address by President von der Leyen*. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655
- Wallace, W. (1999). The Sharing of Sovereignty: The European Paradox. *Political Studies*, 47(3), 503–521. <https://doi.org/10.1111/1467-9248.00214>
- Walt, S. M. (1991). The Renaissance of Security Studies. *International Studies Quarterly*, 35(2), 211–239. <https://doi.org/10.2307/2600471>
- Waltz, K. N. (1979). *Theory of International Politics*. Addison-Wesley Publishing Company.

8 Cyber Diplomacy

Latvia's Voice in the World

Didzis Kļaviņš

Introduction

Diplomacy, as the activity of implementing a country's national goals and protecting its interests, has always been a vital component of a state's foreign policy. Referring to Martin Wight (1979, p. 113), it is the "master institution" of international politics. For more than a quarter of a century, diplomacy has undergone significant changes, as evidenced by the wide range of topics now covered by foreign services and efforts to integrate innovative technologies into diplomatic practices. Various types of diplomacy, such as innovation diplomacy and tech diplomacy, vividly illustrate this evolution. To address emerging global challenges and technological advancements, diplomacy has had to not only learn to skilfully use various digital tools and platforms for diplomatic activities but also focus on better securing cyberspace and managing cyber threats.

Alongside the significant development in information and communication technology (ICT), there has been a marked increase in both the number and complexity of cyber threats. For instance, an annual report by the European Union Agency for Cybersecurity or ENISA (2023) highlights a significant escalation in cybersecurity attacks, highlighting eight prime threat group among which are ransomware, malware, distributed denial-of-service (DDoS), and supply chain attacks. Given that cyber incidents often transcend national borders and countries need to collaborate to establish international rules and standards in the cyber domain, one type of diplomacy whose significance grows each year is cyber diplomacy. Recognising the emerging dimensions of cybersecurity (Cornish, 2021; Tikk & Kerttunen, 2020), the transnational character of cyber threats and incidents, and the seriousness of the situation, countries must prioritise cyber resilience to protect their critical infrastructure and share best practices to effectively combat the evolving nature of cyberattacks. Latvia is no exception, as evidenced by the frequent and increasing threats to its cyberspace, including numerous phishing campaigns, ransomware, malware, system and network hacking attempts, and active DDoS attacks on critical IT systems. According to the Cybersecurity Incident Response Institution (CERT.LV), the number of cyberattacks in Latvia has risen sharply since January 2022, reaching unprecedented levels in the past two years (LSM.lv, 2024c). Strengthening measures to mitigate these escalating risks is imperative,

as they directly impact national security and require comprehensive international cooperation to address effectively.

Considering all this, the aim of this chapter is to explore what cyber diplomacy is and how the Latvian Ministry of Foreign Affairs (MFA), as the leading government institution in foreign affairs, implements this type of diplomacy at both global and regional levels. Based on a retrospective approach, the aim of this study is to understand the directions, focuses, and motivations of Latvia's cyber diplomacy as a foreign policy instrument. Given the sensitive nature of cyber issues, the study relies on publicly available information and personal communication with senior Latvian cybersecurity and cyber diplomacy experts. To elaborate on the role and actions of cyber diplomacy, the interviewees were assured of absolute anonymity in exchange for greater openness. To achieve the aforementioned goals, the following section will delve into the concept of cyber diplomacy within the evolving landscape of cyberspace.

Cyber Diplomacy: Definition and Dimensions

In the academic literature and media reports on cyber diplomacy, there is widespread belief that the dawn of cyber diplomacy occurred in 2007, a year remembered for a highly coordinated series of cyberattacks on Estonian public and private sector organisations (Attatfa et al., 2020, p. 60). Although the Estonian cyberattacks were a significant event that highlighted the vulnerabilities and complexities of cyberspace (Kello, 2024, pp. 121–122; Tamkin, 2017), and even have been referred to as “the world’s first cyber war” (Invest in Estonia, 2017), it is important to note that cyber diplomacy term can be found in earlier discussions related to both cybersecurity and international relations. Early discussions can be traced back to at least the early 2000s, with publications discussing how digital technologies and mass diplomacy are shaping diplomatic practices and strategies (Potter, 2002; Pahlavi, 2003). According to André Barrinha (2024), the term cyber diplomacy was first mentioned in a speech delivered by Gordon Smith, Canada’s Deputy Minister for Foreign Affairs and International Trade, at the Technology in Government Forum in Ottawa in 1996.

Following the cyberattacks in Estonia, the number of publications on cyber diplomacy increased in the subsequent years. Not only in academic publications but also in the media, there was debate about what exactly cyber diplomacy is and how it differs from other types of diplomacy, such as digital diplomacy. One of the scholars in diplomacy research, Shaun Riordan (2016), in the blog *Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction*, addressed the terminological confusion between “digital diplomacy” and “cyber diplomacy” in the digital age. He argued that these terms have often been used interchangeably, leading to misunderstandings in the field. To avoid such confusion, Riordan proposed a clear distinction: “digital diplomacy” should refer to using digital tools and techniques to achieve diplomatic objectives (including consular diplomacy), while “cyber diplomacy” should denote applying diplomatic methods and mindsets to resolve issues in cyberspace. Later, in his book *Cyberdiplomacy: Managing*

Security and Governance Online, Riordan (2019, p. 5) writes, “digital diplomacy is the application of digital tools to diplomacy, whereas cyberdiplomacy is the application of diplomacy to cyberspace”.

In general, cyber diplomacy as a sub-field of diplomacy has been described as the instrument of foreign policy involving diplomatic techniques and negotiations to regulate cyberspace-related issues in international relations, aiming to promote responsible behaviour, safeguard cybersecurity, and maintain stability while facilitating agreements and dialogue between nations during cyber-related disputes (Radanliev, 2024). Authors such as Agnes Kasper, Anna-Maria Osula, and Anna Molnár (2021, p. 3) describe cyber diplomacy “as diplomacy of cyberspace or the use of diplomatic resources, initiatives and the performance of diplomatic functions to promote national interests that are defined in national cybersecurity strategies”. André Barrinhaa and Thomas Renard (2017, p. 355) also define cyber diplomacy as the application of diplomatic resources and the execution of diplomatic functions to safeguard national interests in relation to cyberspace.

Cyber diplomacy, which has become a crucial component of international relations today, is often primarily focused on the security aspects of cyberspace. This includes safeguarding digital infrastructure, preventing cyberattacks, attributing malicious cyber incidents, and establishing international norms and agreements aimed at enhancing cybersecurity. While the security dimension is significant, cyber diplomacy has a much broader scope, encompassing all diplomatic activities related to cyberspace, such as economic, social, and political dimensions. Analysing cyber diplomacy activities clearly delineates its extensive scope, which includes a wide range of issues such as digital governance and regulation, digital trade, data protection, and human rights. Given that many industries such as ICT, finance, energy, security, and healthcare intersect with cyber diplomacy, it covers all diplomatic activities. In the EU context, Kasper et al. (2021, p. 10) have highlighted that cyber diplomacy has a significant economic component and a direct connection to the internal market and its policies.

Moreover, new industries and areas intersect with cyber diplomacy due to their increasing roles in cybersecurity and global connectivity. The space industry is a good example, illustrating how countries and international organisations such as the European Space Agency (2022, 2023) are increasingly making comprehensive efforts to address emerging challenges and cyber risks. As technologies advance and threats evolve, it is important, with the help of cyber diplomacy, to strengthen international partnerships. Especially with like-minded allies, these partnerships are vital for creating new regulations and measures, as well as for developing technological defences against cyber threats and vulnerabilities in space.

Analysing the dimensions of cyber diplomacy, Petar Radanliev (2024, p. 3) identifies key components such as international cooperation, conflict resolution, cybersecurity governance, confidence-building measures, attribution and accountability, public-private partnerships, capacity-building, digital rights, and freedoms. A description of all these component activities clearly illustrates the broad scope of cyber diplomacy and its importance in complex global challenges related to cybersecurity and international relations. Moreover, authors (Attatfa et al., 2020,

p. 66) have emphasised that it is not solely a technical issue, highlighting the need for increased diplomatic engagement to address non-technical security and power dynamics in cyberspace. Christopher A. Ford (2022) also notes that although there are highly technical aspects to this work, such as analysing cyberattackers tactics, techniques, and procedures and intelligence-derived information for attribution assessments, cyber diplomacy is not just a technical matter. It also involves persuasion, as it requires convincing others to agree on cyber threat assessments, attributing specific attacks to particular actors, and determining appropriate responses in each case (Ford, 2022, p. 37). While there is definitely a need for research into diplomatic action, it is important to recognise that the skills required to implement cyber diplomacy, which Shaun Riordan (2016) refers to as “the use of diplomatic tools, and the diplomatic mindset, to resolve issues arising from cyberspace”, nevertheless demand quite specific knowledge of cyberattack techniques and emerging technologies.

Building on this understanding of cyber diplomacy’s diverse dimensions and the need for both technical and diplomatic expertise, Christopher A. Ford (2022) outlines methods for systematically structuring cybersecurity policy interventions to strengthen cyber diplomacy, suggesting a framework for thinking systematically about persuasive engagement between international partners and developing concepts for effective policy interventions. By presenting a framework for understanding threat persuasion in the context of cyberspace and linking cyberspace security diplomacy with cyber diplomacy, Ford (2022, pp. 48–50) highlights five key implications for policy interventions: improved information sharing, third-party validation, risk mitigation, a track record of accuracy, and enhanced information collection. One aspect that could improve not only the prospects for successful cyberspace security diplomacy but also cyber diplomacy in general is strengthening diplomats capabilities to comprehensively assist nations and international organisations in responding to cyber threats. This includes developing both their capacity and expertise.

Expanding on these broader themes of cooperation and capacity-building in cyber diplomacy, Petar Radanliev (2024, pp. 25–27) underscores the significance of cyber threat intelligence sharing as a practical mechanism for empowering organisations to identify emerging threats earlier and implement proactive countermeasures. Private sector organisations often possess substantial threat intelligence and data on cyber incidents, which they can share with governments and international organisations. Consequently, intelligence sharing fosters public-private cooperation, reduces duplication of effort, and promotes collective defence, ultimately building expertise and resilience within the cybersecurity community.

Overall, if we analyse cyber diplomacy in the context of the MFAs and more broadly, it aligns well with Brian Hockings (2002) concept of the “boundary spanner image”. Its role is described as “domestic–international mediation across porous policy arena boundaries; a facilitative role in the management of issue-directed coalitions” (Hocking, 2002, p. 11). Unlike the traditional position of the MFAs as a “gatekeeper image”, the “boundary spanner” model refers to a transformed role of diplomatic institutions that, relinquishing its monopoly in foreign affairs,

positions itself at the centre of international relations. Further, this model reflects a shift towards more proactive and inclusive diplomatic practices, emphasising coordination, cooperation and engagement over traditional hierarchical control. While cyber diplomacy assumes an increasingly significant role in a “complex, mixed actor system environment comprising permeable boundaries according high-salience and multilayered policy arenas” (Hocking, 2002, p. 11), it also strives to mitigate escalation of conflicts. As Jonathan F. Lancelot (2020, p. 252) eloquently describes, “cyber-diplomacy bridges the gaps between cyberspace, physical space, proportionality, error, and escalation”.

Over the last few years, a growing number of articles have highlighted how specific nations approach cyber diplomacy to advance their strategic interests (Bousfield, 2017; Feakin & Weaver, 2020; Jacobsen, 2024; Manantan, 2021). As cyber diplomacy involves leveraging diplomatic resources to support national cybersecurity strategies, understanding how different countries navigate this domain is crucial. Given that cyber diplomacy utilises diplomatic resources and functions to support national cybersecurity strategies, understanding the experiences of different countries in this area is crucial. Therefore, examining Latvia’s national cybersecurity governance will provide valuable insight into how the country employs diplomatic efforts to achieve foreign policy objectives and contribute to global cyber resilience. The following sections will explore these strategic diplomatic initiatives further.

The Landscape of Latvian Cyber Diplomacy

In Latvia, national cybersecurity governance operates through a partially centralised model. Since the adoption of the first National Cybersecurity Strategy in 2014, the Latvian MFA has been entrusted with a responsible role in developing cybersecurity within a comprehensive national defence framework. Over the past decade, three Cyber Security Strategies have been implemented (2014–2018; 2019–2022; 2023–2026), with the MFA leading efforts to ensure international cooperation.

In the 2014 strategy, the Latvian MFA was positioned immediately after the Ministry of Defence, which is formally responsible for formulating and delivering national cybersecurity policy, under the section dedicated to national cybersecurity policy development. The MFA was tasked with coordinating international cooperation and Latvia’s involvement in various international initiatives related to cybersecurity. Within the subsection on “International cooperation”, the first two of six required action points clearly outlined diplomatic tasks:

- 1 Strengthen cooperation with countries from the Baltic and Northern European countries and improve the cooperation with NATO, the EU, OSCE, and United Nations (UN) to improve the security, accessibility, and freedom of ICT.
- 2 Support international efforts in enhancing mutual trust and cooperation, emphasising the equal applicability of international legal norms to both the physical and the virtual environment (Ministry of Defence of the Republic of Latvia, 2014).

Further, it is notable to mention that the *Cybersecurity Strategy of Latvia 2019–2022* (Ministry of Defence of the Republic of Latvia, 2019) outlined the government's dependence on ICT and e-services, with a focus on enhancing ICT resilience at Latvia's diplomatic missions abroad. Similarly, the second strategy mandated the MFA to collaborate with the Ministry of Defence to formulate and present Latvia's national stance, participate in international cooperation programmes and platforms, strengthen Nordic and Baltic partnerships, actively engage in NATO and EU initiatives, and assist partner countries in enhancing their cyber defence capabilities. Moreover, both ministries were required to actively support formal and informal cooperation networks and programmes of international organisations such as the UN and OSCE. Additionally, the strategy included the specification to organise expert consultations on cybersecurity at least once annually to achieve anticipated outcomes and indicators (Ministry of Defence of the Republic of Latvia, 2019).

In the third Cyber Security Strategy (Ministry of Defence of the Republic of Latvia, 2023), covering the period 2023–2026, the description of specific responsibilities for government units and other stakeholders involved defined the role of MFA as follows: “The Ministry of Foreign Affairs (MoFA), within its competence, supports international cooperation and Latvia's participation in various international initiatives related to cybersecurity”. *The Cybersecurity Strategy of Latvia 2023–2026* clearly states the aim is to strengthen global cooperation in cybersecurity by endorsing international norms, creating a dependable network for mutual assistance in cyber threat assessments, and facilitating rapid information sharing and best practices:

In the EU format, legislative and policy initiatives should be promoted to ensure the secure and predictable development of the EU cyberspace, both in the operations of state institutions and in meeting the needs of individuals and legal entities. To deter cyberattacks and cyber incidents against EU ICT systems, the implementation of the EU Cyber Diplomacy Toolbox should be supported, with a consideration for its enhancement if necessary. Active cooperation and information exchange should be established within expert working groups and high-level meetings in the context of the EU and NATO.

(Ministry of Defence of the Republic of Latvia, 2023)

Moreover, the strategy clearly outlines Latvia's foreign policy goals in multilateral formats in the context of cybersecurity. To strengthen multilateral cooperation in cyberspace, the strategy notes the importance of the UN Open-ended working group (OEWG) on the security of and in the use of ICT. It defines that “Participation in the UN's work on ICT security should be sustained, together with like-minded partners, promoting the effectiveness of existing international norms in cyberspace and advocating for responsible state behaviour in it” (Ministry of Defence of the Republic of Latvia, 2023).

On 20 June 2024, the Latvian Parliament (Saeima) adopted the National Cybersecurity Law (*Nacionālās kiberdrošības likums*, 2024) to strengthen cybersecurity in Latvia. A key milestone under this legislation was the establishment of the

National Cybersecurity Centre on 1 September 2024. The centre now operates as the central authority for cybersecurity within the Ministry of Defence. It oversees the implementation of national cybersecurity requirements, serves as the primary point of contact for cybersecurity matters, and leads the development of Latvia's cybersecurity policies and initiatives. According to the Ministry of Defence Andris Sprūds:

The establishment of the National Cybersecurity Center is a significant step in strengthening Latvia's cyber resilience. It will enable more effective monitoring of the situation in cyberspace and faster response to incidents, providing the necessary support to public and private sector organizations.

(LSM.lv, 2024b)

According to Article 18 of the law (*Nacionālās kiberdrošības likums*, 2024), the National Cybersecurity Centre works with government agencies, national security institutions, and representatives from the private sector to develop the National Cybersecurity Strategy every four years. Given the transnational nature of cybersecurity issues, it is expected that the MFA will continue to play a significant role in coordinating international cooperation and ensuring cyber diplomacy at both the international and regional levels during the development and implementation of the strategy. Subsequently, it is important to examine how cyber diplomacy has been addressed in Latvia's annual foreign policy reports and in speeches by the Foreign Minister during the Foreign Policy Debate in the Latvian Parliament (*Saeima*).

Reflecting on historical events, it is noteworthy that the Estonian cyberattacks in 2007 were immediately reflected in the annual report of the Latvian Ministry of Foreign Affairs (*Latvijas Republikas Ārlietu ministrija*, 2008), highlighting the importance of this issue as well as Latvia's support for the newly established NATO Cooperative Cyber Defence Centre of Excellence in Estonia. However, in the following years, the significance of this issue was not particularly emphasised in the Ministry's annual reports. Starting from 2013, cybersecurity issues were more prominently featured in the annual reports on activities performed and planned in national foreign policy and European Union matters. In the context of cybersecurity, one of the issues highlighted in the reports was political dialogue and cooperation with the United States. Referring to the meeting between the Baltic States' presidents and United States President Barack Obama in Washington on 30 August 2013, the Public Report of 2013 (*Latvijas Republikas Ārlietu ministrija*, 2013) emphasised the US commitment and readiness to support Baltic initiatives to enhance cybersecurity. This included efforts to secure critical infrastructure in important economic sectors such as energy and transport. In the following years, foreign policy reports (*Latvijas Republikas Ārlietu ministrija*, 2013; Ministry of Foreign Affairs of the Republic of Latvia, 2014a, 2015a, 2017a) continued to highlight how Latvia played an active role in fostering bilateral cooperation in cybersecurity, including organising joint training exercises in cybersecurity with experts from the Baltic States and the United States.

Since Russia's illegal and illegitimate annexation of Crimea in 2014 and the subsequent escalation of the situation in Ukraine, particular attention should be given to the 2016 Annual Report (Ministry of Foreign Affairs of the Republic of Latvia, 2016a), which highlights the significance of cybersecurity for 2015 and the current year from several perspectives. Firstly, it emphasises the geopolitical dimension, with Russia's aggression in Ukraine further accentuating the importance of strengthening transatlantic links and maintaining a comprehensive political dialogue with the United States. Secondly, the Ministry's report references the *Cyber Security Strategy for 2014–2018*, which clearly defines Latvia's interests in the area of cybersecurity. Thirdly, Latvia held the Presidency of the Council of the European Union in 2015 and actively promoted a common understanding of cybersecurity among EU institutions. This included the adoption of the "Council Conclusions on Cyber Diplomacy" in February 2015 (Council of the European Union), which outlined the EU approach to cyber diplomacy and cybersecurity. Fourthly, the 2016 Annual Report clearly defines that cybersecurity would be one of Latvia's priorities for the same year, as the country coordinating the programme of Baltic and Nordic cooperation (NB8). Thus, the 2016 Annual Report (Ministry of Foreign Affairs of the Republic of Latvia, 2016a) highlights the importance of regional dimensions for promoting cooperation in cybersecurity.

Analysing foreign policy reports in the following years (Latvian Ministry of Foreign Affairs, 2017a, 2023a; Latvijas Republikas Ārlietu ministrija, 2022), several recurring themes can be highlighted. One of the most frequently mentioned topics is the significance of the improved EU Cyber Diplomacy Toolbox, which allows Latvia, along with other EU member states, to respond by applying cyber sanctions. Additionally, the foreign policy reports emphasise that a number of malicious cyber activities are related to Russia and China. In this context, Latvia supports the ongoing review and improvements to the EU cybersecurity regulations, addressing identified deficiencies in the current framework. The reports also highlight issues such as the implementation of the EU Toolbox on 5G cybersecurity, building resilience in hybrid security, including cybersecurity and combating disinformation, considering the possibility of applying sectoral sanctions in the event of a cyberattack, establishing the UN Cyber Programme of Action, and continuing to advocate for the creation of a transparent mechanism for action and cooperation with the private sector.

In addition to the Latvian foreign policy reports, each year the Minister of Foreign Affairs gives a speech at the Foreign Policy Debate to the Parliament (Saeima). Typically, this speech outlines Latvia's foreign policy priorities, strategies, and responses to current international developments. Moreover, it also serves as a platform for discussing the implementation of foreign policy goals and addressing any emerging challenges in the international arena. Over the past ten years, the topic of cyberspace security has also been included in these speeches. Specifically, in early 2014, Minister of Foreign Affairs Edgars Rinkēvičs emphasised the increasing

significance of cybersecurity during the Foreign Policy Debate in Parliament, thereby establishing a clear direction for Latvia's foreign policy.

The past year proved that questions of cyber policy will be more and more significant both at a national level and in international cooperation. As threats to our critical infrastructure increase, Latvia must strengthen its capacity to protect itself against cyber-attacks, while at the same time safeguarding democratic freedoms and taking advantage of the opportunities offered by a free internet and modern technologies.

(Ministry of Foreign Affairs of the Republic of Latvia, 2014b)

Further, when analysing Latvian cyber diplomacy activities, it is important to distinguish the different political formats where diplomats more frequently emphasise cybersecurity threats and underscore the need for action-oriented activities to address cybersecurity challenges through international cooperation. In the following section, from a national foreign policy perspective, several political formats, frameworks, and themes will be highlighted where the most significant efforts and activities in cyber diplomacy can be observed.

Cyber Diplomacy Activities Across Political Formats, Frameworks, and Themes

By analysing the activities and statements of the Latvian MFA and consulting with Latvian senior cybersecurity and cyber diplomacy experts (personal communication, 25 June 2024; 3 July 2024), it is clear that Latvian cyber diplomacy prioritises the security aspects of global cyberspace. This is evidenced by the responsibilities of the Global Security Division within the MFA, which is integrated into the Security Policy Department and the broader Directorate of Security Policy and International Organisations. Simultaneously, the close interaction between the MFA, the Ministry of Defence, and other national institutions highlights the sectoral and multifaceted nature of cyber issues. This broad range of topics necessitates the implementation of cyber diplomacy in international, regional, and bilateral policy formats.

One of the most prominent policy formats that should be highlighted is the UN. Within this framework, Latvian officials have often addressed the evolving cyber threat landscape, underscoring the increasing use of cyberattacks in hybrid warfare. Speaking at the UN, representatives of the Latvian MFA express the view that cyber threats are embedded in almost every aspect of daily life, making cybersecurity essential for maintaining public safety and economic stability. During the Security Council's High-Level Open Debate on cyber threats in June 2024, for instance, Parliamentary Secretary of the Ministry of Foreign Affairs of Latvia, Dace Melbārde highlighted that "today the cyber domain has become the connective tissue of the global economic and social development" (Permanent Mission of the Republic of Latvia to the United Nations, 2024b).

One of the defining elements of Latvia's cyber diplomacy is the strong advocacy for the establishment of a permanent UN mechanism on cybersecurity (Permanent

Mission of the Republic of Latvia to the United Nations, 2024b). For instance, during an Arria-formula meeting in New York on 4 April 2024, an informal gathering of members of the United Nations Security Council, Sanita Pavļuta-Deslandes, Ambassador and Permanent Representative of Latvia, presented Latvia's position. She emphasised the importance of implementing international law in cyberspace, strengthening national cyber resilience, and supported the establishment of a UN Programme of Action (PoA) on cybersecurity by 2026, while advocating for continued involvement of the Security Council in cybersecurity matters:

We do not regard cybersecurity as a matter belonging only to the GA. The Security Council should continue to deliberate on cybersecurity matters, including to reinforce application of international law in cyberspace. As we proceed towards establishment of the PoA, it would be worth exploring options for interaction between this mechanism and the Security Council. It would help ensure that the Council is kept abreast with the developments in the cyber domain and is in position to take the necessary decisions.

(Permanent Mission of the Republic of Latvia
to the United Nations, 2024a)

Latvian MFA representatives regularly emphasise the UN's collective responsibility in the context of cybersecurity and responsible state behaviour:

There is also more work to be done collectively in implementing the framework of responsible state behavior in cyberspace. Anticipating the establishment of a permanent UN mechanism to address cybersecurity, known as "Program of Action", we see potential for new synergies between the Council and the General Assembly in this field.

(Permanent Mission of the Republic of Latvia
to the United Nations, 2024b)

Over the last five years, the United Nations Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security has become an important political format for Latvia's cyber diplomacy. The OEWG was established by the UN General Assembly in December 2018 through resolution 73/27. This group was created to address issues related to cybersecurity and to develop norms, rules, and principles of responsible behaviour of states in cyberspace. One of the operative paragraphs of resolution 73/27 is 1.7., which emphasises the need for each state to safeguard their critical infrastructure against cyber threats:

States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

(United Nations, 2018)

Latvia actively engages in the OEWG on cybersecurity, aligning with EU positions to advocate for a secure cyberspace. In their statements, Latvian diplomats support developing international norms and applying international law in cyberspace, condemning malicious cyber activities and promoting multi-stakeholder engagement to boost cyber resilience (personal communication with Latvia's cyber diplomacy expert, 3 July 2024). Discussions frequently highlight the significant digital and technological divide among UN member states. While some focus on the impacts of emerging technologies like AI and quantum computing, many countries struggle to implement basic cybersecurity measures, such as developing national cybersecurity strategies and identifying critical infrastructure (The GIP Digital Watch, 2024; personal communication with Latvia's cyber diplomacy expert, 3 July 2024).

Further, the common aspects of Latvia's cyber diplomacy and its positions on cybersecurity within the United Nations OEWG have an emphasis on capacity-building and tailored approaches, recognition of increasing cyber threats, international cooperation and dialogue, multi-stakeholder engagement, focus on practical and action-oriented measures and alignment with broader UN and EU efforts. For instance, on 10 May 2024, in New York, the OEWG Chair organised a Global Roundtable on ICT security capacity-building, a high-level meeting open to capacity-building practitioners, state representatives, and various stakeholders. During a roundtable, held under the auspices of the UN, representatives from various countries, international organisations, cybersecurity experts, industry leaders, and civil society stakeholders addressed key challenges including cyber threat awareness gaps, a shortage of cybersecurity professionals, and the impact of the digital divide on global cybersecurity vulnerabilities (UNIDIR, 2024). In this high-level event, Latvia's representative emphasised the uneven playing field created by rapid ICT advancements, which leave gaps and vulnerabilities. Further, Latvia's representative recommends customised capacity-building methods that match the specific needs of each state, particularly small states. Being critique of the "one-size-fits-all" approach in capacity-building, Latvia underscored the efforts of its information technologies security incident response institution (CERT.LV), which provides assistance to countries of similar size, including those in the Western Balkans (The GIP Digital Watch, 2004).

When discussing diplomatic struggles within the OEWG, it is essential to highlight the ongoing debates about norms, principles, and regulations. The discussions have been dominated by two main approaches: Russia and its allies, such as Syria, continue to advocate for the creation of new, legally binding norms, while EU member states, including Latvia, and like-minded countries stress the importance of focusing on the implementation of existing voluntary norms. A significant argument from the group of like-minded states is that the priority should be on achieving a broader and more consistent application of current norms, particularly by developing countries, rather than diverting attention to new norms that could further burden these nations already facing challenges in implementing existing standards (personal communication with Latvia's cyber diplomacy expert, 3 July 2024). In this context, it is worth noting Lucas Kellos (2024, p. 127) general yet insightful observation. Analysing the differing perspectives on cybersecurity between major

nations, he writes, “when Western nations speak of cybersecurity, they often refer to vital infrastructure protection; when China and Russia discuss it, they typically refer to domestic information controls”.

In examining cyber diplomacy activities in the context of the UN, it is important to note Latvia’s candidacy in the 2025 UN Security Council elections. On 9 November 2023, Latvia officially launched its campaign for a United Nations Security Council (UNSC) seat in New York. Under the campaign’s motto, “Together for Peace and Resilience”, Latvia seeks support from at least two-thirds of UN Member States in the 2025 election for the 2026–2027 term on the Security Council (Ministry of Foreign Affairs of the Republic of Latvia, 2023b). Following the approval of the thematic lines of action for the campaign by the Cabinet of Ministers in April 2023, the Interinstitutional Working Group, headed by the Ministry of Foreign Affairs and collaborating with public, non-governmental, and private sector representatives, developed campaign lines. One of the key focus areas includes solutions for security, particularly cybersecurity (Ministry of Foreign Affairs of the Republic of Latvia, 2023b). The MFA has stated that “membership of the UNSC will be one of key instruments in pursuit and protection of Latvia’s foreign policy interests, as well as making it possible for Latvia to expand the scale of its cooperation” (Ministry of Foreign Affairs of the Republic of Latvia, 2023c). Moreover, Latvia also leverages the UN to advocate for the interests of smaller nations, build global support for Ukraine’s territorial integrity and sovereignty, and denounce Russia’s aggression. In its role in the UNSC, Latvia aims to prioritise issues such as bolstering international law, advancing cybersecurity, eliminating sexual violence in conflicts, and combating disinformation. According to the Ministry of Foreign Affairs of Latvia, “membership of the UN Security Council (UNSC) in 2026–2027 is one of the long-term objectives of Latvia’s foreign policy, also set out in the National Development Plan of Latvia for 2021–2027” (Ministry of Foreign Affairs of the Republic of Latvia, 2024d).

As resilience is the overarching theme of the campaign’s lines of action (Ministry of Foreign Affairs of the Republic of Latvia, 2023c), Latvian diplomats both at headquarters and in diplomatic missions abroad are engaging in pre-election activities by addressing UN member states. To enhance Latvia’s international visibility and strengthen its first-time bid for a seat as an elected member of the UNSC, a significant role has been assigned to the Permanent Mission of the Republic of Latvia to the United Nations and the activities they organise.

One notable activity of the “Together for Peace and Resilience” campaign that should be highlighted is a thematic discussion organised by Latvia at the UN on strengthening resilience in cyberspace. Held on 9 July 2024, this event was a collaboration between the Permanent Mission of Latvia to the United Nations, Bahrain, Colombia, and the UN Institute for Disarmament Research (UNIDIR) (Ministry of Foreign Affairs of the Republic of Latvia, 2024c). Representatives from the Latvian Ministry of Defence and CERT.LV, alongside experts from Microsoft, Cisco, and the Paris Peace Forum, participated in the discussion, which emphasised the importance of public-private cooperation and trust in addressing cyber challenges. The event also promoted responsible national behaviour and highlighted Latvia’s

experience in cybersecurity. Notably, Latvian cybersecurity experts introduced attendees to the new national Cyber Security Law (Ministry of Foreign Affairs of the Republic of Latvia, 2024c)

Similar to the UN format, Latvian cyber diplomacy activities within the EU context are multilayered and not always easily identifiable. One example is the Horizontal Working Party on Cyber Issues, which since 2016 has been responsible for coordinating the Council's work on cyber issues, primarily focusing on cyber policy and legislative activities. The main objectives of the working party are to ensure a unified and harmonised approach to cyber policy, promote coherent progress and threat mitigation, expand cooperation, facilitate information sharing, set EU cyber priorities, and represent the EU in alignment with its strategic cyber policy objectives. Although Latvia is represented in this working party by the representative of the Ministry of Defence to NATO and the EU, it is important to highlight that the Latvian MFA is regularly involved in addressing current issues.

As one of the objectives of the Horizontal Working Party on Cyber Issues is "ensuring a horizontal working platform providing for harmonisation and a unified approach on cyber policy issues", cooperation with other related working parties as well as with the European Commission, European External Action Service (EEAS), European Union Agency for Law Enforcement Cooperation (Europol), European Union Agency for Criminal Justice Cooperation (Eurojust), European Union Agency for Fundamental Rights (FRA), European Defence Agency (EDA), and European Union Agency for Cybersecurity (ENISA) means that the scope of issues addressed is broad and intensive (Council of the European Union, 2024). Whereas previously, meetings of the Horizontal Working Party on Cyber Issues were held once a week, they are now organised twice a week, underscoring the importance and relevance of cybersecurity issues (personal communication, 25 June 2024; 3 July 2024). It is also noteworthy that other working parties, such as the Working Party on Telecommunications and Information Society, have also addressed cyber-related questions within their scope (personal communication, June 25, 2024).

When analysing cyber diplomacy in the context of cybersecurity and the EU, it is essential to highlight the EU Cyber Diplomacy Toolbox, which is a joint EU diplomatic approach in cyberspace. In 2017, the Council of the European Union adopted the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") to enhance the EU's ability to prevent, discourage, deter, and respond to malicious cyber activities. One of the conclusions adopted by the Council of the European Union was as follows:

The EU recalls its conclusions on the EU Cybersecurity strategy, in particular its determination to keep cyberspace open, free, stable and secure where fundamental rights and the rule of law fully apply. It also recalls its Conclusions on Cyber Diplomacy, in particular that a common and comprehensive EU approach for cyber diplomacy could contribute to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations.

(Council of the European Union, 2017)

To strengthen EU positions on cybersecurity issues, the EU's Cyber Diplomacy Toolbox includes various collective measures aimed at addressing cyber threats through diplomatic channels. Among the key measures, political statements and declarations, diplomatic demarches, sanctions and restrictive measures, promotion of norms of responsible state behaviour, cyber incident response coordination stand out as crucial. Since the EU emphasises the critical importance of fostering and safeguarding a unified, open, free, and secure cyberspace (Council of the European Union, 2015), in Article 8 of the Revised implementing guidelines of the Cyber Diplomacy Toolbox, the Council also outlines the following:

The measures in the Cyber Diplomacy Toolbox could be used in tandem with other Union measures such as those reflected in the Network and Information Security Directive, the Directive on Attacks against Information Systems, as well as measures by EUIBAs, including by the EU Cybersecurity Agency (ENISA) and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU), and EU networks, in line with their legal mandates and institutional autonomy, to prevent, discourage, deter and respond to and immediately recover from malicious cyber activities which may originate from a state or non-state actor or transit through a States' territory. The measures could inter alia be used to encourage a State to ensure that its territory is not used for malicious cyber activities, or to induce a State to refrain from, or cease activities that are undertaken under its direction or its control.

(Council of the European Union, 2023)

The transnational nature of cybercrime, which is a driving force behind strengthening cyber diplomacy, necessitates a robust framework for conducting criminal investigations and prosecutions (Dragomir, 2021). Consequently, an important aspect of cyber diplomacy is responding to cyberattacks, and each country has its own approach to accountability and cyber incident attribution. In this context, it is important to note that different countries may have varying procedures regarding whether perpetrators are named and how they are identified. Some countries may choose to specifically name the responsible states or actors, while others may opt for expressing solidarity without attribution. The Latvian MFA closely monitors how cyber incident attribution unfolds internationally, such as within the EU, and takes on a coordinating role in this regard. As public attribution is inherently complex and involves various trade-offs (Egloff & Smeets, 2021), Latvian representatives focus on analysing cyber evidence and fostering international collaboration to ensure the accurate identification of perpetrators. Overall, this process involves a combination of technical analysis, diplomatic engagement, and international cooperation to address and attribute cyber incidents. According to Article 38 of the National Cybersecurity Law (2024), the Cabinet of Ministers will establish the criteria and procedures for Latvia's cyber incident attribution. At the same time, the new law stipulates that the Cabinet of Ministers must determine the criteria and procedures for cyber incident attribution by 1 April 2025.

In June 2020, the EU implemented its sanctions regime for the first time, with restrictive measures being enforced in July 2020 against six individuals and three entities from the Russian Federation and the People's Republic of China (Dragomir, 2021, p. 47). Since the establishment of the sanctions regime, the Latvian MFA has expressed solidarity with countries affected by cyber incidents, highlighting its commitment to responding to cyberattacks. One example is the joint statement from December 2023 (Latvijas Republikas Ārlietu ministrija), in which Latvia strongly condemns malicious cyber activities targeting democratic institutions and elections. This statement was issued by the High Representative on behalf of the European Union concerning the protection of democratic processes against malicious cyber activities.

While Latvia's most visible national cyber diplomacy activities are associated with active representation in the EU and UN, equally significant dimensions of cyber diplomacy are NATO and OSCE formats, as well as regional, bilateral, and specialised intergovernmental political formats. For instance, the Latvian MFA has regularly utilised NATO (Ministry of Foreign Affairs of the Republic of Latvia, 2021e) to address cybersecurity issues. At one such event, a side event of the NATO Foreign Ministers Meeting, the Minister of Foreign Affairs of Latvia, Edgars Rinkēvičs, highlighted the collective responsibility of NATO member states to confront these challenges:

We are in an everlasting and fierce competition with our adversaries in all domains of new and emerging challenges and threats. Be it hybrid, cyber, space or any new technology. The Allies have to be ready to address them. We see that hybrid actions have become a preferred and dominant *modus operandi* by our adversaries.

(Ministry of Foreign Affairs of the Republic of Latvia, 2021e)

Within the framework of the OSCE, Latvian diplomats have also advocated for a free, open, and secure cyberspace, including urging Russia to honour its international obligations and adhere to responsible state behaviour in cyberspace. For example, in the Statement of the Republic of Latvia at the OSCE Permanent Council, the Permanent Representative of Latvia, Ambassador Katrīna Kaktiņa, emphasised:

We call on Russia to respect their international obligations and commitments to uphold international law and act within the framework for responsible state behavior in cyberspace as affirmed by all members of the United Nations.

(Permanent Representation of the Republic of Latvia to the UN, OSCE and other international organizations in Vienna, 2024)

Cybersecurity, much like other current issues such as combating disinformation, is regularly addressed in bilateral relationship formats. In this context, it is crucial to highlight the yearly cybersecurity consultations between Baltic and US experts are conducted through close collaboration between Latvia's Ministry of

Foreign Affairs and the Ministry of Defence. Over the past ten years, the scope of these discussions has broadened significantly. For example, in 2021 (Ministry of Foreign Affairs of the Republic of Latvia, 2021c), the consultations covered various cyber threats, including ransomware, botnets, and 5G-related challenges. Furthermore, in these formats, Baltic and US experts also review the advancement of cybersecurity issues within international bodies such as the United Nations, the OSCE, the EU, and NATO (Ministry of Foreign Affairs of the Republic of Latvia, 2021c). The Latvian Ministry of Foreign Affairs has also addressed cyber threats and challenges in other bilateral meetings, such as those with Moldova, Greece, and the United Kingdom (Ministry of Foreign Affairs of the Republic of Latvia, 2022b, 2024a, 2021a).

Further, specialised intergovernmental political meetings have also addressed developments in cybersecurity, such as ransomware attacks, botnets, and challenges related to 5G, while highlighting advancements in cybersecurity within international organisations. One such meeting took place in October 2021, where Latvia, alongside Estonia, Lithuania, and the United States, gathered cyber experts to discuss ongoing concerns about state-sponsored cyber threats and issues related to the protection of critical infrastructure (Ministry of Foreign Affairs of the Republic of Latvia, 2021c). Another notable example is the international cybersecurity session hosted by Latvia in 2019 during an e-PINE (Enhanced Partnership in Northern Europe) meeting in Rīga (LSM.lv, 2019). Launched in 2003, the e-PINE format promotes cooperation between the Baltic, Nordic countries and the United States in security policy, neighbourhood policy, and economic relations. Further, it is important to note that the MFA has also regularly highlighted cybersecurity issues in other political and economic forums, such as the Nordic-Baltic Eight or NB8 (Ministry of Foreign Affairs of the Republic of Latvia, 2023d; LSM.lv, 2019), Three Seas Initiative (Ministry of Foreign Affairs of the Republic of Latvia, 2021d) and the Bucharest Nine (LSM.lv, 2024a).

Latvia's cyber diplomacy is characterised not only by the desire to establish international norms and regulations in cyberspace but also to achieve international agreement on the implementation of clear procedures, including issues related to attribution and sanctions. Highlighting ransomware as an example and the need for a coordinated response by the international community, Sanita Pavļuta-Deslandes, Ambassador and Permanent Representative of Latvia, to the United Nations notes that "the question is not about the rules governing cyberspace, but rather about ensuring their implementation" (Permanent Mission of the Republic of Latvia to the United Nations, 2024a).

Latvia has been implementing this approach, which focuses on establishing clear mechanisms internationally for addressing cybercrimes and ensuring accountability, including defining state responsibilities, in its cyber diplomacy for several years. One event that illustrates this is the e-PINE (Enhanced Partnership in Northern Europe) meeting of cyber experts hosted by Latvia's Ministry of Foreign Affairs in Rīga on 21 October 2019, which included representatives from the Baltic States, Nordic countries (NB8), and the United States of America (LSM.lv,

2019). The statement circulated by the Latvian MFA summarised the objective of the meeting, which is consistent and aligned with Latvia's national interests:

A special focus was placed on cyber security activities in the European Union (EU), including in the G5 context, and on cyber security related processes in the UN, which require an active and common approach by the member states in order to foster responsible behaviour of states in cyberspace.

(LSM.lv, 2019)

Through interviews with Latvia's cybersecurity and cyber diplomacy experts (personal communication, 25 June 2024; 3 July 2024) and in public statements, Latvia has actively contributed to enhancing cybersecurity within EU, UN, and regional political formats and has condemned irresponsible behaviour by certain states in the cyber ecosystem. For instance, Latvia's support for the EU's condemnation of malicious cyber activities originating from China is a notable example (Ministry of Foreign Affairs of the Republic of Latvia, 2019b). The Declaration by the High Representative on behalf of the EU, including Latvia's position, stated:

We have also detected malicious cyber activities with significant effects that targeted government institutions and political organisations in the EU and member states, as well as key European industries. These activities can be linked to the hacker groups known as Advanced Persistent Threat 40 and Advanced Persistent Threat 31 and have been conducted from the territory of China for the purpose of intellectual property theft and espionage.

(Council of the European Union, 2021)

Furthermore, in various international and regional political formats, Latvia emphasises the growing significance of digital technology and the corresponding rise in cyber risks, including the cyber dimension of Russia's war and aggression in Ukraine. As the Parliamentary Secretary of the Ministry of Foreign Affairs of Latvia states:

There is a growing number of cases where critical infrastructure, including critical information infrastructure, has been targeted in cyber-attacks threatening with catastrophic "real world" consequences. Furthermore, we have witnessed cyber-attacks to become integral part of Russia's full-scale aggression against Ukraine.

(Permanent Mission of the Republic of Latvia
to the United Nations, 2024b)

Reflecting on the last decade, Latvian foreign policy has been marked by a steadfast willingness to confront challenges head-on and communicate openly. In achieving its foreign policy goals, Latvia's cyber diplomacy exemplifies this approach. With the onset of Russia's war in Ukraine, the variety and tactics of cyberattacks have diversified. According to researchers at the Centre for Strategic and International

Studies (Mueller et al., 2023), recent years have seen Russian operations increasingly combine sophisticated espionage with criminal malware campaigns. Recognising that Russia has been behind a series of cyberattacks and that these actions are part of Russia's aggressive foreign policy and the war in Ukraine, the Latvian Ministry of Foreign Affairs has consistently highlighted in international, regional, and bilateral formats how these issues are closely interconnected. Emphasising Russia's war of aggression, there is a strong focus on the need for the EU and NATO, as well as cooperation with like-minded states, to support Ukraine and hold Russia accountable in all available international forums.

One event reflecting the holistic view of Latvian foreign policy towards Russian actions and cyber threats is the meeting between the Minister of Foreign Affairs, Baiba Braže, and the German Federal Minister for Foreign Affairs, Annalena Baerbock, during a working visit on 1 July 2024 in Berlin. In a discussion on security matters, the Latvian minister emphasised:

Russia's politics is war. Russia's foreign policy is becoming increasingly destabilizing, including through regular and increasingly aggressive hybrid threats and cyber-attacks, in a bid to cause anxiety among the public and raise doubts about the Allied support to Ukraine. We do not currently have any direct military threat, and this is thanks to Ukraine's success on the battlefield – Ukraine is also fighting for all of us.

(Ministry of Foreign Affairs of the Republic of Latvia, 2024b).

In this context, it is important to add that, describing the situation in Latvian cyberspace, the Constitution Protection Bureau (SAB), a state security service supervised by the Cabinet of Ministers in Latvia, highlighted in the Annual Public Report 2023 that “in most cases, the source of cyber threats was Russia” (The Constitution Protection Bureau (SAB), 2023). Additionally, in 2024, SAB has observed that Latvia and other European countries continue to face significant cyber threats from Russia and its supporting hacktivist groups. DDoS attacks persist against Latvia, targeting public institutions, critical infrastructure, and service providers, including those in the financial, transport, and communications sectors, as well as private companies (The Constitution Protection Bureau (SAB), 2024).

Taking the above into account, it can be concluded that Latvia's proactive and transparent stance in cyber diplomacy and its resolute condemnation of hostile cyber activities underscore its commitment to safeguarding both national and international cybersecurity, while reinforcing collective defence measures within international organisations such as the UN and EU, and utilising regional political formats and bilateral diplomatic opportunities.

Conclusion

One of the authors, describing how small states are engaged in norm entrepreneurship, writes that “an important element of cyber power is the ability to influence

and shape norms and regulation in relation to cyberspace and cybersecurity in particular” (Myatt, 2021, p. 252). Looking retrospectively at the work of the Latvian Ministry of Foreign Affairs over the past decade, and especially in recent years, one can observe a willingness and commitment to implement proactive cyber diplomacy, thus taking on an active role in the adaptation and development of new norms for state behaviour in cyberspace. One example of this political engagement is Latvia’s active involvement in the OEWG.

In recent years, one of the key activities in cyber diplomacy has increasingly focused on shaping and defining international norms, regulations, and standards in cyberspace. As the global technology ecosystem evolves and malicious cyberattacks become more frequent, Latvia’s cyber diplomacy is characterised by a firm stance and strong support for the application of international law and norms in cyberspace.

Examining cyber diplomacy from a national foreign policy perspective, it is important to highlight several political formats where the most significant activities were observed. At the international level, notable activities include those within the UN, particularly the OEWG, and the EU, especially in the context of the EU Cyber Diplomacy Toolbox. In addition to activities within NATO and the OSCE, regional formats, particularly e-PINE and NB8, are also significant. Furthermore, the Latvian Ministry of Foreign Affairs has engaged in bilateral meetings with like-minded countries to address cyber threats and agree on ways to strengthen international norms and regulations, as well as the principles of responsible state behaviour in cyberspace.

Analysing official statements and conducting consultations with Latvian cyber diplomacy and cybersecurity experts, several common aspects of Latvian cyber diplomacy can be identified. First, Latvian diplomats have consistently advocated the need for international and regional cooperation to tackle cybersecurity challenges. One of the best examples is how Latvia promotes the establishment of a permanent UN mechanism for cybersecurity to ensure continuous and structured dialogue and cooperation among states. As such, Latvia supports the proposal to establish the UN Programme of Action (PoA) on cybersecurity no later than 2026 (Permanent Mission of the Republic of Latvia to the United Nations, 2024a). Second, Latvia aligns its statements with broader EU positions on cybersecurity, indicating a coordinated regional approach, as well as with the broader objectives of the United Nations, particularly in enhancing global cybersecurity governance. Working in alignment with the statements of the EU and joint activities of like-minded countries at the OEWG, Latvia has repeatedly emphasised that cybersecurity matters deserve a permanent UN mechanism. Third, it is acknowledgement of increasing cyber threats and the need for proactive measures to combat the rising threats in cyberspace, including cyberattacks on critical infrastructure, state-sponsored threats, politically motivated attacks, and the misuse of technologies such as AI. In this context, Latvian officials in the UN and EU have also highlighted the importance of public education on cyber hygiene and the provision of cybersecurity tools. Fourth, Latvia supports practical, action-oriented initiatives such as training activities and providing assistance to states facing similar cybersecurity challenges.

Fifth, Latvia highlights the importance of multi-stakeholder engagement such as effective private-public partnerships and open dialogue among various stakeholders, including the private sector, civil society, and cross-sectoral representatives to harness all available expertise for cybersecurity efforts. Sixth, Latvian diplomats have been consistent in addressing the importance of capacity-building for enhancing global cyber resilience. For instance, in the UN format, Latvia stresses that a “one-size-fits-all” approach is not effective. Instead, capacity-building efforts should be customised to meet the specific needs and contexts of individual countries, especially small states (The GIP Digital Watch, 2024).

One aspect that hinders the implementation of a more comprehensive cyber diplomacy is related to the lack of human resources. In this context, it is important to note that the EU is working on new cybersecurity regulations, such as the Cyber Resilience Act, which requires manufacturers to place compliant products on the EU market by 2027. Implementation issues will require resources and establish the legal basis for cybersecurity. Both new regulations and the broad range of topics, as well as the emerging cybersecurity threats, indicate that the Latvian MFA will need to significantly strengthen its capacity in cyber diplomacy matters, given its horizontal dimension and the involvement of many stakeholders. Additionally, it is important to note another component of cyber diplomacy: communication whose role will only grow in the coming years. In the context of cybersecurity, communication is very important, as also noted by a senior cybersecurity and cyber diplomacy experts (personal communication, 25 June 2024; 3 July 2024). It is crucial for Latvia, as a small country, to ensure expertise, work on cyber regulations, be heard, understand the latest trends in cybersecurity, and involve the private sector.

Overall, evaluating the work and statements of the Latvian MFA, as well as consulting with Latvian cyber diplomacy and cybersecurity experts, it can be concluded that the MFA, as the leading state administration institution in foreign affairs, is active internationally and makes a significant contribution to Latvian state administration institutions. Moreover, this approach is consistent with Shaun Riordans (2016) observation that cyber diplomacy “should mean applying diplomatic methods and mindset to resolve issues in cyberspace”.

References

- Attatfa, A., Renaud, K., & Paoli S. D. (2020). Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science*, 176, 60–69. <https://doi.org/10.1016/j.procs.2020.08.007>
- Barrinha, A. (2024). Cyber-diplomacy: The Emergence of a Transient Field. *The Hague Journal of Diplomacy*, 19(3), 439–466. <https://doi.org/10.1163/1871191x-bja10183>
- Barrinha, A., & Renard, T. (2017). Cyber-Diplomacy: The Making of an International Society in the Digital Age. *Global Affairs*, 3(4–5), 353–364. <https://doi.org/10.1080/23340460.2017.1414924>
- Bousfield, D. (2017). Revisiting Cyber-Diplomacy: Canada–China Relations Online. *Globalizations*, 14(6), 1045–1059. <https://doi.org/10.1080/14747731.2017.1362176>
- Cornish, P. (Ed.). (2021). *The Oxford Handbook of Cyber Security*. Oxford Handbooks. <https://doi.org/10.1093/oxfordhb/9780198800682.001.0001>

- Council of the European Union. (2015). *Council conclusions on cyber diplomacy* (Document No. 6122/15). General Secretariat of the Council. <https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf>
- Council of the European Union. (2017). *Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities* ("Cyber Diplomacy Toolbox"), 19 June 2017 (Document No. 10474/17; previous document No. 9916/17). General Secretariat of the Council. <https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf>
- Council of the European Union. (2021, July 19). *China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory*. General Secretariat of the Council. <https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/>
- Council of the European Union. (2023). *Revised implementing guidelines of the Cyber Diplomacy Toolbox* (Document No. 10289/23). General Secretariat of the Council. <https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf>
- Council of the European Union. (2024, January 11). *Horizontal working party on cyber issues* (Cyber). <https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/horizontal-working-party-on-cyber-issues/>
- Egloff, F. J., & Smeets, M. (2021). Publicly Attributing Cyber Attacks: A Framework. *Journal of Strategic Studies*, 46(3), 502–533. <https://doi.org/10.1080/01402390.2021.1895117>
- European Space Agency. (2022, February 25). *Cyber resilience for space*. https://www.esa.int/Space_Safety/Cyber_resilience/Cyber_resilience2
- European Space Agency. (2023, October 15). *ESA security for space: Shaping the future, protecting the present*, (ESA-ESO-PL-2023–0068). ESA Security Office. https://esamultimedia.esa.int/docs/corporate/ESA_Cyber_Security_Resilience_Achievement.pdf
- European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. <https://doi.org/10.2824/782573>
- Feakin, T., & Weaver, J. (2020). Cyber Diplomacy: An Australian Perspective. In E. Tikk, & M. Kerttunen (Eds.), *Routledge Handbook of International Cybersecurity* (1st ed., pp. 277–285). Routledge. <https://doi.org/10.4324/9781351038904>
- Ford, C. A. (2022). Conceptualizing Cyberspace Security Diplomacy. *The Cyber Defense Review*, 7(2), 35–53.
- Hocking, B. (2002). Introduction: Gatekeepers and Boundary-Spanners – Thinking about Foreign Ministries in the European Union. In B. Hocking, & D. Spence (Eds.), *Foreign Ministries in the European Union: integrating diplomats* (1st ed., pp. 1–17). Palgrave Macmillan.
- Hocking, B. (2002). Introduction: Gatekeepers and Boundary-Spanners – Thinking about Foreign Ministries in the European Union. In B. Hocking, & D. Spence (Eds.), *Foreign Ministries in the European Union: Integrating Diplomats* (1st ed., pp. 1–17). Palgrave Macmillan.
- Invest in Estonia. (2017, June). *How Estonia became a global heavyweight in cyber security*. <https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/>
- Jacobsen, J. T. (2024). Commitment and Compromise in Danish Cyber and Tech Diplomacy. *International Affairs*, 100(6), 2361–2378. <https://doi.org/10.1093/ia/iaae235>
- Kasper, A., Osula, A.-M., & Molnár, A. (2021). EU Cybersecurity and Cyber Diplomacy. *IDP Journal of Internet, Law and Politics*, 34, 1–15.
- Kello, L. (2024). Digital Diplomacy and Cyber Defence. In C. Bjola, & I. Manor (Eds.), *The Oxford Handbook of Digital Diplomacy* (1st ed., pp. 121–137). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780192859198.001.0001>

- Lancelot, J. F. (2020). Cyber-Diplomacy: Cyberwarfare and the Rules of Engagement. *Journal of Cyber Security Technology*, 4(4), 240–254. <https://doi.org/10.1080/23742917.2020.1798155>
- Latvijas Republikas Ārlietu ministrija. (2008). *Ārlietu ministrijas 2007. gada darba pārskats* [Ministry of Foreign Affairs 2007 Annual Report]. <https://www.mfa.gov.lv/lv/arhivs>
- Latvijas Republikas Ārlietu ministrija. (2013). *Publiskais pārskats* [Public Report]. <https://www.mfa.gov.lv/lv/arhivs>
- Latvijas Republikas Ārlietu ministrija. (2022). *Ārlietu ministrijas publiskais pārskats* [Ministry of Foreign Affairs Public Report]. <https://www.mfa.gov.lv/lv/arlietu-ministrijas-publiskais-parskats>
- Latvijas Republikas Ārlietu ministrija. (2023, December 7). *Kopīgā paziņojumā Latvija stingri nosoda ļaunprātīgas kiberaktivitātes pret demokrātiskām institūcijām un vēlēšanām* [In a joint statement, Latvia strongly condemns malicious cyber activities targeting democratic institutions and elections]. <https://www.mfa.gov.lv/lv/jaunums/kopiga-pazinojuma-latvija-stingri-nosoda-ļauņpratiņas-kiberaktivitates-pret-demokratiskam-institucijam-un-velesanam>
- LSM.lv (2019, October 23). *Latvia hosts international cyber security session*. LSM.lv. <https://eng.lsm.lv/article/politics/diplomacy/latvia-hosts-international-cyber-security-session.a336030/>
- LSM.lv. (2024a, June 11). *Rīga B9 summit releases 'Chairs Statement'*. LSM.lv. <https://eng.lsm.lv/article/politics/president/11.06.2024-riga-b9-summit-releases-chairs-statement.a557646/>
- LSM.lv. (2024b, September 6). *National Cybersecurity Center is up and running*. LSM.lv. <https://eng.lsm.lv/article/society/defense/06.09.2024-national-cybersecurity-center-is-up-and-running.a567810/>
- LSM.lv. (2024c, October 15). *CERT: Latvia sees highest level of cyberattacks in two years*. LSM.lv. <https://eng.lsm.lv/article/society/crime/15.10.2024-cert-latvia-sees-highest-level-of-cyberattacks-in-two-years.a572581/>
- Manantan, M. B. F. (2021). Advancing Cyber Diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*, 75(4), 432–459. <https://doi.org/10.1080/10357718.2021.1926423>
- Ministry of Defence of the Republic of Latvia. (2014). *Cyber Security Strategy of Latvia 2014–2018*. <https://www.coe.int/en/web/octopus/-/latvia>
- Ministry of Defence of the Republic of Latvia. (2019). *Cybersecurity Strategy of Latvia 2019–2022*. <https://www.mod.gov.lv/en/cybersecurity>
- Ministry of Defence of the Republic of Latvia. (2023). *The Cybersecurity Strategy of Latvia 2023–2026*. <https://www.mod.gov.lv/en/cybersecurity>
- Ministry of Foreign Affairs of the Republic of Latvia. (2014a). *Annual Report by the Minister of Foreign Affairs on activities performed and planned in national foreign policy and European Union matters* [2013–2014]. <https://www.mfa.gov.lv/en/arlietu-ministra-ikgadejais-zinojums/arhivs>
- Ministry of Foreign Affairs of the Republic of Latvia. (2014b, January 24). *Speech by the Minister of Foreign Affairs of the Republic of Latvia Mr. Edgars Rinkēvičs at the Foreign Policy Debate in the Saeima, 24 January 2014*. <https://www.mfa.gov.lv/en/article/speech-minister-foreign-affairs-republic-latvia-mr-edgars-rinkevics-foreign-policy-debate-saeima-24-january-2014>
- Ministry of Foreign Affairs of the Republic of Latvia. (2015a). *Annual Report by the Minister of Foreign Affairs on accomplishments and activities planned with respect to national foreign policy and the European Union* [2014–2015]. <https://www.mfa.gov.lv/en/arlietu-ministra-ikgadejais-zinojums/arhivs>

- Ministry of Foreign Affairs of the Republic of Latvia. (2016a). *Annual Report on accomplishments and further work with respect to national foreign policy and the European Union*. <https://www.mfa.gov.lv/en/arlietu-ministra-ikgadejais-zinojums/arhivs>
- Ministry of Foreign Affairs of the Republic of Latvia. (2017a). *Annual Report on accomplishments and further work with respect to national foreign policy and the European Union*. <https://www.mfa.gov.lv/en/arlietu-ministra-ikgadejais-zinojums/arhivs>
- Ministry of Foreign Affairs of the Republic of Latvia. (2018a). *Annual Report of the Minister of Foreign Affairs on the accomplishments and further work with respect to national foreign policy and the European Union*. <https://www.mfa.gov.lv/en/arlietu-ministra-ikgadejais-zinojums/arhivs>
- Ministry of Foreign Affairs of the Republic of Latvia. (2019a). *Annual Report of the Minister of Foreign Affairs on the accomplishments and further work with respect to national foreign policy and the European Union*. <https://www.mfa.gov.lv/en/arlietu-ministra-ikgadejais-zinojums/arhivs>
- Ministry of Foreign Affairs of the Republic of Latvia. (2020a). *Annual Report of the Minister of Foreign Affairs on the accomplishments and further work with respect to national foreign policy and the European Union*. <https://www.mfa.gov.lv/en/arlietu-ministra-ikgadejais-zinojums/arhivs>
- Ministry of Foreign Affairs of the Republic of Latvia. (2021a). *Annual Report of the Minister of Foreign Affairs on the accomplishments and further work with respect to national foreign policy and the European Union*. <https://www.mfa.gov.lv/en/arlietu-ministra-ikgadejais-zinojums/arhivs>
- Ministry of Foreign Affairs of the Republic of Latvia. (2021b, July 19). *Latvia raises its concern about irresponsible behavior in cyberspace*. <https://www.mfa.gov.lv/en/article/latvia-raises-its-concern-about-irresponsible-behavior-cyberspace>
- Ministry of Foreign Affairs of the Republic of Latvia. (2021c, October 22). *The Baltic and U.S. experts discuss cyber security challenges*. Ministry of Foreign Affairs of the Republic of Latvia. <https://www.mfa.gov.lv/en/article/baltic-and-us-experts-discuss-cyber-security-challenges>
- Ministry of Foreign Affairs of the Republic of Latvia. (2021d, September 3). *At the European Cyber security Forum, the State Secretary underlines the importance of a secure digital environment in the Three Seas Initiative Region*. <https://www.mfa.gov.lv/en/article/european-cyber-security-forum-state-secretary-underlines-importance-secure-digital-environment-three-seas-initiative-region>
- Ministry of Foreign Affairs of the Republic of Latvia. (2021e, November 3). *NATO Foreign Ministers to meet in Riga*. <https://www.mfa.gov.lv/en/article/nato-foreign-ministers-meet-riga>
- Ministry of Foreign Affairs of the Republic of Latvia. (2021f, November 30). *Speech by the Minister of Foreign Affairs of the Republic of Latvia Mr. Edgars Rinkēvičs at side event of NATO Foreign Ministers Meeting*. <https://www.mfa.gov.lv/en/article/speech-minister-foreign-affairs-republic-latvia-mr-edgars-rinkevics-side-event-nato-foreign-ministers-meeting>
- Ministry of Foreign Affairs of the Republic of Latvia. (2022a). *Annual Report of the Minister of Foreign Affairs on the accomplishments and further work with respect to national foreign policy and the European Union*. <https://www.mfa.gov.lv/en/arlietu-ministra-ikgadejais-zinojums/arhivs>
- Ministry of Foreign Affairs of the Republic of Latvia. (2022b, October 13). *The Foreign Minister: Latvia will share its experience and support Moldova in digitalization*. <https://www.mfa.gov.lv/en/article/foreign-minister-latvia-will-share-its-experience-and-support-moldova-digitalisation>

- Ministry of Foreign Affairs of the Republic of Latvia. (2023a). *Annual Report of the Foreign Minister on the accomplishments and further work with respect to national foreign policy and the European Union*. <https://www.mfa.gov.lv/en/foreign-ministers-annual-report>
- Ministry of Foreign Affairs of the Republic of Latvia. (2023b, September 11). *Latvia's candidacy to the United Nations Security Council (2026–2027)*. <https://www.mfa.gov.lv/en/latvias-candidacy-to-the-united-nations-security-council-2026-2027>
- Ministry of Foreign Affairs of the Republic of Latvia. (2023c, November 10). *The campaign of Latvia's candidacy for the United Nations Security Council officially launched in New York*. <https://www.mfa.gov.lv/en/article/campaign-latvias-candidacy-united-nations-security-council-officially-launched-new-york>
- Ministry of Foreign Affairs of the Republic of Latvia. (2023d, December 7). *Riga hosts an NB8 meeting on challenges posed by hybrid threats*. <https://www.mfa.gov.lv/en/article/riga-hosts-nb8-meeting-challenges-posed-hybrid-threats>
- Ministry of Foreign Affairs of the Republic of Latvia. (2024a, March 28). *Strengthening of cooperation in multilateral formats discussed in consultations in Greece*. <https://www.mfa.gov.lv/en/article/strengthening-cooperation-multilateral-formats-discussed-consultations-greece>
- Ministry of Foreign Affairs of the Republic of Latvia. (2024b, July 1). *The Foreign Ministers of Latvia and Germany Baiba Braže and Annalena Baerbock: the security of our countries is indivisible, and contribution to defence is also contribution to economy and welfare*. <https://www.mfa.gov.lv/en/article/foreign-ministers-latvia-and-germany-baiba-braze-and-annalena-baerbock-security-our-countries-indivisible-and-contribution-defence-also-contribution-economy-and-welfare>
- Ministry of Foreign Affairs of the Republic of Latvia. (2024c, July 10). *Latvia organizes a thematic discussion at the UN on strengthening resilience in cyberspace*. <https://www.mfa.gov.lv/en/article/latvia-organizes-thematic-discussion-un-strengthening-resilience-cyberspace>
- Ministry of Foreign Affairs of the Republic of Latvia. (2024d, July 16). *Latvia stands up for the protection of values enshrined in the UN Charter and accountability for international crime*. <https://www.mfa.gov.lv/en/article/latvia-stands-protection-values-enshrined-un-charter-and-accountability-international-crime>
- Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). *Cyber operations during the Russo-Ukrainian War: From strange patterns to alternative futures*. Center for Strategic and International Studies (CSIS). <https://www.jstor.org/stable/resrep52130>
- Myatt, M. (2021). Small, Smart, Powerful? Small States and the Competition for Cybertech Superiority in the Digital Age. Madeleine . D. Russ, J. Stafford (Eds.), *Competition in World Politics: Knowledge, Strategies and Institutions* (1st ed., pp. 233–260). transcript Verlag. <https://doi.org/10.1515/9783839457474-011>
- Nacionālās kiberdrošības likums [National Cybersecurity Law], 2024/128A.1 (2024). <https://www.vestnesis.lv/op/2024/128A.1>
- Pahlavi, P. C. (2003, May 30). *Cyber-diplomacy: A new strategy of influence*. Paper presented at the Canadian Political Science Association General Meeting, Halifax, Nova Scotia.
- Permanent Mission of the Republic of Latvia to the United Nations. (2024a, April 5). *Statement during Arrria-formula Meeting on “Cyber Security Evolving Cyberthreat Landscape and its Implications for the Maintenance of International Peace and Security” by Permanent Representative of Latvia, Ambassador H.E. Ms. Sanita Pavļuta-Deslandes*. Permanent Mission of the Republic of Latvia to the United Nations. <https://www2.mfa.gov.lv/en/newyork/statements/statements-at-the-general-assembly-general-debate>

- Permanent Mission of the Republic of Latvia to the United Nations. (2024b, June 20). *Statement at the Security Council High Level-Open Debate on "Maintenance of International Peace and Security: Addressing Evolving Threats in Cyberspace"* by Parliamentary Secretary of the Ministry of Foreign Affairs of Latvia, Dace Melbārde. Permanent Mission of the Republic of Latvia to the United Nations. <https://www2.mfa.gov.lv/en/newyork/statements/statements-at-the-general-assembly-general-debate>
- Permanent Representation of the Republic of Latvia to the UN, OSCE and other international organizations in Vienna. (2024, May 16). *Statement of the Republic of Latvia at the OSCE Permanent Council No.1473, 16 May 2024*. <https://www2.mfa.gov.lv/en/vienna/news/71237-statement-of-the-republic-of-latvia-at-the-osce-permanent-council-no-1473-16-may-2026>
- Potter, E. H. (2002). *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. McGill-Queen's University Press.
- Radanliev, P. (2024). Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks From Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, 1–51. <https://doi.org/10.1080/23742917.2024.2312671>
- Riordan, S. (2016, May 12). Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction. <https://uscpublishediplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction>
- Riordan, S. (2019). *Cyberdiplomacy: Managing Security and Governance Online* (1st ed.). Polity.
- Tamkin, E. (2017, April 27). Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? *Foreign Policy*. <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>
- The Constitution Protection Bureau (SAB). (2023). *Annual public report 2023*. <https://www.sab.gov.lv/en/annual-reports/>
- The Constitution Protection Bureau (SAB). (2024, May 15). *Russia's hybrid threats: Trends and developments*. <https://www.sab.gov.lv/en/news/russias-hybrid-threats-trends-and-developments/>
- The GIP Digital Watch. (2024, May 10). *Global roundtable on ICT security capacity-building*. <https://dig.watch/event/global-roundtable-on-ict-security-capacity-building>
- Tikk, W. & Kerttunen, M. (2020). (Eds.). *Routledge Handbook of International Cybersecurity* (1st ed.). Routledge. <https://doi.org/10.4324/9781351038904>
- UNIDIR. (2024, June 27). *Accelerating ICT security capacity-building: Takeaways from the Global Roundtable on ICT Security Capacity-Building*. <https://unidir.org/publication/accelerating-ict-security-capacity-building-take-aways-from-the-global-roundtable-on-ict-security-capacity-building/>
- United Nations. (2018). *Developments in the field of information and telecommunications in the context of international security: Resolution adopted by the General Assembly (A/RES/73/27)*. <https://digitallibrary.un.org/record/1655670?v=pdf>
- Wight, M. (1979). *Power politics*. Royal Institute of International Affairs.

9 Cybersecurity Transformation in Latvia

Heinrihs K. Skrodelis, Mārtiņš Štāls and Andrejs Romānovs

Introduction

In an era marked by rapid digitization and enhanced digital interconnectedness, cybersecurity has emerged as an integral facet of national and corporate strategies worldwide. As countries, including Latvia, progressively translocate their operations into the digital realm, the imperative to secure digital infrastructures against advanced cyber threats has grown substantially. Despite cybersecurity being perceived as a key concern by a significant majority (75%) of industry experts, a mere 16% believe that their organization is aptly equipped to counteract these cyber challenges (Iaiani et al., 2021). The potential financial impact of these deficiencies in cybersecurity measures is substantial.

Regrettably, numerous institutions continue to adhere to a reactive posture with regard to cybersecurity, invariably leading to their security frameworks trailing the rapid progression of business and digital technology norms. It is absolutely crucial that there is a strategic redirection toward a transformative approach to cybersecurity (Grima et al., 2023). This adaptation should involve proactive strategies for rapidly mitigating cyber risks and integrating budding digital technologies with confidence, and in a manner that aligns with organizational and national strategic goals.

In a world where technology advancements and the growth in digital interconnectivity have given birth to a new era of intricate and widespread cyberattacks, swift and decisive action is needed. Modern technological developments have equipped cybercriminals with tools to automate and launch more sophisticated attacks (Sarker, 2023). The rapid expansion of the digital landscape, encompassing smartphone usage, tablets, Internet of Things devices, cloud computing platforms, and social media, amongst others, has amplified the potential arenas for cyberattacks.

Historically, cybercrime has undergone a drastic evolution, from modest pranks to intricate and damaging attacks, which results in significant economic costs estimated to be in trillions annually on a global scale. It is imperative to study and address these evolutions as part of the broader discourse concerning cybersecurity (Mallick & Nath, 2024).

This chapter delves into the evolution of Latvia's cybersecurity landscape, offering a comprehensive analysis of its current state, identifying predominant challenges, and projecting future developments. It aims to provide insights into how

Latvia can fortify its cybersecurity measures to ensure a resilient digital environment for its citizens and enterprises.

Literature Review

The exploration of cybersecurity in the digital era, particularly within the context of Latvia, reveals a complex landscape shaped by various factors including legislative frameworks, institutional responses, and the evolving nature of cyber threats. This literature review synthesizes existing research to provide a comprehensive understanding of these dynamics, focusing on the current challenges faced by Latvia and the measures being implemented to enhance its cybersecurity posture.

Latvia's cybersecurity framework is significantly influenced by its membership in the European Union (EU) and NATO, which necessitates compliance with broader regional cybersecurity policies. The EU Cybersecurity Act has established a foundational legal framework that mandates member states to enhance their cybersecurity capabilities, thereby fostering cooperation among nations. This act is complemented by Latvia's National Cybersecurity Law, which outlines specific responsibilities and protocols for both public and private sectors in managing cyber threats (Done, 2022).

The challenges Latvia faces in the realm of cybersecurity are multifaceted. The increasing sophistication of cyberattacks, particularly in the wake of the COVID-19 pandemic, has underscored the need for proactive measures and collaborative approaches to cybersecurity (Haryanto & Ramli, 2023). Research indicates that traditional cybersecurity measures are often insufficient to combat the dynamic nature of these threats, necessitating the integration of advanced technologies such as artificial intelligence (AI) and machine learning (ML) to enhance detection and response capabilities (Pissanidis, 2024). Moreover, the literature highlights the importance of human factors in cybersecurity, emphasizing that individual behaviors and decision-making processes significantly influence vulnerability to cyber threats (Skrodelis et al., 2020).

The centralization of cybersecurity efforts has emerged as a key trend in Latvia's approach to managing cyber risks. This trend is characterized by the consolidation of resources and expertise within centralized institutions, which can lead to improved coordination and efficiency in responding to cyber incidents (Yanakiev, 2020). However, this centralization also poses risks, including potential bottlenecks in decision-making and the challenge of ensuring that localized needs are adequately addressed (Górka, 2023). The balance between centralization and decentralization is critical, as it impacts the overall effectiveness of cybersecurity strategies in addressing both national and regional threats.

In examining the case studies of major Latvian organizations, it becomes evident that cybersecurity practices vary significantly across sectors. These organizations face unique challenges, influenced by their operational contexts and the specific threats they encounter. For instance, the financial sector may prioritize compliance with stringent regulatory requirements, while the healthcare sector must navigate the complexities of protecting sensitive patient data amidst increasing cyber threats

(Volkova et al., 2021). By situating these case studies within the broader context of global cybersecurity trends, the research highlights the interconnectedness of local and global cybersecurity landscapes, illustrating how international events can influence national strategies (Done, 2022).

The literature also emphasizes the importance of continuous capacity building in enhancing Latvia's cybersecurity resilience. Comparative studies indicate that a nation's wealth and the robustness of its internet infrastructure are critical determinants of its cybersecurity capacity (Creese et al., 2021). As such, Latvia's ongoing investments in digital infrastructure and cybersecurity training initiatives are essential for fostering a culture of security awareness and preparedness among its citizens and organizations (Siemers et al., 2021).

In conclusion, the exploration of cybersecurity in Latvia reveals a dynamic interplay between legislative frameworks, institutional responses, and the challenges posed by an increasingly complex cyber threat environment. The integration of advanced technologies, the centralization of cybersecurity efforts, and the importance of international cooperation are critical components of Latvia's strategy to enhance its cybersecurity resilience. By examining the distinctive practices and challenges faced by major organizations within the country, this research contributes valuable insights into the broader context of global cybersecurity trends and their implications for local practices.

Methods and Approach

This study employs a qualitative, multiple-case study design to examine cybersecurity transformations within Latvian organizations. A case study method is particularly suited for exploring complex, context-dependent phenomena such as national-level cyber resilience and evolving organizational security measures (Yin, 2018). The objective is to generate in-depth insights into cybersecurity practices and challenges across diverse sectors in Latvia.

Five major Latvian organizations were selected using purposive sampling to capture a broad spectrum of cybersecurity experiences and strategic responses. The chosen organizations include:

- Tet: A leading telecommunications and internet service provider.
- Riga Technical University (RTU): The oldest technical university in the Baltic region.
- Latvia University of Life Sciences and Technologies (LBTU): A key institution representing the academic sector.
- Latvijas Mobilais Telefons (LMT): A state-controlled telecommunications company.
- Latvian State Radio and Television Centre (LVRTC): A central entity in public communications and data services.

This selection was guided by criteria outlined by Stake (1995), which recommend choosing cases that provide contrasting perspectives on the phenomenon under

investigation. By including both public and private sector organizations from different industries, the study ensures that the findings reflect the multifaceted nature of Latvia's cybersecurity landscape.

Data were collected using a triangulation of methods to enhance the robustness and validity of the findings (Creswell, 2013). The primary method was semi-structured expert interviews, supplemented by document analysis and direct observations. Specific procedures included:

- **Semi-Structured Interviews:** Approximately 25 in-depth interviews were conducted in total, with each organization contributing between 4 and 6 key participants. Interviewees were selected based on their roles in cybersecurity and IT operations—ranging from cybersecurity managers and IT specialists to senior executives and policymakers. This approach ensured a comprehensive perspective on both strategic and operational cybersecurity challenges.
- **Document Analysis:** Internal policies, public reports, and relevant legislative documents were reviewed to contextualize the cybersecurity measures and strategic directions adopted by the organizations.
- **Direct Observations:** Participation in select cybersecurity forums and events provided additional insights into industry practices and emerging trends.

All interview transcripts and documents were systematically coded and analyzed using thematic analysis. This process enabled the identification of recurring patterns and themes related to cybersecurity strategies, regulatory compliance, and risk mitigation efforts (Braun & Clarke, 2023). Data were then compared across the five cases to discern both shared trends and unique organizational responses, contributing to a richer understanding of Latvia's overall cybersecurity framework.

Global Cybersecurity Landscape

The cybersecurity landscape today is marked by the continuous emergence of sophisticated, new, and diverse cyber threats that affect both individuals and organizations (Doğrul et al., 2023). Recognizing the crucial role of cybersecurity in countering these threats and safeguarding citizens, infrastructure, and future sustainability, nations worldwide are making substantial investments in this area.

However, the strategic cybersecurity landscape presents several challenges, each characterized by its complexity and the evolving nature of digital threats (Möller, 2023). These challenges differ fundamentally from conventional cybersecurity risks and necessitate a deeper understanding and tailored responses. For example, the complexity of strategic cybersecurity challenges requires a nuanced approach for effective management and mitigation. In turn, this complex landscape aids governments in allocating resources more effectively and implementing appropriate defense strategies.

The ever-changing landscape of cyber threats demands continuous adaptation and innovation in cybersecurity strategies to address new vulnerabilities and attack vectors. This evolution necessitates a novel taxonomy to classify and categorize

these strategic cybersecurity challenges, enriching the understanding of the cybersecurity environment and aiding in the development of more effective strategies (Ogugua Chimezie Obi et al., 2024; Sendjaja et al., 2024). Addressing these challenges is crucial for nations to enhance their cybersecurity posture and resilience against sophisticated threats in the digital realm.

The report by World Economic Forum and Accenture (2024) offers an in-depth analysis of the current state of cybersecurity challenges and opportunities facing organizations worldwide. It highlights several key themes such as cyber inequity, geopolitical and technological transitions, cyber skills shortage, cyber resilience, and the need for public-private collaboration. The report serves as a call to action for leaders to recognize these challenges and work collaboratively towards a more secure and resilient digital future. Additionally, the report provides several recommendations for enhancing cyber resilience. For instance, integrating cybersecurity into enterprise risk management, gaining executive leadership buy-in, focusing on cyber-resilience essentials, building collaborative ecosystems, understanding third-party risks, and investing in cyber insurance. Implementing these recommendations can help organizations better prepare for and respond to cyber threats, ultimately enhancing their resilience in an increasingly complex digital landscape.

Similarly, the ENISA (2023) report outlines several cyberattack trends observed recently. These include the escalation in cybersecurity attacks, the rise of ransomware groups, the expansion of hacktivism, a diverse threat landscape, and the impact on critical sectors. Likewise, the World Economic Forum report identifies several key trends in cyberattacks, such as an increase in sophistication of attacks, rise in ransomware and cyber extortion, exploitation of emerging technologies, third-party vulnerabilities, growing exposure to cybercrime, and increased targeting of critical infrastructure.

Moreover, the integration of cybersecurity into organizational strategy has gained prominence. Rattanapong and Ayuthaya (2025) argue that collaboration between cybersecurity professionals and executives is critical for developing robust cybersecurity strategies that align with organizational goals. This alignment is increasingly vital as businesses transition to digital enterprises, necessitating a proactive stance on cybersecurity investments and awareness. Abrahams et al. (2023) further explore this intersection, noting that the integration of cybersecurity with accounting practices is essential for maintaining data confidentiality and financial security in a digitized economy.

The need for adaptive cybersecurity cultures is underscored by Gundu (2024), who proposes a model that emphasizes continuous learning and adaptation to counter evolving threats. This is particularly relevant in the context of remote work, which has proliferated since the COVID-19 pandemic, exposing organizations to new vulnerabilities and necessitating robust cybersecurity measures (Treacy et al., 2023).

Overall, the current cybersecurity landscape is complex and rapidly evolving, marked by an increase in cyber threats and strategic challenges. By implementing recommendations to enhance cyber resilience, integrating cybersecurity into organizational strategies, and fostering adaptive cybersecurity cultures, nations and organizations can work towards a more secure and resilient digital future.

Current Cybersecurity Landscape and Strategic Directions in Latvia

Latvia's cybersecurity landscape is experiencing dynamic changes, driven by both emerging threats and technological advancements. Insights from the CERT.lv report (CERT.lv, 2023) and the nation's Cybersecurity Strategy for 2023–2026 (Aizsardzības ministrija, 2023) reveal several pivotal trends shaping the country's approach to cyber defense.

Among the most pressing concerns are supply chain attacks, which are anticipated to persist as a formidable challenge. This necessitates not only internal vigilance but also stringent monitoring of cybersecurity practices among suppliers. The intensity of cyberattacks is expected to remain high, demanding continuous preparedness and robust defensive mechanisms.

A significant portion of these attacks can be attributed to Russia-linked hacktivists, who pose substantial threats through organized Distributed Denial-of-Service (DDoS) attacks targeting Latvia and other EU and NATO members. These activities are often politically motivated, aligning with Russia's broader geopolitical objectives.

The National Cyber Security Index (NCSI) serves as an authoritative metric reflecting the preparedness of countries to preemptively address cyber threats and manage cyber incidents. This index, focusing on aspects implemented by central governments across four primary pillars—legislation in force, established units, cooperation formats, and outcomes—positions Latvia as a leader in the realm of cybersecurity. Currently, Latvia holds the 12th rank in the NCSI and 15th in the Global Cybersecurity Index (NCSI, 2023), demonstrating the nation's robust cybersecurity policies. These include formidable protection of critical information infrastructure, comprehensive cyber threat analysis, efficient personal data protection, and stringent measures against cybercrime. However, areas necessitating further enhancement include military cyber defense capabilities, crisis management in cyber contexts, global contributions to cybersecurity, and research and development initiatives in this sphere.

The evolving role of AI and ML is also set to revolutionize cybersecurity (Swain et al., 2022). AI and ML offer advanced solutions for protecting extensive networks and critical infrastructure by enabling real-time anomaly detection and automated incident response (Skrodelis et al., 2024).

Latvia's Cybersecurity Strategy highlights the critical need to adapt to new digital technologies, including AI, big data, quantum computing, 5G, and even the emerging 6G. These advancements bring about new cybersecurity requirements, making it imperative for both public and private sectors to proactively secure valuable information and digital infrastructures. The evolving landscape also underscores the importance of cultivating specialized cybersecurity professionals to meet the growing demands.

The strategic trajectory emphasizes the development of international collaborations and intelligence-sharing protocols to enhance collective cybersecurity resilience. Integrating this multifaceted approach underscores Latvia's commitment

to fortifying its cybersecurity posture amidst a rapidly evolving threat landscape. Therefore, continued investment in cybersecurity education, research, and innovation, coupled with strategic policy enactment, is indispensable for safeguarding Latvia's digital future (Bērziņš, 2023).

The legislative and compliance frameworks discussed above do more than just ensure basic cybersecurity standards; they also set the boundaries within which organizations pursue broader strategic objectives. As we will see in the following section, these same regulations can serve both as catalysts and as guardrails for centralized cybersecurity approaches streamlining resource allocation but also introducing certain operational risks.

Compliance Landscape and Legislative Initiatives

As global dependence on digital technologies grows, so too does the sophistication and frequency of cyberattacks. Governments and industries alike face escalating cybersecurity risks that threaten critical infrastructure, disrupt essential services, and compromise sensitive data. Against this backdrop, the EU has taken significant steps to coordinate cybersecurity measures across Member States. The goal is to establish common standards, streamline compliance requirements, and foster cross-border cooperation in preventing and responding to cyber threats (Salvaggio & González, 2023).

A central component of this approach involves harmonizing legal frameworks and clearly defining the responsibilities of governments and organizations in protecting digital assets. Several directives and regulations have emerged in recent years, reflecting the EU's commitment to bolstering collective cyber resilience. These initiatives also provide guidance on effective governance, risk management, and reporting structures. By encouraging Member States to align their national legislation with overarching EU objectives, the EU aims to create a level playing field that not only deters cyber threats but also underpins secure digital growth.

The following list outlines key EU and Latvian legislative measures that shape the cybersecurity landscape, highlighting how these laws work together to enhance digital security and resilience across Europe.

- **The EU Cybersecurity Act**

A cornerstone of this legislative framework is the EU Cybersecurity Act, which bolsters the cybersecurity infrastructure across EU Member States (The EU Cybersecurity Act, 2019). The Act enhances the mandate of the EU Agency for Cybersecurity (ENISA) and establishes a comprehensive certification scheme for a broad spectrum of ICT products, services, and processes. Under this scheme, certifications issued in one Member State are recognized throughout the EU, thereby streamlining compliance efforts for organizations operating within multiple jurisdictions.

- **National Cybersecurity Law (NCL) of Latvia**

On September 1, 2024, the previous “Information Technology Security Law” was repealed and replaced with the new “National Cybersecurity Law”. This transition echoed the provisions of the Council of the European Union Directive (EU) 2022/2555 (NIS2), adopted on December 14, 2022, aiming to enhance resilience among EU companies, standardizing cybersecurity protection procedures, and fostering cooperation among member states (*Nacionālās Kiberdrošības Likums*, 2024).

- **National Cybersecurity Center (NKDC)**

The National Cybersecurity Law also outlines the functions and authority of the newly formed NKDC, situated under the Ministry of Defense. As the central point of contact for cybersecurity incidents and inquiries, the NKDC takes the lead on national cybersecurity management, policy development, and international cooperation (Ministru kabinets, 2022a). Furthermore, Article 13, Section 3 of the Law mandates regular information-sharing among the NKDC and other relevant institutions, thereby enhancing coordination and fortifying Latvia’s overall cybersecurity posture.

- **Cybersecurity Strategy of Latvia for 2023–2026**

Latvia’s vision for a robust cyber environment is articulated in the informational report “On the Cybersecurity Strategy of Latvia for 2023–2026”. This strategy underscores the newly assigned responsibilities stemming from NIS2 implementation, aligning them with national legislation and the mandates of key institutions (Ministru kabinets, 2023). By establishing a cohesive vision and designating clear roles, the strategy seeks to build a secure and trustworthy digital ecosystem within the country. By incorporating these legislative edicts and institutional frameworks, Latvia, along with other EU nations, is fostering a robust and resilient cybersecurity infrastructure. This not only deters cyber threats but also provides a solid platform for continued digital growth and development in the future.

The Centralization of Cybersecurity: Benefits and Risks

The technological developments and resource efficiency considerations in recent times have heralded a wave of centralization in many aspects of IT operations. While centralization offers benefits like resource savings, streamlined services, and better cybersecurity in certain aspects, it also introduces a myriad of risks and challenges (Liu et al., 2020). This section offers a comprehensive exploration of the centralization trend in Latvia, detailing its positive influences, potential drawbacks, and some noteworthy incidents that underline the complexity of this domain.

Centralization: An Economical Measure and a Quality Enhancer

The centralization process appears to be a preferred direction for several organizations and governmental establishments in Latvia. Notably, resource consolidation was outlined as a desired objective back in a 2008 report by the State Land Service, aiming to centralize all IT resources for more economical allocation and enhanced service development (Valsts zemes dienests, 2008). This consolidation process saw fruition in the field with increased server capacity and accelerated internet transmission speeds enabling the centralization of all IT systems into one location from the eight regional departments of the State Land Service.

Moreover, the Cabinet of Ministers in 2013 issued a concept for the organizational model of State ICT technology management (Ministru kabinets, 2013). Although the initial stages of this centralization did not yield the expected savings, over time, it provided a unified user support mechanism, standardized procedures within the institutions of one sector, and increased the capacity of ICT infrastructure maintainers and cybersecurity specialists.

In view of this, the Public Administration Modernization Plan for 2023–2027 takes it a step further, proposing the standardization and centralization of various support functions, such as personnel management, human resources management, financial accounting, ICT services, procurement, property management, and other areas of public administration (Ministru kabinets, 2022b). The goal is to improve service quality and efficiency and offer economic gains. Yet, given the sensitive data these systems handle, a high standard of cybersecurity is very important, and the influence of cybersecurity risks could grow furnished with a more extensive user base.

Risks Associated with Centralization

While the benefits of centralization are apparent, it does introduce new sets of challenges and risks (Chen, 2022):

- 1 **Single Point of Failure:** Effectively, centralization can result in the entire operations relying heavily on one central point. Any disruption in this central point could cause widespread difficulties in service provision.
- 2 **Monopolization:** A centralized model could lead to monopolization by manufacturers or suppliers, resulting in restricted choice and potential exploitation.
- 3 **Loss of Control:** The owner might lose control over all stages of the information as the control gets concentrated in the central mechanism.

Real-world examples of these risks materializing are seen in different sectors and scenarios:

- **The CrowdStrike Case**

The CrowdStrike case illustrates the risks of a “single point of failure” strategy. An error in a software update resulted in a kernel-level issue that halted system operation. The nation-wide centralization model compounded the problem as IT

personnel were located far from the computer systems, making resolution challenging (Weston, 2024).

- **The Latvian National Library (LNB) Data Center Incident**

The LNB incident serves as another example wherein a system malfunction resulted from an IT failure. The issue affected several systems, causing extensive disruption and forcing manual operation for certain processes (Kultūras informācijas sistēmu centrs, 2024). This reflects the risks inherent in centralizing the IT operations in one body that may lack prioritization for cybersecurity undertakings.

- **The LVRTC Data Center Incident**

A human-induced error at LVRTC led to an outage of data center services, affecting mobile operators' services. This case underscores that human error is still a significant risk, further accentuating the need for robust cybersecurity practices (LVRTC, 2023).

Centralization Organizations in Latvia

Latvia has increasingly embraced centralization in the realm of information technology as a key strategy to enhance efficiency, drive innovation, and foster collaboration across its academic and scientific sectors. In an era where digital transformation is critical to maintaining global competitiveness, the consolidation of IT resources not only streamlines service delivery but also ensures that institutions can more effectively manage costs, optimize performance, and respond to emerging technological challenges. By centralizing IT services, Latvia is able to offer uniform, high-quality support to a wide array of stakeholders—from universities and research centers to cultural institutions—thus creating a robust digital backbone that supports both educational excellence and scientific inquiry.

In line with this national strategy, targeted initiatives have been launched to address the specific needs of Latvia's higher education and research communities. These efforts demonstrate how centralization can drive not only operational efficiency but also innovation and collaboration in the academic realm. Two prominent examples illustrate this approach: the Association of Higher Education and Science Information Technology Shared Services Center (VPC) and the Latvian Academic Data Transmission Network. While each initiative has its unique focus, together they form a comprehensive framework that enhances IT service delivery, promotes resource optimization, and ultimately supports the country's academic and research objectives.

Association of Higher Education and Science Information Technology Shared Services Center (VPC)

The VPC was established in early 2022 by a consortium of Latvian universities and represents a significant percentage of researchers and students in Latvian

educational institutions. VPC aims to empower the development and international competitiveness of higher education and scientific institutions via high-quality shared IT services. Their current service offerings include high-performance computing infrastructure, unified network member identification, and access to the National Scientific Activity Information System (VPC, 2024).

Latvian Academic Data Transmission Network

The Latvian Academic Data Transmission Network is another example of IT centralization benefiting from a unified system procurement and centralized payment system managed by the Ministry of Education and Science (Izglītības un zinātnes ministrija, 2023). This network includes universities, research centers, and the National Library of Latvia, providing a consolidated landscape for enhanced academic and research collaborations. However, these centralizations' ultimate impact on cybersecurity deserves ongoing monitoring, considering the associated risks and the increasing network of stakeholders involved.

Balancing Centralization in Latvia's Cybersecurity Landscape

The centralization of cybersecurity services in Latvia presents both significant opportunities and notable challenges. While organizations like VPC and the Latvian Academic Data Transmission Network demonstrate the potential benefits of consolidated IT services—including enhanced efficiency, standardized security protocols, and cost optimization—the documented incidents at LVRTC, LNB, and other facilities underscore the inherent risks of centralized approaches.

The evolution of Latvia's centralized IT infrastructure reflects a careful balance between resource optimization and risk management. Organizations must weigh the economic advantages of consolidated services against the potential vulnerabilities of single-point failures. The experiences of various institutions suggest that successful centralization requires robust backup systems, comprehensive contingency planning, and regular security audits to mitigate risks effectively.

As Latvia continues to develop its cybersecurity infrastructure, the lessons learned from both successful implementations and encountered challenges provide valuable insights for future initiatives. The establishment of organizations like VPC and the implementation of unified networks demonstrate the government's commitment to enhancing digital security while pursuing operational efficiency.

These observations set the stage for a deeper examination of how individual organizations navigate the complexities of cybersecurity transformation. The following case studies of five major Latvian organizations will provide concrete examples of how these institutions balance centralization with security requirements, implement various cybersecurity measures, and address the evolving challenges in their respective sectors.

Cybersecurity Transformation Case Studies

The manifestation of the digital paradigm shift and the exponential increase in cyber threats have prompted a surge in research and initiatives geared towards cybersecurity enhancement globally. This section elucidates the transformational cybersecurity journeys of five significant organizations in Latvia—SIA Tet, RTU, LBTU, LMT, and LVRTC. Each case study will explore the unique strategic shifts, developments, and challenges experienced by these entities from 2019 to 2024.

The narrative derived from data collection, interviews, and comprehensive analysis of their cybersecurity initiatives is designed to provide a nuanced understanding of their experiences. Moreover, it will present institutionalized evidence for the theoretical and practical enhancements in cybersecurity practices. This will significantly contribute to the understanding and growth of cybersecurity science and the development of safer global digital landscapes.

Case Study 1—Tet

The past five years have witnessed a significant transformation in the cybersecurity landscape of leading Latvian enterprises, exemplified by Tet, a major player in the nation's technological sphere. Formerly known as Lattelekom, Tet is now one of the largest Latvian internet service providers and a leading company in telecommunications, technology, and entertainment. Through extensive interviews and data collection, this chapter explores the key developments and strategic shifts in Tet's cybersecurity initiatives from 2019 to 2024, providing a nuanced understanding of their experience and journey toward a more secure digital environment.

Organizational Evolution of the Cybersecurity Team

One of Tet's most notable advancements has been the evolution of its cybersecurity team into a distinct structural unit. Initially a single-person operation in 2016, the team expanded to four members by 2018 and reached a robust team of ten cybersecurity professionals by 2024. This growth reflects Tet's increasing recognition of cybersecurity as a critical component of its operational framework, necessitated by the growing complexity and frequency of cyber threats.

Transition to a Zero Trust Architecture

Tet's security perimeter concept has undergone a paradigm shift, influenced by the proliferation of cloud services, remote work, and enhanced collaborations with external partners. The clear boundaries that once separated internal networks from the untrusted external internet have blurred, prompting Tet to implement a "zero trust" architecture. This model assumes that threats could exist both inside and outside the traditional perimeter, thus requiring stringent verification processes for every access request. This strategic shift has successfully redefined Tet's security posture in practice.

Enhanced Update Frequency

The cadence of cybersecurity updates at Tet has shifted dramatically—from annual updates to quarterly, then to monthly updates. The company is rapidly advancing towards continuous updates, where vulnerabilities are patched as soon as they are discovered. This agile approach ensures that Tet remains ahead of emerging threats and minimizes the window of exposure, enhancing the overall security posture of their digital assets.

Increasing Dependence on IT Continuity

The dependence on reliable IT resources has only grown, reinforcing the critical need for digital resilience. Tet recognizes that the availability of IT services directly correlates with operational capabilities. As a result, there is a concerted effort towards ensuring continuity and readiness, thereby positioning Tet to swiftly recover from disruptions and maintain service integrity.

Continuous Vulnerability Monitoring and Testing

Vulnerability monitoring and regular testing, which were once sporadic and limited to initial operational phases, have become continuous processes at Tet. The firm strictly adheres to ongoing assessments and real-time monitoring to identify and address security flaws proactively. This persistent vigilance is crucial for sustaining robust cybersecurity defense mechanisms.

Evolution in DDoS Attack Mitigation

The nature of DDoS attacks has evolved, with a pronounced shift towards application-level (Layer 7) attacks aimed at overwhelming web servers and load balancers. In the past, DDoS attacks targeted internet connections and firewalls. Recognizing the insufficiency of standard DDoS protection tools, Tet has implemented advanced Layer 7 DDoS protection solutions, ensuring comprehensive security against sophisticated attack vectors.

Regulatory Compliance and Audit Routines

In alignment with the National Cyber Security Act and the Digital Operational Resilience Act (DORA) regulations, Tet has intensified its focus on regulatory compliance. The firm now mandates adherence to stringent cybersecurity requirements not only for its employees but also for its service providers. Regular compliance checks and audits have become integral to Tet's daily operations, reinforcing a culture of security and accountability.

Implementation of Web Application Firewall (WAF)

To safeguard its online resources, Tet has deployed and maintained a robust WAF. This strategic implementation is pivotal in defending against application-layer attacks, thus securing the integrity and availability of critical web services.

Case Study 2—RTU

The period from 2019 to 2024 has marked a transformative phase in the cybersecurity posture of RTU, the oldest technical university in the Baltic countries. In response to evolving cyber threats and the increasing complexity of digital infrastructures, RTU has implemented a series of innovative strategies and technologies aimed at bolstering its cybersecurity defenses. This chapter delves into the critical developments and lessons learned through RTU's recent initiatives, providing valuable insights into the changing landscape of academic cybersecurity.

Automated Security Management Solutions

RTU has pioneered the development of automated security management solutions that actively involve end users. These solutions are designed to mitigate the consequences of identified security incidents promptly. By automating responses and involving the end user in the security process, RTU has reduced the impact of security breaches and bolstered its overall security resilience.

The Role of Automation and Big Data

Automation and big data processing have become cornerstones of effective security management at RTU. These technologies are mandatory for the implementation of responsive and adaptive security measures, allowing the institution to quickly analyze vast amounts of data and respond to security incidents in real time.

User Acceptance of Security Measures

Much like drivers who have adapted to wearing seat belts for safety, RTU users have accepted additional cybersecurity burdens. Notable among these measures is multi-factor authentication (MFA), which has become a standard practice to enhance account security. User buy-in is critical for the successful implementation of security protocols, and RTU has seen positive user engagement in adopting these necessary precautions.

Evolving Security Perimeters

The traditional notion of a security perimeter has become increasingly conditional. RTU recognizes that simply monitoring the firewall is no longer sufficient. Hence, the focus has shifted to ensuring that end-user devices are securely configured and regularly monitored. This new approach necessitates comprehensive audits to ensure that all devices connected to the university's network adhere to stringent security standards.

Advanced DDoS Mitigation

RTU has had to adapt to more sophisticated DDoS attacks, which no longer rely solely on standard GET or SYN packets. Modern attacks may include modified packets incorporating both SYN and GET data. By evolving their DDoS mitigation strategies, RTU has been able to better defend against these complex attack vectors.

Cloud Service Vulnerabilities

Cloud-based solutions have certainly offered cost savings and improved security by centralizing vulnerability patching duties with a single vendor. However, attackers have adapted, particularly targeting the widespread use of Microsoft 365 within the institution. RTU has encountered password-guessing bots that bypass traditional protection methods by trying the same password across multiple user accounts rather than targeting individual users. This method has notably targeted the @edu.rtu.lv domain, requiring enhanced defensive measures.

Limitations of Multi-Factor Authentication

While multi-factor authentication (MFA) adds a significant layer of security, it is not a foolproof solution. RTU has experienced instances where users were tricked into providing all necessary information, thus allowing attackers to steal authentication tokens. These incidents underscore the need for continuous user education and advanced authentication methods.

Email Security Challenges

Email continues to be an insecure communication channel, often exploited for fraudulent activities such as altering invoice information to divert funds. Despite the availability of solutions such as e-signatures to ensure email authenticity and confidentiality, user adoption has been slow, highlighting the ongoing challenge of integrating secure communication practices.

Cryptovirus Evolution

Cryptoviruses have become increasingly sophisticated, initially targeting online backups before encrypting primary data. Additionally, these viruses often exfiltrate sensitive data before encryption to facilitate future blackmail attempts. RTU's cybersecurity strategies now include measures to detect and counter such threats proactively.

System Aging and Vulnerability Management

The aging of systems and the necessity for timely updates are persistent challenges. Even widely used open source programs such as SSH are continuously identified with new vulnerabilities. RTU's approach includes a rigorous schedule for system upgrades and vulnerability patching to mitigate this ever-present risk.

Case Study 3—LBTU

The LBTU, a key regional university, has been experiencing a steady state of cybersecurity conditions from 2018 to 2023. Despite having a wide-reaching IT infrastructure with several properties, LBTU faced an average of 29 cybersecurity incidents each year with no drastic fluctuations or pandemic-induced changes.

Through an in-depth analysis of LBTU's cybersecurity framework and an interview with the institution's IT director, this chapter outlines key strategies, challenges, and the impact of their initiatives on bolstering the cybersecurity environment.

Integration of Cybersecurity in All Projects

Cybersecurity at LBTU is not viewed as a separate entity with an independent budget but is considered crucial for every change or investment project. This approach ensures that every initiative, from installing solar panels to infrastructure upgrades, adheres to robust security protocols, integrating cybersecurity into the core operational strategy of the university.

Implementation of Diverse Cybersecurity Measures

LBTU's cybersecurity framework comprises a variety of measures, from blocking suspicious URLs with a DNS firewall to regularly monitoring device performance parameters and audit logs. They have implemented a Single Sign-On mechanism for simpler user authentication across multiple systems. Additionally, LBTU's unique tactic of maintaining its private email server sets it apart from other universities, providing enhanced spam filtration.

Utilization of the Early Warning System (EWS)

To enhance predictive abilities and proactive defense, LBTU utilizes the EWS, scanning the entire network traffic for anomalies and providing an additional layer of security that promotes faster detection of potential threats.

Establishing a Private Optical Network

In Jelgava, LBTU has set up a private optical network, linking the central building with various faculties and dormitories, significantly reducing network latency for accessing roughly 60 systems. This high-speed private network enhances the swift sharing and access of data while also ensuring a secure network environment.

Cybersecurity Challenges

Like all institutions, LBTU faces several cybersecurity challenges. The scientific collaborations of the university, which see frequent access attempts by individuals unfamiliar with or indifferent to usage policies, present risks. There are also vulnerabilities related to a large number of laptops used by the academic staff that often connect to networks beyond LBTU's control, possibly resulting in outdated software and altered device configurations. Issues with regular updates for all devices, servers, and infrastructure elements also highlight resource-intensive processes that must be tackled strategically.

Extensive VPN and Remote Access

In 2023, as many as 232 users utilized VPN connections, and nine accessed their computers remotely. With VPN connections and remote access becoming integral to work processes, LBTU faces the challenge of managing such access points securely, ensuring their digital operations are protected from potential exposure to cyber threats.

Case Study 4—LMT

LMT is a state-controlled telecommunications company with a multi-faceted approach to cybersecurity, incorporating defense mechanisms within its infrastructure while simultaneously offering security solutions to its clients. This chapter explores LMT's unique strategies, policies, challenges, and the impact of its cybersecurity initiatives, providing insights into how telecommunications companies can bolster their cybersecurity defenses.

Integrated Cybersecurity Solutions

LMT has integrated cybersecurity solutions into several of its services, including Mobile Internet, Internet for Home, Unlimited Internet+, and Professional Internet, in collaboration with Whalebone, a DNS filtration service provider. This blending of telecommunications and cybersecurity services marks a strategic shift in enhancing digital protection for its clients.

Introduction of the Internet Guard Service

LMT launched the “Internet Guard” service for its customers, designed to protect users from cyber threats without the need for additional software installation. In October 2023 alone, this service successfully prevented 6.9 million cyber threats, including blocking visits to fake online stores and thwarting Command-and-Control attack attempts. This indicates the effectiveness and scale of LMT's cybersecurity measures.

Convergence of Physical Security and IT

LMT's Security Service Director acknowledged the intersection of physical security and IT during the Baltic Security Conference. Despite this convergence, LMT maintains separate specialists in each area, recognizing the distinctive knowledge and skills required for each security facet.

Proactive Strategy Regarding Sanctions

LMT's foresight in not purchasing from politically “unfriendly” countries, despite potential cost advantages, has been beneficial. This proactive approach enables LMT to adapt to new requirements and continue offering services to clients in

critical infrastructure and military sectors, despite the higher demands imposed by sanctions and the NIS2 directive.

Ultimate Impact of Technological Advancements

While emerging technologies offer new possibilities for innovative products such as 5G, IoT, and drone technologies, they also intensify the complexity of cybersecurity. Regulatory constraints and the requirement for regular updates to devices highlight the intricate challenges in sustaining a secure digital environment amid rapid technological advancement.

Collaborative Efforts with Latvian Military

LMT recognizes the potential in securing commercial and military 5G networks through collaboration with the Latvian military. Although current efforts are exploratory and experimental at this stage, this collaboration sets the stage for emerging cybersecurity products and services geared towards military use.

Case Study 5—LVRTC

The LVRTC, a wholly state-controlled enterprise, offers a myriad of services that encompass radio, data transmission, and data centers. With its recent designation as the State Electronic Communications Service Centre (VESPC), LVRTC's role in cybersecurity has significantly expanded. This chapter explores the institution's key policies, strategies, challenges, and the role it plays in fortifying Latvia's digital infrastructure against cybersecurity threats.

Designation as the State Electronic Communications Service Centre

With the Cabinet of Ministers Instruction in November 2022, LVRTC was designated as the VESPC, enabling it to provide a myriad of services to public entities, public corporations, or public-controlled corporations. This directive allows these bodies to access resources and services like cybersecurity, cloud computing, and data centers without going through the procedures dictated by the Public Procurement Law.

Implementation of Stringent Service Level Agreements

The directive also mandates LVRTC to ensure several service level agreements (SLAs) and protection mechanisms, focusing on safeguarding against DoS attacks and aspects like SQL injection attacks. These SLAs ensure the provision of high-security and high-availability services to all public administration institutions.

Ensuring Data Centre Standards

The data center provided by LVRTC must meet the specifications of certain international standards. These include Level 2 of the TIA-942 standard and Level 2 of

the EN50600 standard, ensuring a high-security, reliable data center that conforms to global norms.

Key Role in Providing High-Security Services

The government's decision to designate LVRTC as the VESPC emphasizes the institution's capability and potential to contribute towards enhancing the country's cybersecurity landscape. By providing high-security and high-availability data centers, LVRTC plays a crucial role in ensuring that all public administration institutions can access robust cybersecurity resources and services.

Through its recent transition to the VESPC, LVRTC's role in strengthening Latvia's cybersecurity framework has become more pronounced, offering critical services in data transmission, data centers, and cybersecurity to other public entities.

An Analysis Across Five Latvian Organizations

Analysis of the presented case studies reveals several common trends that are consistently observed across all the organizations, ranging from telecommunications companies to academic institutions. These trends reflect both the universal challenges posed by the evolving cyber threat landscape and the strategies being adopted to mitigate them.

A prevalent trend found across the five organizations is the shift from a perimeter-based security model to a "zero trust" architecture. This trend is most apparent in LMT and Tet but is also evident to a certain degree in RTU, LBTU, and LVRTC. The increasing complexity of digital networks and the proliferation of remote work environments have blurred the boundaries between internal and external networks. Hence, the adoption of a zero trust model, where every access request is stringently verified regardless of its origin, is becoming a common cybersecurity strategy.

The evolution of DDoS mitigation strategies is another trend noticeable across organizations. Entities like Tet, RTU, and LMT have all noted a shift in the nature of DDoS attacks, with a significant increase in application-level (Layer 7) attacks. Consequently, these organizations have implemented advanced Layer 7 DDoS protection measures to defend against these sophisticated attack vectors.

Continuous vulnerability monitoring and regular system updates are becoming integral parts of cybersecurity practices. LMT, Tet, and RTU, for instance, have shifted from sporadic assessments and updates to real-time monitoring and more frequent updates. This new approach aids in proactive threat detection and ensures timely mitigation of vulnerabilities, enhancing the overall cybersecurity posture.

Another key trend is the increased focus on regulatory compliance. Tet and LMT, for instance, have intensified their adherence to national and international cybersecurity regulations. This not only reinforces a culture of security and accountability but also helps these organizations align their cybersecurity practices with global standards, thereby enhancing their resilience against cyber threats.

A final trend is the integration of cybersecurity in all aspects of operations. LBTU and LMT, in particular, demonstrate this by incorporating cybersecurity considerations into every change or investment project and integrating cybersecurity

solutions into their services. This trend underscores the recognition of cybersecurity as a critical operational component rather than a separate entity.

In summary, the top trends across these organizations highlight the shift towards advanced cybersecurity strategies to combat the evolving threat landscape. The universal adoption of these trends points towards a more security-conscious culture within organizations, marking significant progress in the field of cybersecurity.

Discussion

The findings from this study provide a panoramic view of Latvia's cybersecurity landscape in the context of global shifts and rising threat vectors. By comparing the experiences of five major Latvian organizations—LMT, Tet, RTU, LVRTC, and LBTU—the discussion reveals how local strategies mirror international practices. These strategies underscore a concerted emphasis on proactive defense mechanisms, regulatory compliance, and the balanced pursuit of centralization and decentralization for robust cyber resilience.

A central takeaway is the critical role that legislative and institutional frameworks play in shaping organizational behavior. For instance, the National Cybersecurity Law and the EU Cybersecurity Act have driven Latvian institutions to bolster threat intelligence, align with strict security standards, and formalize incident response measures. This legal context sets the groundwork for consistent risk management while also fostering an environment where advanced technologies, such as AI and ML, can thrive.

Alignment with Global Trends

Globally, cybersecurity incidents—particularly large-scale DDoS attacks—have grown in sophistication, reflecting an alarming ability to target application layers (Layer 7). Latvia has not been immune to this trend, as evidenced by Tet's and LMT's swift pivot to enhanced DDoS mitigation strategies designed to safeguard critical infrastructure. This alignment with global best practices highlights how local organizations are positioning themselves against internationally evolving threats.

Regulatory compliance and strict adherence to established standards, such as those outlined in the Global Cybersecurity Index, further illustrate the synergy between local efforts and global priorities. These measures extend beyond mere box-ticking, compelling entities like Tet and LMT to integrate compliance checks into their daily routines. As a result, organizations develop a culture of accountability, ensuring that preventive measures and continual audits remain core components of their cybersecurity posture.

Moreover, the adoption of advanced AI and ML tools at RTU resonates with worldwide endorsements of automation as a gamechanger in threat detection. Real-time anomaly alerts, automated responses to potential breaches, and predictive analytics collectively demonstrate how Latvian institutions are embracing the same cutting-edge solutions recommended at international cybersecurity forums. In turn, this forward-thinking approach catalyzes more efficient resource allocation and fosters resilience.

Centralization vs. Decentralization in Cybersecurity

A salient theme emerging from the study is the trend toward centralizing IT resources and services. Centralization promises cost efficiency, uniform security standards, and streamlined responses to incidents, a point illustrated by large-scale data center initiatives at LVRTC and VPC. These setups allow for shared defenses and unified monitoring, thereby reducing fragmentation and improving overall situational awareness in the face of escalating threats.

Yet, the drawbacks of a single point of failure remain significant. As shown by incidents at the LNB data center and in CrowdStrike's case, a localized error or misconfiguration may ripple across an entire system, potentially causing widespread service outages. This underscores the importance of implementing robust backup sites, distributed architectures, and human-error minimization protocols as counterbalances to full-scale centralization.

The analysis reveals that some organizations pursue a hybrid model, centralizing certain critical functions while allowing decentralized elements for specialized tasks or local autonomy. This balanced approach aims to combine the best of both worlds: harnessing centralized efficiencies and advanced security measures while mitigating the risk of crippling single-point failures. In the Latvian context, this appears particularly apt given the variety of sector-specific needs—ranging from academic collaboration at RTU and LBTU to robust telecom operations at LMT.

Future Outlook and Continuing Challenges

Looking ahead, the drive to embed cybersecurity as an integral, organization-wide principle is poised to intensify. Greater adoption of the zero trust model suggests that trust boundaries will continue to shrink, with every system and user regarded as a potential threat entry point. Such a paradigm demands more granular access controls and enhanced user education—efforts that prove vital as attackers develop increasingly refined social engineering techniques.

Regulatory landscapes in the EU are also expected to evolve, further raising the bar for compliance. Future revisions to the NIS2 directive and related frameworks will likely set stricter requirements on risk assessments, incident reporting, and cross-border cooperation. These directives will stimulate additional cybersecurity spending, particularly around continuous monitoring and advanced AI-based threat detection solutions.

Finally, while centralization is on the rise, decentralization remains a potent strategy in mitigating systemic risks and fostering adaptability. Organizations may leverage decentralized data stores, microservices architectures, or localized incident response teams to avoid single points of failure. The long-term challenge involves striking the right balance: ensuring robust, centralized controls without stifling the flexibility and redundancy that decentralization can bring. By continually refining these approaches, Latvia's cybersecurity landscape will evolve in tandem with global best practices, fortifying the nation's digital future against an ever-shifting array of cyber threats.

Conclusion

The research findings underscore the urgent need for nations and organizations—including those in Latvia—to prioritize cybersecurity as a critical safeguard for digital assets and operations. While the financial repercussions of breaches can be substantial, the implications extend beyond economic losses, threatening both national security and public trust in digital services.

Within Latvia's landscape, several significant trends have emerged. Supply chain attacks persist as a notable threat, necessitating stringent vetting and monitoring of third-party partners. Politically motivated attacks underscore the geo-strategic dimensions of cybersecurity, while the expanding role of AI and ML reveals both promising opportunities for rapid threat detection and heightened risks if misused by attackers. New and emerging digital technologies—such as 5G and cloud computing—magnify the complexity of security demands, making compliance with evolving regulations and directives, including NIS2, an essential pillar of national defense.

The case studies of five major Latvian organizations highlight both the strides made and the challenges encountered in implementing and maintaining robust cybersecurity practices. These organizations illustrate the value of continuous vulnerability testing, proactive security strategies, and the embedding of cybersecurity in every facet of operations. Concurrently, they face ongoing obstacles related to converging physical and digital security, the complexities of centralizing IT resources without creating single points of failure, and ensuring sufficient budgetary allocations specifically dedicated to cybersecurity.

Although Latvia demonstrates a strong overall cybersecurity posture, further development and sustained investment remain paramount. In particular, the NIS2-mandated thorough supply chain evaluations and the adoption of certification (e.g., EUCC) can reinforce cyber readiness and resilience. Equally vital is recognizing the risks and costs associated with centralizing cybersecurity functions, where resource efficiency must be balanced against potential vulnerability in single points of failure.

In essence, this research affirms that Latvia's robust efforts are well-aligned with global trends, but the rapidly evolving threat landscape demands that organizations continue to refine their strategies and allocate dedicated resources for security. By proactively confronting emerging challenges—be they technological, regulatory, or operational—Latvia can solidify its defense capabilities and contribute to a more secure, resilient, and innovative digital future.

References

- Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2023). Review of Strategic Alignment: Accounting and Cybersecurity for Data Confidentiality and Financial Security. *World Journal of Advanced Research and Reviews*, 20(3), 1743–1756. <https://doi.org/10.30574/wjarr.2023.20.3.2691>
- Aizsardzības ministrija. (2023). *Latvijas Kiberdrošības Stratēģija*. Ministry of Defence of the Republic of Latvia.

- Bērziņš, J. (2023). From Total Defense to Comprehensive Defense. *PRISM*, 10(2), 38–53. <https://www.jstor.org/stable/48718172>
- Braun, V., & Clarke, V. (2023). Thematic Analysis. In F. Maggino (Ed.), *Encyclopedia of Quality of Life and Well-Being Research* (pp. 7187–7193). Springer International Publishing. https://doi.org/10.1007/978-3-031-17299-1_3470
- CERT.lv. (2023). Latvijas kiberdrošības 2023. gada pārskats. <https://www.cert.lv/pakalpojumi>.
- Chen, R. (2022). Design and Protection Strategy of Distributed Intrusion Detection System in Big Data Environment. *Computational Intelligence and Neuroscience*, 2022(1), 4720169. <https://doi.org/https://doi.org/10.1155/2022/4720169>
- Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions. *Personal and Ubiquitous Computing*. <https://doi.org/10.1007/s00779-021-01569-6>
- Creswell, J. (2013). *Qualitative Inquiry & Research Design: Choosing Among Five Approaches*. SAGE Publications, 11.
- Doğrul, M., Yalçın, H., & Daim, T. U. (2023). *Cybersecurity Technology: A Landscape Analysis* (pp. 3–21). Springer. https://doi.org/10.1007/978-3-031-34843-3_1
- Done, L. (2022). Applicability of International Law in Cyberspace: Positions by Estonia and Latvia. *Socrates Rīgas Stradiņa Universitātes Juridiskās Fakultātes Elektroniskais Juridisko Zinātnisko Rakstu Žurnāls / Socrates Rīga Stradiņš. University Faculty of Law Electronic Scientific Journal of Law*. <https://www.researchgate.net/publication/366639417>
- ENISA. (2023). ENISA Threat Landscape. <https://doi.org/10.2824/782573>
- Górka, M. (2023). Baltic States Cyber Security Policy: Development of Digital Capabilities in 2017–2022. *Stosunki Międzynarodowe – International Relations*. <https://doi.org/10.12688/stomiedintrelat.17684.1>
- Grima, S., Thalassinou, E., Cristea, M., Kadłubek, M., Maditinos, D., & Peiseniece, L. (Eds.), (2023). Digital Transformation, Strategic Resilience, Cyber Security and Risk Management. In *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management*. Emerald Publishing Limited. <https://doi.org/10.1108/S1569-37592023000111A018>
- Gundu, T. (2024). Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model. *International Conference on Cyber Warfare and Security*, 19(1), 95–102. <https://doi.org/10.34190/iccws.19.1.2177>
- Haryanto, T., & Ramli, K. (2023). Secure Cybersecurity Information Sharing for Sectoral Organizations Using Ethereum Blockchain and IPFS. *Jurnal Resti (Rekayasa Sistem Dan Teknologi Informasi)*. <https://doi.org/10.29207/resti.v7i3.4956>
- Iaiani, M., Tugnoli, A., Bonvicini, S., & Cozzani, V. (2021). Analysis of Cybersecurity-Related Incidents in the Process Industry. *Reliability Engineering & System Safety*, 209, 107485. <https://doi.org/10.1016/J.RESS.2021.107485>
- Izglītības un zinātnes ministrija. (2023). Latvija turpinās dalību Eiropas akadēmiskā tīkla GEANT projektā. <https://www.izm.gov.lv/lv/jaunums/latvija-turpinas-dalibu-eiropas-akademiska-tikla-geant-projekta>
- Kultūras informācijas sistēmu centrs. (2024). Atjaunota integrētās sistēmas ALEPH darbība, turpinās darbs pie pārējo kultūras resora IT sistēmu atjaunošanas. <https://www.kis.gov.lv/lv/jaunums/atjaunota-integretas-sistemas-aleph-darbiba-turpinas-darbs-pie-parejo-kulturas-resora-it-sistemu-atjaunosanas>
- Liu, C.-W., Huang, P., & Lucas Jr., H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*, 37(3), 758–787. <https://doi.org/10.1080/07421222.2020.1790190>

- LVRTC. (2023). Tehnoloģiskā avārija novērsta, pakalpojumi secīgi tiek atjaunoti. <https://www.lvrtc.lv/jaunumi/jaunumi/tehnologiska-avarija-noversta-pakalpojumi-secigi-tiek-atjaunoti/>
- Mallik, A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. www.worldscientificnews.com
- Ministru kabinets. (2022a). Nacionālās kiberdrošības likums. <https://tapportals.mk.gov.lv/annotation/d7803af8-e515-43c6-b0db-61c39a0da17e>
- Ministru kabinets. (2022b). Valsts pārvaldes vienoto pakalpojumu centra attīstība Latvijā. <https://www.mk.gov.lv/lv/projekts/valsts-parvaldes-vienoto-pakalpojumu-centra-attistiba-latvija#3-uz-kuram-valsts-parvaldes-funkcijam-ta-attieksies>
- Ministru kabinets. (2023). Par Latvijas kiberdrošības stratēģiju 2023.-2026. gadam. https://tapportals.mk.gov.lv/legal_acts/dcaf6fc4-4dbe-491d-bcc6-1579837cd1ff#
- Möller, D. P. F. (2023). *Guide to Cybersecurity in Digital Transformation* (Vol. 103). Springer Nature Switzerland. <https://doi.org/10.1007/978-3-031-26845-8>
- Nacionālās kiberdrošības likums. (2024). <https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums>
- NCSI. (2023). National Cyber Security Index. <https://ncsi.ega.ee/country/lv/>
- Ogugua Chimezie Obi, Onyinyechi Vivian Akagha, Samuel Onimisi Dawodu, ` A. C. A., Shedrack Onwusinkwue, & ` I. A. I. A. (2024). Comprehensive Review On Cybersecurity: Modern Threats And Advanced Defense Strategies. *Computer Science & IT Research Journal*, 5(2), 293–310. <https://doi.org/10.51594/csitrj.v5i2.758>
- Ministru kabinets. (2013). Par koncepciju ‘Valsts informācijas un komunikācijas tehnoloģiju pārvaldības organizatoriskais modelis’. <https://likumi.lv/ta/id/254909-par-koncepciju-valsts-informacijas-un-komunikacijas-tehnologiju-parvaldibas-organizatoriskais-modelis>
- Pissanidis, D. L. (2024). Integrating AI/ML in Cybersecurity: An Analysis of Open XDR Technology and Its Application in Intrusion Detection and System Log Management. <https://doi.org/10.20944/preprints202312.0205.v2>
- Rattanapong, P., & Ayuthaya, S. D. N. (2025). Influential Factors of Cybersecurity Investment: A Quantitative SEM Analysis. *Management Science Letters*, 15(1), 31–44. <https://doi.org/10.5267/j.msl.2024.3.005>
- Salvaggio, S. A., & González, N. (2023). The European Framework for Cybersecurity: Strong Assets, Intricate History. *International Cybersecurity Law Review*, 4(1), 137–146. <https://doi.org/10.1365/s43439-022-00072-9>
- Sarker, I. H. (2023). Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*, 10(6), 1473–1498. Springer Science and Business Media Deutschland GmbH. <https://doi.org/10.1007/s40745-022-00444-2>
- Sendjaja, T., Irwandi, Prastiawan, E., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity In The Digital Age: Developing Robust Strategies to Protect Against Evolving Global Digital Threats and Cyber Attacks. *International Journal of Science and Society*, 6(1), 1008–1019. <https://doi.org/10.54783/ijssoc.v6i1.1098>
- Siemers, B., Attarha, S., Kamsamrong, J., Brand, M., Valliou, M., Pirta-Dreimane, R., Grabis, J., Kunicina, N., Mekkanen, M., Vartiainen, T., & Lehnhoff, S. (2021). Modern Trends and Skill Gaps of Cyber Security in Smart Grid : Invited Paper. *IEEE EUROCON 2021-19th International Conference on Smart Technologies*, 565–570. <https://doi.org/10.1109/EUROCON52738.2021.9535632>
- Skrodelis, H. K., Strebko, J., & Romanovs, A. (2020, October 15). The Information System Security Governance Tasks in Small and Medium Enterprises. *2020 61st International Scientific Conference on Information Technology and Management Science of Riga*

- Technical University, ITMS 2020- Proceedings*. Riga, Latvia <https://doi.org/10.1109/ITMS51158.2020.9259305>
- Skrodelis, H., Kelle, R., & Romanovs, A. (2024). Cybersecurity in SCADA Systems with Advanced AI and ML Techniques. *2024 IEEE 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, 1–5. Riga, Latvia <https://doi.org/10.1109/ITMS64072.2024.10741936>
- Stake, R. E. (1995). *The Art of Case Study Research*. Sage Publications, Inc.
- Swain, A., Swain, K. P., Pattnaik, S. K., Samal, S. R., & Das, J. K. (2022). Cybersecurity in Digital Transformations, 247–252. https://doi.org/10.1007/978-981-19-0825-5_26
- The EU Cybersecurity Act. (2019). <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
- Treacy, S., Sabu, A., Bond, T., O’Sullivan, J., Sullivan, J., & Sylvester, P. E. (2023). Organizational Cybersecurity Post the Pandemic: An Exploration of Remote Working Risks and Mitigation Strategies. *International Conference on Cyber Warfare and Security*, 18(1), 394–401. <https://doi.org/10.34190/iccws.18.1.973>
- Valsts zemes dienests. (2008). *2008.Gada Publiskais Pārskats*. The State Land Service of the Republic of Latvia.
- Volkova, T., JEKABSONE, L., LAVRINOVICA, Z., Saba, E., & Saba, M. (2021). The Challenges of Cybersecurity Insurance Development: The Case of Latvia. *Journal of Business Management*. <https://www.researchgate.net/publication/357920230>
- VPC. (2024). Par VPC. <https://vpc.lv/lv/pakalpojumi/>
- Weston, D. (2024). Helping our customers through the CrowdStrike outage - The Official Microsoft Blog. <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>
- World Economic Forum, & Accenture. (2024). *Global Cybersecurity Outlook*. World Economic Forum.
- Yanakiev, Y. (2020). A Governance Model of a Collaborative Networked Organization for Cybersecurity Research. *Information & Security an International Journal*. <https://doi.org/10.11610/isij.4606>
- Yin, R. K. (2018). *Case Study Research: Design and Methods* (Sixth Edition). SAGE Publications, Inc.

10 Shaping the Latvian Cyber Workforce of Tomorrow

Rūta Pirta and Matīss Veigurs

Introduction

Cybersecurity (CS) is a critical business capability to ensure the continuous operation of organizations. Over the past decade, Europe has encountered pandemics, warfare, natural disasters and various other disruptive events, including large-scale CS incidents. For the fourth consecutive year, cyber risks have retained their position as the foremost global risk, as indicated by the global enterprise survey (Allianz Commercial, 2025). The European Commission estimates that the annual cost of cybercrime to the global economy has reached 5.5 trillion euros in 2020. European Union Agency for Cybersecurity (ENISA) emphasizes the importance of proper cyber crisis management and highlights that European member states must increase their capacities to prevent and respond to large-scale cyberattacks (ENISA, 2025). Having the appropriate CS competences is essential for effectively managing today's CS threats and being prepared for those of tomorrow.

Studies and market analyses reveal a growing shortage of qualified CS professionals worldwide, posing challenges for both public and private sectors (ISACA, 2021, ISC2, 2023). The shortage of skilled CS specialists has been widely acknowledged across the industry and academia (Jelo & Helebrandt, 2022). ISC2 Cyber Workforce Study 2024 estimates lack of more than 4.8 million CS specialists worldwide and this number is continuing to rise (ISC2, 2024). The growing gap is related to several factors, including inadequate interest in the subject, lack of diversity and significant challenges within CS education (Blažič, 2022). To close the skill gap, it's essential to build workforce and student-oriented CS education offering, considering not only current abilities but also those needed for the future.

This chapter aims to investigate CS education needs to face future challenges, considering existing and target workforce requirements, technology development trends, effective collaboration and secure behaviour aspects. The study presents the CS education ecosystem in Latvia, identifies gaps, investigates required future competences and provides recommendations to stakeholders regarding target education offering to advance human performance in the CS. The key contributions of this chapter are multi-fold. Firstly, the existing CS education ecosystem of Latvia is investigated, along with the planned initiatives to define the existing CS education offering. Secondly, the structure of the Latvian CS workforce is analysed to

explore the required CS roles and competences of Latvian organizations. Thirdly, competences gaps and future needs are specified as requirements towards future educational programmes. Finally, this chapter provides recommendations for stakeholders to enhance CS education offering.

The research questions (RQ) of this study are defined as follows:

- RQ1. What are current CS education provisions in Latvia in different education levels?
- RQ2. What is the structure of Latvian CS workforce?
- RQ3. What are the competences gaps and future needs of Latvian organizations towards CS education?

This study delivers two primary contributions. Firstly, this chapter fills the knowledge gap about CS education ecosystem of Latvia, along with Latvian CS roles and competences gaps. Secondly, this chapter proposes recommendations to improve CS education offering and provision, considering the needs of different stakeholder groups (such as industry, academia, and students).

The rest of this chapter is structured as follows. Literature Review introduces the main findings from related studies, after which the research methodology is presented in the next section. Section of CS Education Ecosystem of Latvia describes the CS education offering considering different study levels and forms. The structure of the Latvian CS personnel is demonstrated in section on Insights of the Latvian CS Workforce, followed by section of Competences Gaps and Future Needs. Another section is dedicated to recommended Future CS Education Provision and CS. Finally, the last section concludes findings and provides an overview of future research directions.

Literature Review

Research suggests that CS awareness and knowledge are associated with a decrease in the number of cyber incidents in organizations (Alshaikh & Adamson, 2021; Hore et al., 2024; Kweon et al., 2021). In developing a national CS education strategy, there is a tendency to align desirable skills with the security situation, technological requirements and defence needs in the geographic area; less common is the approach for a universal “education for all” model (AlDaajeh et al., 2022). In academic literature, there are several proposals for universal higher education curricula in CS (Cutas et al., 2023; Dragoni et al., 2020; Payne et al., 2021; Ramezani & Niemi, 2024). This section provides a deeper overview of the European education ecosystem and current advancements in CS education design, including CS competence models and required future skills.

European CS Educational System

Academic research suggests that CS topics in primary- and secondary-level education are important for organizations providing education and their technology suppliers. Considering the shift to EduTech solutions, educational institutions are

also becoming targets of cybercrime, thus the introduction of cyber hygiene and awareness training for both employees and students is becoming necessary (Torres & Thompson, 2020). However, an even bigger problem is addressing (future) industry needs. In 2023, the CS workforce in Europe is estimated at 1.3 million people with a gap of approximately 300,000 positions to be filled (ENISA, 2023; ISC2, 2023; OECD, 2024). Both problems highlight the need for a more uniform inclusion of CS topics within all levels of education.

There is no single European-wide approach for the incorporation of CS topics into school curricula in primary and secondary education in the EU. As education policies are largely controlled by national governments, each has a different vision, level of incorporation and learning methods regarding CS topics, and it can vary even within one state. A study conducted in the United States also pointed out that there are differences in secondary-level Computer Science education across the country, making it difficult to integrate a universal CS programme/module into education standards (Yang & Wen, 2017). Globally, the United Kingdom and Australia are good examples as both have made considerable efforts to incorporate CS for schoolchildren through interactive learning platforms and updates of general school curricula (Australian Government, 2023; Cabinet Office, 2023).

One of the main hubs of CS education mapping initiatives is ENISA as it has specifically been delegated to it in the European Cybersecurity Act. ENISA emphasizes facilitating CS skills development for professionals and attracting young talent to the CS domain, namely by organizing the annual European Cybersecurity Challenge. The institution has also published a study on Cybersecurity Education Initiatives in the EU member states which concluded that there are various national CS initiatives for primary and secondary education levels but insufficient cooperation between EU member states to share these best practices. EU member states face several challenges such as measuring the impact of CS education, decentralized approach, lack of physical and human resources and lack of recognition from stakeholders. According to ENISA, the development of successful CS education initiatives is usually driven by collaboration with stakeholders, including teachers and parents, who also need to be educated, as well as long-term planning efforts with set KPIs and planned improvements (ENISA, 2022a).

ENISA maintains The Cybersecurity Higher Education Database (CyberHEAD) which provides updated information on bachelor's and master's programmes in Cybersecurity in EU and EFTA countries, the majority of which focus on technical and management competences. As of 2024, CyberHEAD holds records of 151 programmes out of which 80% are master's level or postgraduate training (ENISA, 2024). Several European-level CS ecosystem research projects funded by "Horizon 2020" and "Horizon Europe" programmes examine the university level. *Concordia* project has identified that there is still a lack of interdisciplinarity in CS education, and it also impacts the offer of short-term training which fails to provide a bigger picture of the field (Cutas et al., 2023). *CyberSec4Europe* project organized a survey of 104 CS university-level programmes in EU member states. By looking at coverage of various knowledge areas the survey

concluded that all of them are covered in all programmes, however, the most neglected are organizational security, system retirement, societal security – CS customer service and technical support, component security, physical interface and connectors. Overall, data security and connection security have the largest coverage. Overall, programmes from larger countries tend to have broader coverage (Dragoni et al., 2020). *CyberSecPro* project, based on their desk research on CS practical skills gaps, suggests that education should focus on the utilization of awareness programmes for various industries and inclusion of gamification, simulation, situated learning and demonstration of theory application in practice. Also, inclusion and diversity within education and training are highlighted as drivers for the future innovation (Rathod et al., 2023).

CS Competence Frameworks

CS roles, tasks and competences are proposed in several competence models (ENISA, 2022b, Petersen et al., 2020). These models provide a basis for developing realistic assessments that reflect the industry needs. The models are mainly role-based, defining the CS roles, competences, skills and abilities.

ENISA has developed the European Cybersecurity Skills Framework (ECSF) (ENISA, 2022b). ECSF proposes 12 different CS roles, defining their tasks and required competences: Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy and Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, Cybersecurity Risk Manager, Digital Forensics Investigator and Penetration Tester. ECSF highlights the interdisciplinarity of the CS competences, combining management, law and computer science. The framework mainly focuses on the technical competences of particular roles, meanwhile also some soft skills are identified, such as communication, coordination and cooperation with internal and external stakeholders.

The National Institute of Standards and Technology (NIST) proposed a different set of roles and competences in the Cybersecurity Workforce Framework (CWF) (Petersen et al., 2020). Differing from the ECSF, the framework identifies 52 CS workforce roles, showing the bigger nations' perspective. Certain roles are similar in both frameworks, such as the Cybersecurity Risk Manager and Cyber Incident Responder. However, the roles within the CWF are more specialized. Similar as ECSF, the CWF mainly defines the technical competences along with a few soft skills, such as skill in talking to others to convey information effectively and skill to use critical thinking to analyse organizational patterns and relationships.

Although the competences models differentiate several roles, in smaller countries these roles are usually combined due to the lack of resources and competences (Bukauskas et al., 2023). Therefore, it is suggested that formal CS education covers several roles, providing the core competences. Meanwhile, non-formal education could consider role-specific education paths.

CS Future skills

CS historically has been positioned as a discipline of computer science, nowadays it is considered multi-disciplinary domain, joining a wide set of areas, such as computer science, mathematics, economics, law, psychology and engineering. Therefore, the future CS workforce is conceptualized to consist of individuals demonstrating exceptional performance and possessing a diverse array of competences (Dawson & Thomson, 2018). It is strongly emphasized that (Furnell, 2021): “cybersecurity is a spectrum and not a silo”. At the same time, it is acknowledged that no single educational programme can encompass all that is desired by each employer (Blažič, 2022). Thus, the main challenge lies in finding the right balance of competences and integrating a diverse range of skills.

The current understanding of the skills required for the future cyber workforce remains fragmented, and further investigation is required (Dawson & Thomson, 2018). Meanwhile, related studies highlight several trends (Blažič, 2022, de Casanove & Sèdes, 2021, ISC2, 2023), such as soft-skill-related competences integration in the technical subjects, emphasizing on human aspects in CS and need of emerging technologies related competences, including cloud computing, artificial intelligence and machine learning. Future CS education must also incorporate technical fundamentals like understanding basic computer architectures, data, cryptography, networking, secure coding principles and operating systems (Blažič, 2022).

CS competence models traditionally focus on the technical proficiency, while related research more and more emphasizes a solid mix of technical skills, soft skills and social intelligence (Neigel et al., 2020, Pirta-Dreimane et al., 2022). The study made by Dawson and Thomson (2018) stresses the ignorance of social traits in the realm of CS workforce development and argues that the social aspect of human behaviour on networks disregards a crucial element of the cyber domain. The authors identify the requirement for systemic thinkers, team players, a love for continued learning, strong communication ability, a sense of civic duty and a blend of technical and social skills. Similar future skills are suggested by Blažič (2022). The study identifies the main challenges in the current European CS education ecosystem, including gaps between workforce competence needs and education offering, limited use of modern teaching methods and lack of skilled CS educators. The authors refer to Concordia CS competence centre surveys and highlight five main pillars for future CS education: device centric security, network-centric security, software/system-centric security, data/application-centric security and user-centric security.

Besides the related research results from the scientific community, recently established European competence centres *Concordia*, *Cybersec4Europe* and *ECHO* have performed extensive studies on EU CS education ecosystem. The competence centres aim to reshape the EU CS education ecosystem by providing new industry-driven programmes, along with the policies and recommendations for CS curriculum development in the higher education institutions. The conducted studies identified existing limitations within the ecosystem and suggested enhancements. It was recommended to enhance the study content to meet the workforce

requirements, in particular, the authors suggested that educational programme content should be enhanced by incorporating topics that are currently underrepresented, such as organizational or human aspects of CS (Blažič, 2022).

Technology advancements also impact required CS competences. Skillsets needed for CS professionals are evolving rapidly within advanced technology domains. ISC2 CS workforce study 2023 (ISC2, 2023) identifies that organizations report the following main skill gaps in their organizations: cloud computing security, artificial intelligence/machine learning and Zero Trust implementation. Besides, enterprises point out a lack of skills in more traditional CS topics, such as penetration testing, application security, digital forensics and incident response. The most required soft skills are problem-solving, curiosity/eagerness to learn and communication. Similar skill demand highlights the enterprises survey performed by the *CyberSecPro* project (Rathod et al., 2023): CS for artificial intelligence and machine learning, CS threat management/security operation centre, ethical hacking and penetration testing, CS management systems, CS tools and technologies and others. Other survey by *ECISO* (Blažič, 2022) supplements the future skills with a need of security provision skills for the following emerging technologies: big data, blockchain, IoT, cyber-physical systems, network software, mobile device and software engineering technologies.

To summarize, the future CS skillset encompasses the knowledge of basic computer science and CS concepts, usage of SC tools and management systems, organizational and human security-related topics and an understanding of emerging technologies and methods for safeguarding them. The technological topics must consider soft-skill-related competences integration, for example, critical thinking in CS risk management, collaboration and communication in CS incident management and others. The competences must be role-oriented and cover workforce requirements.

Methods and Approach

The study follows the design science problem-solving method (Hevner et al., 2004). It is a systematic approach, connecting practical problems with domain-specific solutions by conducting multiple studies. The investigated challenge is to identify the skills of future workforce for better human performance in cyberspace, considering Latvian context elements, such as workforce structure, knowledge gaps and industry requirements, and define the recommendations to the stakeholders.

Design science research enhances human knowledge by creating innovative artefacts: constructs, models, methods and instantiations. Models use constructs to represent a real-world problem and its solution in the chosen problem communication and definition language. Furthermore, methods define processes and guide how to solve problems. Instantiation demonstrates how other artefacts can be implemented in a working system. Three repeatable cycles make the design science research process (Hevner, 2007). The relevance cycle uses the environmental context and provides research requirements to improve the knowledge base and solve the research problem. The design cycle includes artefact development

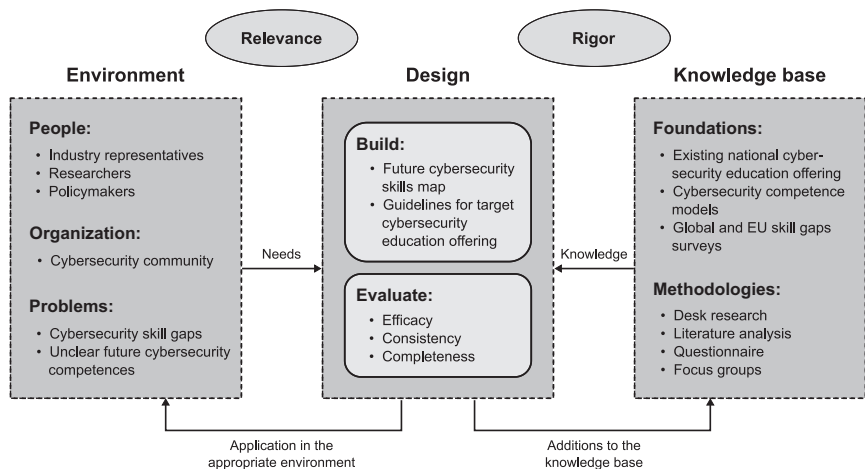


Figure 10.1 Research methodology.

and evaluation. The rigour cycle supports the research with prior knowledge and ensures the solution is innovative.

This study aims to identify future CS skills and provide recommendations for stakeholders about the target CS offering. The stakeholders include academia, policymakers and industry representatives. Figure 10.1 presents the environment, design and knowledge base of the study. Existing national CS education offering (Section 4), CS competence models and global and EU-level skill gaps surveys (Section 5), along with applied research methodologies forms the knowledge base.

Design science problem-solving method allows to combine multiple research methods for comprehensive problem domain investigation and solution design. The primary methods utilized comprised literature analysis, desk research, focus group discussions and questionnaires.

Initially, the desk research was conducted to investigate the CS education ecosystem of Latvia defining the baseline (situation before changes), considering different education levels of CS education ecosystem of Latvia. Desk research involved reviewing Latvian registers and open data, along with exploring information published by educational institutions such as study programmes and courses. Along with the CS education ecosystem analysis, the existing Latvian CS workforce structure was acknowledged, to comprehend the current specialists and competence requirements. The investigation included various sources, such as Latvian open data portal, State Employment Agency of Latvia registers and Latvian vacancies portals.

Following the desk research, an analysis of the state-of-the-art of future CS skills was conducted. The future CS skills were analysed, based on the skill gaps and future competences identified in related research. The analysis of literature laid the foundation for creating a future competences map in the field of CS, considering the context of Latvia. The initial competences map was evaluated by industry experts, adjusting and supplementing it with Latvian-wide CS education needs. For evaluation, a survey was created in the EU Survey tool and populated by the

members of the Latvian CS community, coordinated by the Ministry of Defence of the Republic of Latvia.¹ In total, 45 answers were collected during April 2024.²

The expertise of the Latvian CS community was used to form the guidelines for target CS education offering. In March 2024, the Latvian CS community under the NCC Latvia gathered to participate in a workshop on CS education development. The goal of this activity was to provide qualitative insights for this research and summarize the main gaps and best practices for the development of the Cybersecurity Education Roadmap, further used in policy planning. Thirty-five community experts took part in the workshop, out of which 10 represented public administration, 12 – the industry and 13 – educational institutions. Experts voluntarily split into three equivalent groups and discussed CS education in domains of general basic and secondary education, vocational and higher education and non-formal education and lifelong learning. Design thinking methods were applied to moderate the workshop. Groups were tasked to discuss the topic, and everyone offered their expertise. As a result, groups populated three respective Lean UX Canvas adjusted for this activity, describing stakeholders, problems, opportunities, solutions, activities, outcomes, metrics of success and risks. The whole activity took 90 minutes of experts' work.

The conclusions derived from applied research are condensed in the following sections, establishing a knowledge base for stakeholders.

CS Education Ecosystem of Latvia

CS education ecosystem of Latvia spans across all education levels, starting from general basic education up to second-cycle higher education (master's degree) level. Along with formal education, CS-specific knowledge and competences are widely provided in non-formal education programmes for different adult target groups, while also some for children.

General Basic Education

General education in Latvia encompasses digital knowledge and skills development starting from the very first grade. However, it was only during the school year of 2020/2021 that its scope in all general education programmes switched from applied skills and software to a broader set of topics replacing the subject of Informatics with Computing. At the same time, the gradual switch to competences-based education was introduced at all general education levels. Therefore, CS-related topics, if addressed, can and should be covered within different subjects depending on the perspective (technical, social, legal, etc.).

Current *Cabinet of Ministers* (executive government branch) Regulations on education standards set specific learning outcomes in all fields, including the CS topic. Table 10.1 provides an overview of all CS-related knowledge, skills and competences requirements set in education standards. They can be classified in three categories, where *awareness* describes topics, the student is required to have knowledge about, *hygiene* describes necessary everyday skills and actions of safe computer use while *response* describes skills and competences of preventing and dealing with CS incidents.

Learning outcomes pertaining to CS in general primary education (grades 1–9) are set under two skills:

- 1 Management and use of specific and common functionalities of the office, image, video and audio processing applications.
- 2 Acknowledging the importance of working environment, safety and ethics during the development of qualitative design solutions.

General primary education focuses on building awareness about the virtual environment not only from the perspective of a helpful working space but also from the perspective of security. Primary education does not focus on building skills which could be beneficial for joining a CS career track after the 9th grade. However, the standard sets out only minimum learning outcomes and each educational institution can offer a broader set of skills and knowledge, including focus on CS skills, if it chooses so, but there are no good examples confirming such focus in any of general education institutions. Students are supposed to meet the standard by attending Computing and Design & Technology classes.

Secondary education (grades 10 –12) standard is divided into three levels – general, optimum and the highest. The general level describes the basic standard for any student graduating secondary level of education. Optimum level describes the standard which must be achieved if the student has chosen a subject in optimum level in their programme or the programme focuses on a certain set of subjects (for example, cluster of subjects for career track in engineering). The highest level can be offered through a very specialized set of subjects and not every educational institution is able to offer a wide range of such subjects. They typically are offered during the last year of education (if available at all) to allow students to deepen their knowledge in key examination subjects of their choice. Learning outcomes related to CS for secondary-level students are also set out under two skills:

- 1 Management and use of common and specific features of programmable devices and applications.
- 2 Acknowledging the importance of environmental sustainability, safety and ethics during the use of design solutions and software.

General secondary education provides elements of CS skills and knowledge beyond cyber hygiene, however, applied CS skills are being taught only at the optimum and highest-level subjects if offered by the educational institution. According to the information of the National Centre of Education, the highest-level courses of Programming and Design & Technology are offered only in 1/3 of secondary education institutions, overwhelmingly in Riga region and regions of a few other bigger cities (for example, Liepāja, Ventspils, Rēzekne, Cēsis). The tendency to offer a wider selection of focused courses in secondary education is also closely tied to the number of students in educational institutions: the higher the number of students, the wider the selection of subjects. It suggests that students who are interested in more focused computing education are forced to choose bigger

Table 10.1 CS knowledge, skills and competences matrix of Latvian general basic education standards (Ministru kabineta noteikumi Nr. 416, 2019; Ministru kabineta noteikumi Nr. 747, 2018)

| <i>Education level</i> | | <i>Cybersecurity knowledge, skills and competences</i> | | |
|------------------------|------------|---|--|---|
| <i>Awareness</i> | | <i>Awareness</i> | <i>Hygiene</i> | <i>Response</i> |
| <i>Hygiene</i> | | | | |
| Primary | Grades 1–3 | Knows and reports virtual environment hazards Knows basic factors that can threaten security of devices, software and data | Reduces risk of data loss through automatic and continuous file-saving practices | Turns to an adult for help in critical situations |
| | Grades 4–6 | Knows all factors that can threaten security of devices, software and data | Follows safety rules when working with programmable devices online Uses secure data storing practices Securely manages online identity | Takes measures to avoid possible threats with an assistance of a competent person |
| | Grades 7–9 | Knows security criteria for Internet service subscription and online collaboration tools Identifies identity theft and theft methods | Manages file access rights Saves files in specified storage devices and formats | Takes measures to avoid possible threats |

(Continued)

Table 10.1 (Continued)

| <i>Education level</i> | | | <i>Cybersecurity knowledge, skills and competences</i> | | |
|------------------------|--------------|-------------------|---|---|---|
| <i>Awareness</i> | | | <i>Awareness</i> | <i>Hygiene</i> | <i>Response</i> |
| Secondary | Grades 10–12 | General level | Knows commonly used computer network types and solutions emphasizing safety Knows possible security risks when using open data exchange Compares advantages and disadvantages of open and encrypted data exchange | Selects the most suitable network considering safety Adapts operating system and applications' settings to user needs promoting safety | |
| | | Optimum level | Compares different types of computer networks, their structure, security solutions, and usage options Compares options for preventing security risks when using programmable devices | Configures the router using the computer network wizard | |
| | | The highest level | | Creates and configures an open or local multi-user secured network Creates a simple server and configures access to it from the Internet | Uses cryptographic methods for the solution of specific tasks |

secondary schools, including relocation, or seek extra education outside of the formal education system.

Secondary Professional (Vocational) Education

The only vocational education programme explicitly focusing on CS is “Cybersecurity Technician” offered by Saldus Vocational School.³ It is a part of the civil security and defence cluster of educational programmes. Apart from general secondary education subjects, the programme offers a variety of professional subjects combining technical CS knowledge and skills with broader civil security topics such as crisis response and communication. The only professional education programme in national defence “Junior Military Instructor” at Col. O. Kalpaks Professional Secondary School contains a course of Cybersecurity Fundamentals as part of the mandatory curriculum.⁴

There are no professional secondary education offerings in civilian CS under engineering, computing or management thematic clusters. Even though there is a balanced distribution of professional education programmes in IT (most programmes being “Programming Technician” and “Computer Systems Technician”) throughout the country, they currently lack a focused CS module and include only a broad subject of IT security management, among others. However, the work on a professional standard of a “Cybersecurity Technician” (EQF4) was completed in 2024. It likely will facilitate the creation of vocational programmes throughout the country beyond Saldus Vocational School. The main problem is attracting sufficient and professional teaching staff to ensure the smooth delivery of such a programme.

Non-Formal Education

Non-formal CS education caters for two main audiences – children and teenagers who are interested in the topic and adults who are upskilling or retraining from other fields. Therefore, it is mainly influenced by supply and demand, trying to fill gaps in formal education and meet industry needs.

Children and Teenagers

Children and teenagers are not systematically exposed to non-formal CS education in the form of regular groups. Interest may be sparked while participating in activities under more generic non-formal education programmes (for example, programming) and those are distributed evenly throughout the country. Only Saldus region offers a non-formal CS education group within the premises of Saldus Vocational School. It suggests that the development of non-formal CS education for schoolchildren could be based in the vicinity of several formal professional and/or academic education hubs and not general education institutions.

There are occasional competitions organized for young CS enthusiasts, however, currently, they lack permanence and tradition. A private sector initiative “Kiberplēsis” has been organized since 2022. It is a “capture the flag” (CTF) competition for 16- to 24-year olds. In 2024, the Ministry of Defence in cooperation

with CERT.LV, the University of Latvia and the Latvian National Guard organized the first National Cybersecurity Challenge for 14- to 24-year olds in three stages, encompassing simple test questions, various tasks and CTF challenges. It is intended to keep it as an official state-organized CS competition which provides the national team for the annual European Cybersecurity Challenge organized by ENISA.

A non-formal military education programme of Youth Guard for 10- to 21-year olds which is curated by the Ministry of Defence of the Republic of Latvia spans eight years and is offered in schools of all regions of Latvia. It encompasses some CS topics for all participants within the module “Communications and Cyber Environment” which takes up to 5% of the whole programme and focuses on privacy and security while operating within digital communication environments. Like the Latvian National Guard, also Youth Guard has introduced a specialized unit of a Cyber Youth Guard curated in Saldus Vocational School.

Adults

Non-formal education for adults can be organized as a self-teaching process or as a course. Self-taught knowledge and skills are important in workforce shortage conditions. The most popular MOOC platforms in Europe – Coursera and edEX (Blažič, 2022) – can help to fill some personnel gaps and widen the knowledge of the existing workforce, especially with the support of employers, but no data or signs are confirming that it is a widespread practice in Latvian CS industry. Few state institutions are trying to actively promote enrolment in various offline and online courses. From 2017 until 2023 State Education Development Agency implemented a European Social Fund project “Improvement of professional competences of the employed” which offered various courses and qualifications for employed aged 25+ wishing to develop their knowledge and skills in a variety of fields. During the project almost 77 thousand participants completed courses offered by public and private educational institutions, most of them in their middle adulthood (25–44 years old: 70%) with high educational level (81%). Almost half of all participants (46%) completed various ICT courses. State Employment Agency offers to enrol both unemployed (their direct clients) and employed persons in Coursera courses (previously also Google courses) under institution-owned licences within management, business, languages and IT topics, including CS. The downside of this initiative is that there are no courses in the Latvian language with specifically tailored examples and use cases from Latvia.

Several private companies in Latvia offer regular bootcamps for IT students and professionals from other fields wishing to qualify for entry-level jobs in the industry (for example, *Accenture*, *TietoEvry*, *TestDevLab* and *MageBit*). However, none of them focus on CS explicitly. There are several private learning centres providing CS courses, among which the most important player is *Baltijas Datoru Akadēmija (BDA)* which offers various generic CS courses and specified courses for obtaining CS professional certifications (CISM, CEH, CISSP, CFR-410 and CompTIA Security+/Pentest+/CASP/CySa+). Also notable is *Riga Coding School*

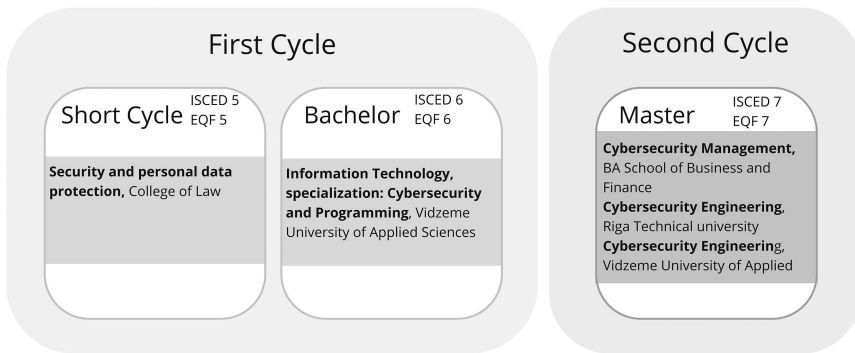


Figure 10.2 Latvian higher education system.

which organizes a Cybersecurity Fundamentals course in English, and its purpose is to serve as a bootcamp but without a specific company affiliation. They provide career centre services to help their graduates in finding internships or entry-level jobs after finishing their courses. To promote inclusion and gender balance in the IT industry, such private initiatives as *Riga TechGirls* and the Latvian branch of *Women4Cyber* are active. Both organizations offer IT training to girls and women (some of them are open to everybody) through online and offline classes, hackathons, targeted workshops and mentorship. Naturally, the CS career track is one of many these organizations are trying to promote.

Higher Education

Higher education addresses the subject of CS in two main ways: first, by incorporating CS-related courses into both postgraduate and undergraduate study programmes and, second, by establishing specialized study programmes focused specifically on CS.

CS higher education programmes are provided from four educational institutions in Latvia⁵: Riga Technical University, BA School of Business and Finance, Vidzeme University of Applied Sciences and College of Law. Latvian higher education system is a part of the Bologna process and follows the 3-cycle system (Zahavi & Friedman, 2019). The programmes correspond to distinct education cycles (Figure 10.2).

College of Law provides a short cycle study programme “Security and personal data protection”.⁶ The study programme aims to ensure an opportunity to obtain the profession of security specialist and educate for professional activities in the field of security and personal data protection (College of Law, 2021). The content of the study programme encompasses law, management, information technology, CS management, security and personal data protection competences, which are required for the security specialist. Upon successful completion of the study programme, graduates are conferred with a professional qualification as a

“security specialist”. Form and duration of implementation of the programme: full time – two years one month and part time – two years six months. The study programme is provided in Latvian language.

Vidzeme University of Applied Sciences provides a bachelor-level study programme “Information Technology” (with specialization of Cybersecurity and Programming) and a professional master’s level study programme “Cybersecurity Engineering”.⁷ The bachelor-level study programme aims to promote the development of the IT industry by educating new specialists, thus promoting the creation of new and innovative products and services with an emphasis on the following areas of specialization – CS and virtual reality and smart technologies, by including the basic skills and knowledge required by the industry in the studies. The content of the study programme includes general IT courses and specialized CS courses, such as information security, applied cryptography, introduction to AI and machine learning, data protection and security and introduction to data science. Form and duration of implementation of the programme: full time – four years. The study programme is provided in the Latvian and English languages. The master’s level study programme aims to provide the necessary competences for a CS specialist who is responsible for strengthening information systems as well as preventing cyberattacks and security incidents, carrying out risk analysis and offering security measures to mitigate threats in their workplace or for an external client. The content of the study programme encompasses CS engineering, CS policy, strengthening information systems and legal and ethical compliance competences. Upon the successful completion of the study programme, graduates receive a professional qualification as “Programming engineer”. Form and duration of implementation of the programme: full time – two years. The study programme is provided in Latvian and English languages.

BA School of Business and Finance provides a master’s level study programme “Cybersecurity Management”.⁸ The study programme aims to provide persons with an opportunity to acquire the profession “information security manager” and to prepare them for professional activities to ensure information security and CS management in the organization. The content of the study programme encompasses management module (leadership, strategic ICT management, information security crisis management, etc.), CS module (CS and critical infrastructure protection, information security governance, etc.) and technical module (cybercrime investigation, personal data protection, information security methods, etc.). Upon the successful completion of the study programme, graduates receive a professional qualification as “Information security manager”. Form and duration of implementation of the programme: full time with professional qualification – two years, full time with academic qualification – 2.5 years. The study programme is provided in Latvian and English languages.

Riga Technical University provides a master’s level study programme “Cybersecurity Engineering”.⁹ to provide a set of theoretical knowledge and practical skills for students to achieve competences corresponding to a master’s degree in CS engineering. In the academic master’s studies, the student acquires the necessary knowledge, skills and competence for comprehensive and effective action in the

field of CS engineering in the chosen economic sector – design, implementation, improvement and management of IT security systems, understanding of professional ethics and socially responsible management, which forms the basis for further studies for a higher level of knowledge and skills acquisition. The content of the study programme includes technically oriented study courses (industrial safety, network security, software security, etc.) and few security management and governance-related courses (social responsibility and business ethics, etc.). Form and duration of implementation of the programme: full time – two years. The study programme is provided in English language.

Besides the specific CS-related study programmes, CS study courses are included in several other study programmes (see illustrative examples¹⁰ in Table 10.2). Mainly, the CS courses are included in computer science programmes, although some courses are included also in social sciences study programmes, as well as in law and civil defence study programmes. The focus of CS courses primarily revolves around technical competences, with less emphasis on human factors. The CS-related courses are mainly included in the master-level study programmes.

To summarize, Latvian higher education institutions provide CS study programmes in first- and second-cycle study levels and cover law, organization and entrepreneurship management, computer science and engineering disciplines. The CS study programmes encompass all Latvian CS professions¹¹: security specialist and information security manager. In general, the coverage of CS study programmes might be evaluated as sufficient. In contrast, there are improvement possibilities in the integration of CS-related courses into non-CS study programmes. Currently, CS courses are integrated mainly in master-level study programmes in computer science discipline. In the future, it is recommended to incorporate information security and privacy aspects into a broader range of study programmes.

Insights of the Latvian CS workforce

Latvian professional standards provide requirements for professional education. The Ministry of Education and Science and the National Centre for Education in cooperation with the Tripartite Cooperation sub-council of Vocational Education and Employment organize the development and expert examination of draft professional standards and vocational standards, inviting representatives of sectoral ministries and professional organizations. As of April 2024, four CS-related professions are defined – information security engineer, information security manager, information systems security specialist and security specialist (Figure 10.3).

Security specialist provides security services to legal and natural persons. Identifies threats within the framework of the law, recognizing the nature of conflict situations. The profession incorporates tasks related to enterprise-wide security, also including CS aspects (for example, the role is responsible about necessary safety technical solutions assessment to ensure personal data protection). Information systems security specialist (specialization of the role “computer and network administrator”) implements the company/institution information and communication technology (ICT) security policy, proposes and implements the

Table 10.2 Illustrative examples of CS courses in undergraduate and graduate study programmes

| <i>Study course</i> | <i>Study programme</i> | <i>Level</i> | <i>Institution</i> |
|---|---|----------------|---|
| Computer Security and Vulnerabilities | Computer Science | Graduate | University of Latvia |
| Secure System Modelling | Computer Science | Graduate | University of Latvia |
| Information Systems Security | Computer Science | Graduate | University of Latvia |
| | Geoinformatics | Under graduate | |
| Web application security | Pre-Trial Investigation | Graduate | University of Latvia |
| | Computer Science | Under graduate | |
| Operating Systems, Servers and Network Security | Teacher of Computing [2020] | Under graduate | University of Latvia |
| | E-Business Management | | |
| Fundamentals of Criminal Investigation, Criminal Intelligence and the Legal Framework for Information Security | Pre-Trial Investigation | Under graduate | University of Latvia |
| Information Systems Security | Computer Systems | Graduate | Riga Technical University |
| Information Security and Personal Data Protection | Information Technology Project Management | Graduate | Riga Technical University |
| Security Management of Enterprise Information Technology | Information Technology | Graduate | Riga Technical University |
| Network Security Requirements | Business Informatics | Graduate | Riga Technical University |
| Fundamentals of Cybersecurity | Information technology | Under graduate | Riga Technical University |
| Fundamentals of Cybersecurity and Personal and Enterprise Information Security | Computer Science | Graduate | Daugavpils University |
| Information Protection | Information Technology | Graduate | Latvia University of Life Sciences and Technologies |
| Economic Cybercrime and Security | Economic Security | Graduate | Riga Stradins University |
| IS Security | Computer Science | Under graduate | Ventspils University of Applied Sciences |
| IS Testing and Cybersecurity | Computer Science | Graduate | Ventspils University of Applied Sciences |
| Information Systems Use and Protection | Land Forces Military Leadership | Under graduate | National Defense Academy of Latvia |

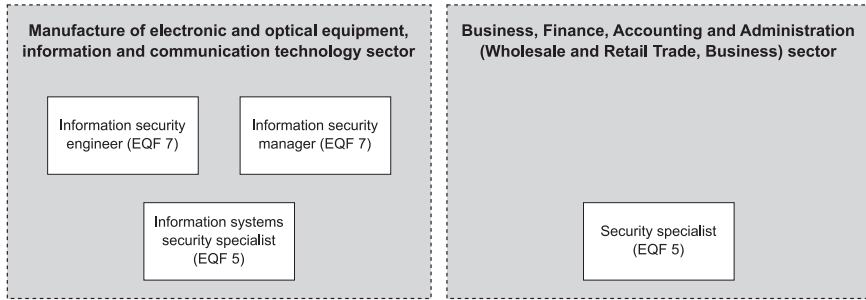


Figure 10.3 Latvian CS professional standards.

necessary security controls, advice, support and information to ensure secure ICT to take direct action to secure all or part of the network or ICT systems. Information security manager manages the implementation, planning, development and monitoring of the information security management system. Organizes the management of risks and incidents related to information resources and contributes to business continuity. Evaluates, analyses and makes proposals to improve the effectiveness of the information security management system. Trains and advises staff within the scope of his/her competence. The profession standard “Information security engineer” is under development.

Meanwhile, the open data of Latvian employment agency¹² and Latvian leading employment portals (CV.lv, WorkingDay) and social networks (LinkedIn) present more complex CS roles’ structure (data on 15.03.2024). Overall, over 12 distinct roles in CS are observed in vacancies data. Table 10.3 provides a summary of the most common vacant roles, each with a minimum of three open vacancies within Latvian enterprises.

In general, Latvian CS roles observed in employment data sources match with ENISA recommendations, showing a diverse set of required CS experts and competences. Meantime, several ENISA roles are compiled in one CS role, showing the need for a wider set of competences. Employers highlight not only technical skills but also general skills and expected personality traits. The most common observed open vacancies are information system security manager (ENISA role: CISO), information technology security analyst/engineer (ENISA roles: Cyber Incident Responder, Cyber Threat Intelligence Specialist), data privacy analyst/data protection officer (ENISA role: Cyber Legal, Policy and Compliance Officer) and security risk management specialist (ENISA role: Cybersecurity Risk Manager). Required competences represent a solid mix of technical, operational, professional and leadership competences, based on the classification proposed in Hajny et al. (2021). Common technical competences include threats analysis and vulnerabilities assessment, information systems/network security and computer network defence. Risk management and data privacy and protection are among the most essential required operational competences. Conflict management, written and oral communications are most wanted professional competences. While, workforce management is essential, considering the leadership competences. In summary,

Table 10.3 Latvian CS vacant roles overview (data on 15.03.2024)

| | <i>Overview</i> | <i>Role</i> | <i>Personal traits and soft skills</i> | <i>Education requirements</i> |
|---|---|--|--|--|
| Information system security manager | Implements, maintains and controls information system security requirements. | knowledge and understanding of information systems security risks and their management practical experience in the field of information technology (at least two years) knowledge of the laws and regulations governing the security of information systems and of the measures to be taken to ensure IS security | Ability to work in high-pressure environments and to find solutions to complex situations | Academic or second-level professional higher education, preferably in information technology. |
| Information technology security analyst/engineer | Protects enterprise digital assets and systems by identifying and responding to CS incidents. | practical experience in OS/IS administration or incident response (more than three to five years) Understanding of Windows and Linux operating systems knowledge of security solutions (SIEM, Antivirus, Vulnerability Management, DLP, etc.) knowledge of Computer networks, firewalls and management tools ability to use cybersecurity programming languages (Python Powershell, etc.) ability to use CS research tools (Binwalk, Procmon, etc.) | High level of self-motivation and ability to work independently and as part of a team, to plan work and take decisions. Ability to work with multiple teams. High sense of responsibility; honesty, integrity. | University degree in computer science, information technology or related field. CS certification (SANS, etc.) |

| | | | | |
|--|--|---|---|---|
| Data privacy analyst/ data protection officer | Ensures compliance with personal data protection legislation requirements. | practical experience in Information Security and/or Data Privacy (at last one to three years) knowledge of data protection law and practice | Good written and verbal communication skills. Proactivity, responsibility and punctuality. Ability to plan and organize work independently, prioritize. Good communication skills, team orientation. | Master's degree in IT, Telecommunications, Law or related areas Passed qualification exam of State Data Protection Inspectorate. |
| Security risk management specialist | Identifies, tracks and reduces security risks. | a deep technical understanding of security assessments and risk management expertise in threat modelling and risk management frameworks broad knowledge of how to operationalize the management of security risk experience in Secure Development Lifecycle and Security by Design methodology | Problem-solver with excellent communication skills. Deep personal motivation. Leadership and management ability. | Undergraduate degree in Computer Science or STEM |

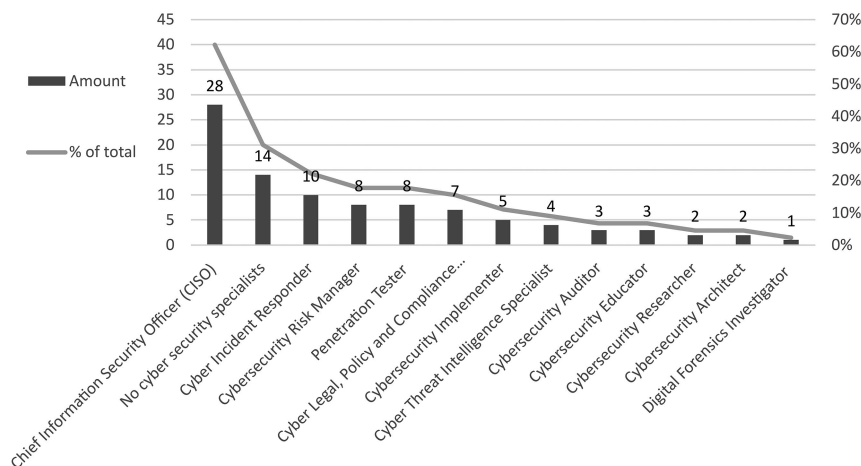


Figure 10.4 Latvian CS roles in organizations (survey data, 45 organizations).

Latvian vacancy data aligns with findings from related studies, confirming the need for multi-disciplinary competences among CS specialists (Figure 10.4).

The survey results show that all ENISA roles are presented in Latvian organizations. The most commonly reported roles are: CISO (existing role in 62% of surveyed organizations), Cyber Incident Responder (existing role in 22% of surveyed organizations), Cybersecurity Risk Manager and Penetration Tester (existing roles in 18% of surveyed organizations). Less represented roles are: Digital Forensics Investigator (existing role in 2% of surveyed enterprises), Cybersecurity Architect and Cybersecurity Researcher (existing roles in 4% of surveyed enterprises). This correlates with Latvian professional standards and vacancy data analysis. Information security manager profession as defined in the profession standard corresponds with the CISO. Therefore, the need of such role is acknowledged within the Latvian organizations. The vacancy data analysis shows that digital evidence investigation and appropriate roles are still missing in enterprises. At the same time, 31% of surveyed enterprises reports no CS specialists in organization. It highlights the rising needs of CS specialists and competences, especially considering NIS2 requirements of certain roles.

Currently, CS specialists of organizations have different educational background (Figure 10.5). Over 70% of surveyed organizations report that, in most of the cases, majority of their CS specialists possess education relevant to the field. Most of the employed CS specialists (an average 51% of surveyed organizations report this profile as the most common) hold a formal degree in CS, information technology, computer science or other field relevant to ENISA's role structure. However, in 27% of surveyed organizations the most common CS specialist profile is a person without any formal education in the field but with the necessary knowledge and skills. It hints that the industry is willing and able to accommodate the needed workforce

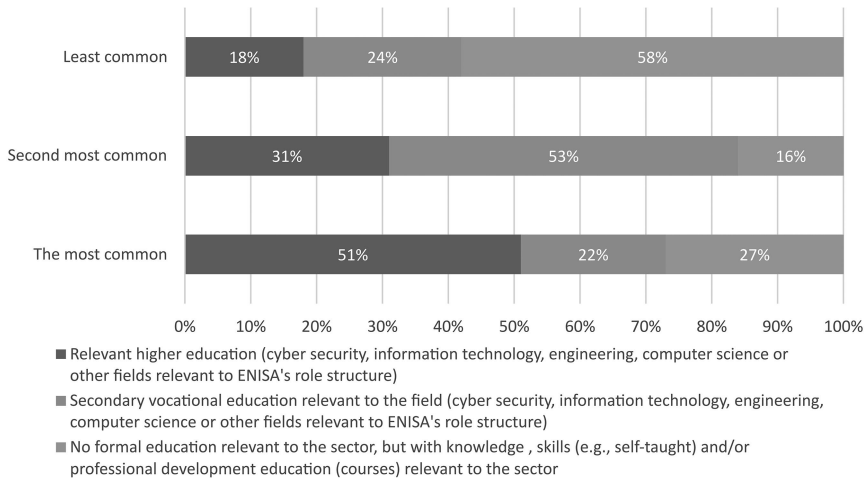


Figure 10.5 Latvian CS specialists' education level (survey data, 45 organizations).

regardless of gaps in formal education provision. Looking at the most common and second most common profiles combined, it is confirmed that the majority of the workforce possesses some formal qualification (82% of organizations reported relevant higher education and 85% reported relevant vocational education as the most common or second most common characteristic). Therefore, it can be concluded that CS education is important for CS specialists and organizations.

Competences Gaps and Future Needs

CS competences gaps and future requirements are defined by Latvian CS community representatives as part of the survey results. Competences are defined, following ENISA ECSF roles' structure, while future needs are based on the related research results, what organizations need to evaluate (using Likert scale), along with the definition of other competences requirements.

The survey results show that the CS competencies gaps of Latvian organizations are diverse, with a notable emphasis on digital forensics, cyber threat intelligence and the development of CS architecture (Figure 10.6).

The most competences gaps are reported in the areas of digital forensics (49% of surveyed enterprises) and cyber threat intelligence (47% of surveyed enterprises). This is also evident in the vacancy data analysis. The finding corresponds to the identified EU-level skill gaps (ISC2, 2023). Besides, the analysis shows that this area is currently weakly covered by educational programmes of Latvia. The relevant study courses in digital forensics and cyber threat analysis are represented only in the part of higher education programmes of CS. The competence is weakly covered also in non-formal education courses in Latvia.

Future competences required by organizations well aligns with the results of related studies described in Section 2.3 (Figure 10.7).

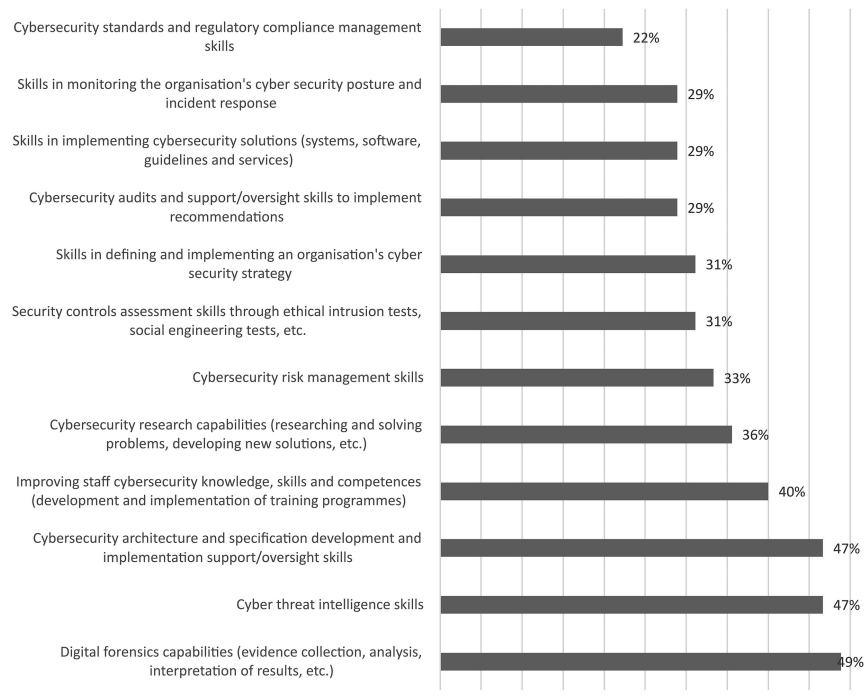


Figure 10.6 Competences gaps of Latvian organizations (survey data, 45 organizations).

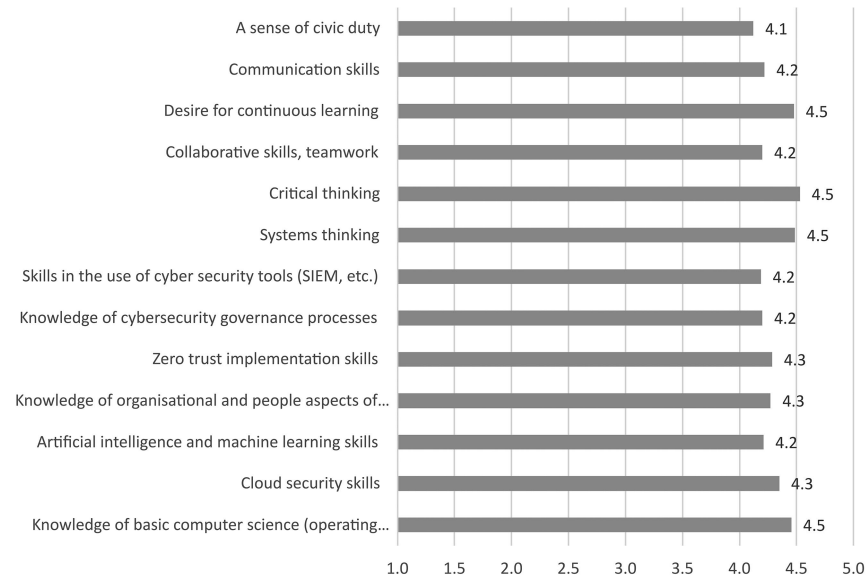


Figure 10.7 Future CS competency needs (survey data, 45 organizations).

Organizations admit that all future skills identified in related research studies are relevant for CS professionals. Results of survey show that, besides the knowledge of basic computer science (operating systems, computer networks, programming, system architecture, etc.), soft skills are becoming critical, considering the workforce of tomorrow. The organizations highlight the following important future competences: basic computer science, critical thinking, systems thinking and desire for continuous learning (average rating 4.5 from 5 points). Reported less important skills are sense of civic duty (average rating 4.1 from 5 points), artificial intelligence and machine learning skills, collaboration, communication and team work, skills in the use of CS tools and knowledge of CS governance processes (average rating 4.2 from 5 points). Meantime, all listed competences are rated above 4 points of 5, therefore it might be concluded that all of them are relevant in terms of future workforce.

Besides the mentioned skills, organizations suggest the following future skills: stress tolerance, ability to convince to implement a solution (getting buy-in, ability to justify to ordinary users why controls are needed), reverse engineering, binary analysis, data forensics, incident tracking, exploit development, bug chain exploration, responsible vulnerability disclosure, open attack activities, ability to combine multiple areas into one, DFIR, xdev, monitoring and ability to create migration schemes (on-premises – cloud, etc.).

Future CS Education Provision and CS Skills

The study highlights several improvement areas within the area of CS education provision and defines future CS skills to be integrated in education programmes. Education provision recommendations can serve as a basis to plan future CS education development, considering the initiatives of government bodies, education institutions, communities and groups of interest. Future CS skills can serve as a competences map to be integrated in the future educational programme design.

Education Provision

CS education in Latvia is fragmented and there is no process owner (an institution or a collegial body) nationally which is assigned to lead the effort of coordinated development of this field. While most of the education development processes are overseen by the Ministry of Education and Science, it does not concentrate on CS as a distinct field. Also, CS community experts revealed that many educational initiatives are reaction to the industry needs, yet they do not guarantee quality and matching with the right audiences. Overall, experts felt that CS knowledge and skills development is as important task for educational institutions as it is also for society, especially family who should practice cyber hygiene.

General basic education only recently switched to competences-based model and replaced a focus on computer use (such as applied informatics) to general computing knowledge and skills. Even though general basic education incorporates some CS topics throughout grades 1–12, deeper knowledge in computing is

available only in a select number of schools and regions. Experts also noted that there is a problematic CS environment in schools, including insufficient cyber hygiene among schoolchildren and their parents as well as among staff. General educational institutions tend to have no IT security policy in place and not all teachers of Computing are proficient in CS field to address this topic, both in their organizations and the classroom. Organized non-formal CS education for kids is mostly non-existent, however, lately several state-wide competitions have emerged. Based on this research, general basic education shall:

- Start introducing the CS topic early, for example, through cartoons.
- Include more non-formal activities to fill the gaps – informal visits to schools by field experts, competitions (e.g., “hack your classmate” CTF and state-wide challenges), gamification elements, summer camps and non-formal education groups.
- Introduce universal cyber hygiene evaluation tests to assess the situation and progress.
- Integrate the topic in other classes, for example, when developing interpersonal (digital) communication and critical thinking skills, as well as providing materials for teachers of other fields on integration methodology.
- Support teachers on efficient and secure use of technology, including cyber hygiene and tools training, especially when obtaining new hardware and software.

Secondary professional education in CS is not developed, yet there are initiatives to widen it through standardization.

Non-formal CS education for adults is rather widely available. State institutions acknowledge the shortage of ICT specialists and try to encourage people to use various lifelong learning opportunities. The private sector also is reacting to this problem; however, CS courses due to their specificity are largely targeted towards industry specialists who seek professional upskilling and certification, much less on people who are trying to land entry-level jobs. Overall, courses are expensive, not centrally coordinated by government bodies and fragmented. A positive sign is the promotion of diversity and inclusion in the Latvian ICT industry which fosters various societal groups to consider a career in IT, including CS. Non-formal education for adults shall:

- Be included as a focused part of Cybersecurity Education Roadmap; thus, assigning an institutional and strategic ownership of this field.
- Continue to receive support in the form of public investment through various lifelong learning projects and schemes.
- Be communicated to right audiences to motivate them to take part in CS education.
- Introduce certification or evaluation schemes to determine quality of courses.

Higher education offering of Latvia currently includes several CS study programmes (see Section 4), therefore, experts acknowledge that the general CS study programmes coverage is sufficient in the graduate and undergraduate study levels. Meanwhile, there is lack of doctoral study programmes in CS, what could enhance CS research capabilities. The experts also highlight that integration of CS-related courses into non-CS study programmes remains limited, primarily confined to master's level computer science programmes.

Higher education shall:

- Integrate cyber hygiene, information security, CS and privacy aspects into a wider array of educational programmes (including also non-IT study programmes).
- Specify CS as a separate unit in the education classification.
- Define legislation requirement to include cyber hygiene as a compulsory course in all study programmes (similar to occupational safety courses).
- Establishment of a motivation system for CS educators.
- Establish a PhD study programme in CS.
- Align the content of CS study programmes with the topics of certificates required by the industry (so that after graduation, students are able to take certificates and obtain additional qualifications).
- Train educators in different CS-related fields using a “train the trainer” approach.
- Consolidate and maintain CS training materials in a common environment (MOOC-type courses, materials, etc.).
- Expand training opportunities for CS managers (demand for competences will increase significantly as a result of the NIS2 Directive).
- Establishment of a research grant programme in the field of CS.

In addition to the opinions of CS community experts in the workshop, several recommendations have been provided by representatives of the surveyed organizations. The recommendations have been classified, considering the target stakeholder group to consider the recommendation (Table 10.4).

To summarize, recommendations include starting CS education early, integrating CS into non-formal activities and evaluating cyber hygiene universally. Furthermore, initiatives to integrate CS into all levels of education, improve training for educators and align educational content with industry standards are essential. Collaboration with international organizations and industry stakeholders, along with the establishment of a virtual university and a public buyback programme for Zero Day vulnerabilities, are suggested to bolster CS education in Latvia.

Future CS Skills

Future CS skills must be aligned with the industry requirements (see Section 6), considering missing competences, soft skills and new technology trends. The summary of the required skills is presented in Table 10.5, considering the classification proposed in Hajny et al. (2021).

Table 10.4 Organizations recommendations for CS capabilities strengthening (data on 30.04.2024)

| <i>Stakeholder group</i> | <i>Recommendations</i> |
|--------------------------|--|
| Policy makers | <p>Promote transparency of national infrastructure and provide formats where students can test and improve national infrastructure.</p> <p>Include cyber hygiene awareness-raising content from an early stage of education. More educate citizens and find simple ways how to stress CS importance.</p> <p>Develop and diversify occupational standards and provide educational content material for all age groups, with the opportunity (and funding) for educational institutions and professionals to contribute to their development. Establish common requirements for the competences of CS professionals. Establish common criteria for the introduction/non-introduction of a CS specialist.</p> <p>Provide additional funding to attract cybersecurity experts.</p> <p>Ensure more research programmes for researchers in CS and security software (dfir, xdev, c2, etcml) development, both at hardware level, IoT devices and software level research for IoT devices.</p> <p>Establish a public Zero day/bug buyback programme and/or ban Zero day and related code trading in Latvia.</p> <p>Revamp Latvia's competences standards to align with current industry standards, focusing on in-depth Linux/Windows topics such as Phrack and PoC GTFO. Update training materials regularly to incorporate the latest information, ensuring compatibility with current security measures like ALSR, Apparmor and SELinux.</p> <p>Empower CS experts and specialists to advocate for the adoption of the latest security standards and legislation, driving the rapid and robust development of CS competences.</p> <p>Maintain an up-to-date website with a register of all available institutions and courses, demonstrating the knowledge areas covered by each and linking to ENISA profiles,</p> <p>Establish a virtual university for CS training in Latvia, offering comprehensive roadmaps and certifications. Fees waived for critical infrastructure or government employees, with reimbursement required if they leave within two years unless transitioning to another critical role.</p> |

| | |
|----------------------------|---|
| Education providers | <p>Develop an education programme and training plan for public administration employees.</p> <p>Enhance CS education at all levels: Introduce CS basics in primary schools. Organize conferences, lectures and competitions on cybersecurity for primary and secondary students. Offer CS courses in technical schools and colleges. Develop specialized courses in higher education. Provide flexibility for students to change focus. Strengthen managerial, architectural skills and interdisciplinary aspects in master's programmes.</p> <p>Align training programmes with industry-recognized standards, structured for various age groups and skill levels.</p> <p>Utilize modern digital training systems for adaptive learning, enhancing outcomes.</p> <p>Ensure flexible and rapid processes for updating programmes to meet evolving needs. Educational programmes must be able to react and adapt (Agile education).</p> <p>Involve foreign lecturers in the teaching process.</p> <p>Encourage participation in competitions and create new development programmes aimed at school/college students to attract as many people as possible into the field.</p> <p>Increase education on modern technologies, making them accessible to beginners, including topics like SIEM, FW and XDR, along with migration strategies. Incorporate current IT trends such as containers and cloud services into training materials. Enhance understanding of attacker perspectives to strengthen CS knowledge.</p> |
| Industry | <p>Increase awareness of the importance and contribution of CS professionals to organizations.</p> <p>Educate employees in CS at least at three levels – basic cybersecurity for employees working with internal IT systems (all companies) intermediate cybersecurity (cybersecurity manager in the company (all companies)) level-3 senior cybersecurity specialist (cybersecurity research, intelligence, etc., preventive actions (in specialized organizations)).</p> |
| All groups | <p>De-emphasizing or de-emphasizing hackathon events and more frequent CTF or publicly available security events. More emphasis on reverse engineering, similar to the recon.cx conference, could invite guests from Europe.</p> <p>More frequent events in the regions, engagement from municipalities with current challenges, their way forward in CS, engagement with educational institutions, possible internships.</p> <p>Establish volunteer programmes focused on teaching CS topics, facilitating experiential learning and engaging in incident response and malware research. Participants of these programmes can include individuals seeking to address technical challenges.</p> <p>Present to new stakeholders what attacks are relevant today, including the use of Zero day. Promote cooperation with public authorities on new types of attack, their disclosure in the public information space.</p> <p>Create publicly available resources on good programming practices, their adherence in the learning environment.</p> <p>Create an initiative for programmers/developers to outsource software or functions for testing or testing in a research environment to reduce software bugs and vulnerabilities.</p> <p>Strengthen collaboration with NIST/CISA to teach how to use existing tools, standards for business or critical infrastructure.</p> <p>Collaborate with large companies to promote the interest of trainees (Latvia, EU/EEA, NATO).</p> |

(Continued)

Table 10.4 (Continued)

| <i>Stakeholder group</i> | <i>Recommendations</i> |
|--------------------------|---|
| Policy makers | <p>Promote transparency of national infrastructure and provide formats where students can test and improve national infrastructure. Include cyber hygiene awareness-raising content from an early stage of education. More educate citizens and find simple ways how to stress CS importance.</p> <p>Develop and diversify occupational standards and provide educational content material for all age groups, with the opportunity (and funding) for educational institutions and professionals to contribute to their development. Establish common requirements for the competences of CS professionals. Establish common criteria for the introduction/non-introduction of a CS specialist.</p> <p>Provide additional funding to attract cybersecurity experts.</p> <p>Ensure more research programmes for researchers in CS and security software (dfir, xdev, c2, etcml) development, both at hardware level, IoT devices and software level research for IoT devices.</p> <p>Establish a public Zero day/bug buyback programme and/or ban Zero day and related code trading in Latvia.</p> <p>Revamp Latvia's competences standards to align with current industry standards, focusing on in-depth Linux/Windows topics such as Phrack and PoC GTFO. Update training materials regularly to incorporate the latest information, ensuring compatibility with current security measures like ALSR, Apparmor and SELinux.</p> <p>Empower CS experts and specialists to advocate for the adoption of the latest security standards and legislation, driving the rapid and robust development of CS competences.</p> <p>Maintain an up-to-date website with a register of all available institutions and courses, demonstrating the knowledge areas covered by each and linking to ENISA profiles.</p> <p>Establish a virtual university for CS training in Latvia, offering comprehensive roadmaps and certifications. Fees waived for critical infrastructure or government employees, with reimbursement required if they leave within two years unless transitioning to another critical role.</p> |

Table 10.5 Future CS skills recommendations (data on 30.04.2024)

| <i>Type of competences</i> | <i>Competences</i> |
|---------------------------------|--|
| Technical competences | Basic computer science knowledge Artificial intelligence and machine learning Skills in the use of CS tools Cloud security Zero trust implementation Reverse engineering Binary analysis Data forensics Incident tracking Cybersecurity tools (SIEM, etc.) Exploit development Bug chain exploration Responsible vulnerability disclosure Open attack activities Ability to combine multiple areas Digital Forensics and Incident Response (DFIR) Cross-development (xdev) Monitoring Ability to create migration schemes (e.g., on-premises to cloud) |
| Operational competences | CS governance processes Organizational and people aspects of cybersecurity Critical thinking Systems thinking |
| Professional competences | Desire for continuous learning Sense of civic duty Collaboration, communication and teamwork Stress tolerance |
| Leadership competences | Ability to convince others to implement solutions |

These skills highlight the evolving demands on CS professionals in the future workplace.

Conclusion

This study investigated the existing CS education ecosystem in Latvia, gaps and future education needs to straighten human performance in CS. It was concluded that Latvian situation and needs correspond with EU-level findings. There is a notable deficiency of CS professionals and competences, and the skills gap is continuing to widen. Organizations lack several roles with the biggest emphasis on: Digital Forensics Investigator, Cybersecurity Architect and Cybersecurity Researcher. In terms of the missing competences organizations highlight digital forensics and cyber threat intelligence. Therefore, it is concluded that digital forensics capabilities represent the most critical area requiring enhancement. This can be achieved by offering specialized education programmes in various formats, including formal education, lifelong learning courses and other initiatives. The research results show that, currently, these competences are less represented in educational offering. Besides, organizations highlight several future competences needs,

including basic computer science knowledge, critical thinking, systems thinking, desire for continuous learning. These competences should be taken into account when updating existing education programmes and developing new ones.

The study indicated several findings and provided recommendations to stakeholders to enhance CS educational offering and capabilities. It was concluded that CS education in Latvia is fragmented and lacks a dedicated national coordinating body. Other findings varied across different education levels. Basic education includes some CS topics, but deeper knowledge is limited to select schools, and overall cyber hygiene in schools is insufficient. Non-formal education for both children and adults is available but fragmented and often expensive, with a need for better coordination and quality assurance. Experts recommend early introduction of CS topics, increased non-formal activities, support for teachers and integration of CS into a wider array of educational programmes, along with the establishment of doctoral programmes and a research grant system in CS.

The study provides insightful findings on existing CS education ecosystem and future competences needs, while it has also limitations. The notable limitation is relatively small survey respondents' amount (45 organizations). Meanwhile, the surveyed organizations are members of the Latvian CS community, indicating they likely have considerable interest in and expertise on the topic. The respondents' amount could be extended as part of the future research. Besides, the industry or domain-specific CS roles and competences could be analysed to present findings tailored to each industry or domain.

Notes

- 1 ECCC National Coordination Center | Aizsardzības ministrija (mod.gov.lv).
- 2 The number of organisations registered in the Latvian CS community at the time of questionnaire – 46.
- 3 Saldus tehnikums | Kiberdrošības tehnikis.
- 4 Mācības | Pulkveža Oskara Kalpaka profesionālā vidusskola (kalpakaskola.lv).
- 5 NIID.LV | Nacionālā izglītības iespēju datubāze.
- 6 Security and Personal Data Protection – Juridiska Koledža (jk.lv).
- 7 Cybersecurity Engineering | Vidzeme University (va.lv).
- 8 Professional Master's Degree in Cybersecurity Management (ba.lv).
- 9 Cybersecurity Engineering | Riga Technical University (rtu.lv).
- 10 The list offers only illustrative examples; it does not encompass the full range of CS-related study courses.
- 11 Profesiju standarti un profesionālās kvalifikācijas prasības | Valsts izglītības satura centrs (visc.gov.lv).
- 12 Vakances – Datu kopas – Latvijas Atvērto datu portāls (data.gov.lv).

References

- AlDaajeh, S., Saleous, H., Alrabae, S., Barka, E., Breiting, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119, 102754. <https://doi.org/10.1016/j.cose.2022.102754>
- Allianz Commercial. (2025). Allianz Risk Barometer: Identifying the Major Business Risks for 2025. *Allianz Global Corporate & Specialty SE*.

- Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, 25(5), 829–841. <https://doi.org/10.1007/s00779-021-01551-2>
- Australian Government. (2023). 2023–2030 Australian Cyber Security Strategy. *Department of Home Affairs*.
- Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, 27(3), 3011–3036. <https://doi.org/10.1007/s10639-021-10704-y>
- Bukauskas, L., Brilingaitė, A., Juozapavičius, A., Lepaitė, D., Ikamas, K., & Andrijauskaitė, R. (2023). Remapping cybersecurity competences in a small nation state. *Heliyon*, 9(1). <https://doi.org/10.1016/j.heliyon.2023.e12808>
- Cabinet Office. (2023). *National Cyber Strategy 2022: Annual Progress Report 2022–2023*. Cabinet Office.
- College of Law. (2021). *Self-Evaluation Report of the Study Field “Management, Administration and Management of Real Property” 2021/2022*. College of Law. <https://jk.lv/en/2023/08/14/2700-educational-institutions-and-study-programs-recommended-by-employers/>
- Cutas, F., Chatzopoulous, A., Athanatos, M., & Antonakaki, D. (2023). *CONCORDIA Governance model for a European Education Ecosystem for Cybersecurity*.
- Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 9, Issue (JUN). <https://doi.org/10.3389/fpsyg.2018.00744>
- de Casanove, O., & Sèdes, F. (2021). Guidelines for {Security} {Education}, {Training} and {Awareness}: a literature review. *{CEUR} {Workshop} {Proceedings} ({CEUR}-{WS}.Org)*.
- Dragoni, N., Lafuente, A. L., Schlichtkrull, A., & Zhao, L. (2020). D6.2 Education and Training Review. *CyberSec4Europe Project*. <https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submitted.pdf>
- ENISA. (2022a). *Cybersecurity Education Initiatives in the EU Member States*.
- ENISA. (2023, September 21). *Cybersecurity Skills Conference: Strengthening human capital in the EU*. <https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu>.
- ENISA. (2024, May 15). *Cybersecurity Higher Education Database*. <https://www.enisa.europa.eu/topics/education/cyberhead#/>.
- ENISA. (2022b). *European Cybersecurity Skills Framework*. <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>.
- Furnell, S. (2021). The cybersecurity workforce and skills. *Computers and Security*, 100. <https://doi.org/10.1016/j.cose.2020.102080>
- Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, tools and good practices for cybersecurity curricula. *IEEE Access*, 9, pp. 94723–94747, <https://doi.org/10.1109/ACCESS.2021.3093952>
- Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems*, 19(2). Article 4. <https://aisel.aisnet.org/sjjs/vol19/iss2/4>
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- Hore, K., Hoi Tan, M., Kehoe, A., Beegan, A., Mason, S., Al Mane, N., Hughes, D., Kelly, C., Wells, J., & Magner, C. (2024). Cybersecurity and critical care staff: A mixed methods study. *International Journal of Medical Informatics*, 185, 105412. <https://doi.org/10.1016/j.ijmedinf.2024.105412>

- ISACA. (2021). *State of Cybersecurity 2021, Part 1*. Isaca.
- ISC2. (2023). *ISC2 Cybersecurity Workforce Study 2023*. ISC2. https://media.isc2.org/-/media/project/ISC2/main/media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e
- ISC2. (2024, September 11). *Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen*. ISC2. <https://www.isc2.org/insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen>.
- Jelo, M., & Helebrandt, P. (2022). Gamification of cyber ranges in cybersecurity education. *20th Anniversary of IEEE International Conference on Emerging ELearning Technologies and Applications, ICETA 2022- Proceedings*. Stary Smokovec, Slovakia. <https://doi.org/10.1109/ICETA57911.2022.9974714>
- Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, 23(2), 361–373. <https://doi.org/10.1007/s10796-019-09977-z>
- Ministru kabineta noteikumi Nr. 747 “Noteikumi par valsts pamatizglītības standartu un pamatizglītības programmu paraugiem” (2018).
- Ministru kabineta noteikumi Nr. 416 “Noteikumi par valsts vispārējās vidējās izglītības standartu un vispārējās vidējās izglītības programmu paraugiem” (2019).
- Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers and Security*, 92. <https://doi.org/10.1016/j.cose.2020.101731>
- OECD. (2024). *Building a Skilled Cyber Security Workforce in Europe*. OECD. <https://doi.org/10.1787/3673cd60-en>
- Payne, B. K., He, W., Wang, C., Wittkower, D. E., & Wu, H. (2021). Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course. *Journal of Information Systems Education*, 32(2), 134–149. <https://doi.org/10.21428/cb6ab371.8113760b>
- Petersen, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). *NIST Special Publication 800-181, Revision 1, 3*.
- Pirta-Dreimane, R., Brilingaitė, A., Majore, G., Knox, B. J., Lapin, K., Parish, K., Sütterlin, S., & Lugo, R. G. (2022). Application of intervention mapping in cybersecurity education design. *Frontiers in Education*, 7. <https://doi.org/10.3389/feduc.2022.998335>
- Ramezani, S., & Niemi, V. (2024). Cybersecurity education in universities: A comprehensive guide to curriculum development. *IEEE Access*, 12, 61741–61766. <https://doi.org/10.1109/ACCESS.2024.3392970>
- Rathod, P., Ofem, P., Polemi, N., Hynninen, T., Lugo, R. G., Alcaraz, C., Kioskli, K., & Rannenberg, K. (2023). D2.1 Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyse. *CyberSecPro Project*. https://www.cybersecpro-project.eu/wp-content/uploads/2023/07/D2.1_Cybersecurity_Practical_Skills_Gaps_in_Europe_v1.0.pdf
- ENISA (2025). *EU incident response and cyber crisis management*. <https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management>.
- Torres, M., & Thompson, N. (2020). Toward a cyber security adoption framework for primary and secondary education providers. *Australasian Conference on Information Systems 2020 Proceedings, Wellington, New Zealand*, 1–8.
- Yang, S. C., & Wen, B. (2017). Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States. *Journal of Education for Business*, 92(1), 1–8. <https://doi.org/10.1080/08832323.2016.1261790>
- Zahavi, H., & Friedman, Y. (2019). The bologna process: An international higher education regime. *European Journal of Higher Education*, 9(1), 23–39. <https://doi.org/10.1080/21568235.2018.1561314>

11 Cyber-Physical Systems

Securing Latvia's Future

*Krišjānis Nesenbergs, Eduards Blumbergs
and Pēteris Paikens*

Introduction: Cyber-Physical Systems at the Crossroads of Emerging Security Issues

In the contemporary era, driven by technological innovation, a multitude of sophisticated systems have emerged that combine the domains of physical operations and computational intelligence, including smart transportation, urban infrastructure, advanced biomedical wearables, consumer devices, and resilient military technologies. These systems, collectively known as cyber-physical systems (CPS), represent a significant advancement in the integration of computational algorithms and the physical world. CPSs play a key role in enabling advanced defense mechanisms, increased situational awareness, and optimized logistic and support systems, focusing on increased automation, precision, reliability, and operational efficiency through the integration of sensors, actuators, and embedded systems that interact directly with the operational environment.

The major categories of CPSs are the following:

- 1 **Agriculture:** Sensors and automated machines that improve the efficiency of farming.
- 2 **Autonomous vehicles:** Cars, UAVs, and other vehicles that can perform tasks without human intervention, including aircraft flight systems.
- 3 **Civil infrastructure and transportation:** Systems designed to improve efficiency through digital techniques, including Internet of Things (IoT) sensors.
- 4 **Healthcare and medical monitors:** Connected medical devices and wearables that track health metrics and provide data to healthcare providers.
- 5 **Mobile and wearable systems:** Robotic equipment and electronics that can be worn by humans or animals, commonly associated with the use of smartphones.
- 6 **Robotics and manufacturing:** Systems provide interaction with the physical world and are typically used in manufacturing, inspection, and service operations.
- 7 **Smart grids and industrial control:** Systems that monitor and control industrial processes, including manufacturing, power generation, and refineries.

Characterized by the ability to continuously monitor and control physical processes, CPSs rely on real-time computing and network connectivity. Due to their

integrated nature and high reliability and security requirements, these systems are more complex than traditional IoT devices. They can operate at different levels of time and space, exhibit multiple and distinct behaviors, and interact with each other in a context-aware manner.

As CPSs become more prevalent in various domains, the security threats associated with these systems become more critical. The security of CPSs is a complex and multidimensional issue that must consider the protection of various elements, including hardware, software, and communication channels, from potential malicious attacks and vulnerabilities.

Global Relevance of CPS Security

The security of CPS presents unique challenges compared to the general approach to information system security which is primarily concerned with formally structured organizations and technologies (Koskosas & Asimopoulos, 2011). When considering threats to the general society (contrasting to threats to functioning of commercial organizations), it is important to consider all the informal consumer activities in their daily life and threats to the IT systems used, which increasingly are local CPSs.

Currently, we observe (Paikens & Nesenbergs, 2024) a contrast between the security practices of systems relying on formally structured and well-understood communications technologies, forming a network that is explicitly managed by an organization, such as Ethernet and WiFi access points, while the more flexible wireless communications and consumer networking technologies are often designed with inherent security flaws (Schmidt, 2006). Although this should motivate a greater scrutiny of CPSs and their security, the opposite is often true.

There is a subset of more mature technologies, such as cell phone protocols (Ferag et al., 2018; Odarchenko et al., 2018; Wang et al., 2016) and WiFi (Hooper et al., 2016; Peng, 2012; Sagers et al., 2015), which are dominantly used by businesses that can and do apply market pressure to require investigation and improvement of security issues, and thus for these technologies more control and understanding has been accumulated over the years even if the resilience of these technologies is highly reliant on minimizing the attack surface. However, the challenges of CPSs appear when going beyond a limited diversity of organization-issued devices with a limited number of known wireless connections – the advent of smaller, more energy-efficient IoT devices and the related differentiation in specialized needs for wireless communications has motivated device manufacturers to adopt new, less mature protocols that lack verified, secure implementation mechanisms. The usage of consumer market CPSs has had little practical investment in security than the corporate and government systems. The market growth of a large variety of cheap wireless consumer devices means that they are treated as disposable and not worthy of attention, so neither users nor manufacturers have much desire to pay attention to their security risks. At the same time, these devices have powerful capabilities and accompany their users almost everywhere, in their homes and workplaces, during transit, and in leisure time.

The risks to personal privacy are growing as many people carry not only a smartphone but also multiple smart embedded or IoT devices with wireless connection capabilities. If a malicious actor takes control of such devices, they can create a variety of security risks – they can serve as Trojan horses into secure infrastructure (Arias et al., 2015); become sources of distributed denial-of-service (DDoS) attacks (Doshi et al., 2021; Khader & Eleyan, 2021); allow the extraction of secret information leading to industrial espionage (D’Mello et al., 2018), political espionage (Carstens et al., 2019), and extortion (Ibarra et al., 2019); and could also potentially hold malware from advanced persistent threats (APTs) or state actors (Blow et al., 2020). There are also the privacy and surveillance risks of tracking or fingerprinting specific devices using their wireless communications (Blumbergs et al., 2022; Xu et al., 2015). The straightforward solution of having a policy to remove every consumer-wearable device is feasible only in highly controlled environments, and even in this case, there may be issues with devices such as medical implants that have similar risks but cannot be removed or sometimes even detected (Kim et al., 2015). These risks to CPSs and the lack of social resilience in case they should be abused on a large scale motivate the following work.

CPS Communication Security Challenges

The integration of wireless consumer devices, such as rugged smartphones, wearables, and IoT solutions, represents a critical evolution and serves not only as channels for communication but also as strategic assets that merge the digital with the physical, significantly increasing operational efficiency and situational awareness in various domains. For example, drones equipped with IoT sensors provide real-time information and insight into battlefield conditions. Similarly, intelligent tracking systems streamline the movement of supplies, mitigating the risks associated with mismanagement and loss.

However, the growing reliance on these technologies underscores the critical need to address their inherent security vulnerabilities, especially given the need for secure and reliable communications. The widespread availability of advanced hacking tools, such as software-defined radios (SDRs), underscores the need for rigorous cybersecurity measures specifically tailored to meet unique operational and strategic requirements. CPS devices use a variety of wireless communication protocols that are critical to facilitating real-time data sharing, strategic mobility, and improved field operations.

Access Control Systems

Access control systems are vital for safeguarding physical and digital assets by controlling who can access specific resources. These systems comprise components such as chip cards, readers, controllers, and management software. However, they are also vulnerable to a range of risks that could potentially compromise security.

The most common vulnerabilities in access control systems are broken access control itself, card cloning, wire tampering, and communication channel hacking (Pao, 2021). Inadequate access control occurs when the restrictions placed on

authenticated users are not properly enforced. This can be avoided by implementing the least-privilege principle, conducting regular system audits, and employing robust session management. Replication of RFID or magnetic stripe cards can be achieved through the use of inexpensive hardware when the encryption of the chips and shielded badge holders are not employed. Furthermore, exposure to access control system wires presents a risk of unauthorized manipulation, which can lead to gain access to critical systems. Lack of encapsulation or weak encryption of communication channels between access control components can result in unauthorized access and data interception. By understanding these vulnerabilities and implementing robust solutions, organizations can enhance their security posture and protect critical CPSs from unauthorized access.

The use of biometric data (e.g., fingerprints and facial recognition) for access control is becoming more common, offering enhanced security and convenience in authentication procedures. This approach takes advantage of the unique physical characteristics of individuals, making it difficult for unauthorized users to gain access. Recent studies highlight the integration of biometric systems in IoT environments, particularly to secure a wide range of emerging devices (Yang et al., 2021).

Artificial intelligence (AI) and machine learning are increasingly being used to identify anomalies in access patterns, enabling the real-time detection of potential security threats by analyzing user behavior and flagging deviations from typical patterns. This proactive approach improves the security of access control systems by preventing unauthorized access before it occurs (Alotaibi, 2023).

Blockchain technology is being explored as a potential solution for decentralized access control systems. By providing a tamper-proof and transparent approach to access management, the blockchain ensures that access control decisions are verifiable and immutable. This can significantly reduce the risk of unauthorized access and improve overall system integrity (Yang et al., 2021).

As the number of IoT devices continues to grow, it is increasingly important to integrate robust access control mechanisms to secure interconnected environments. Future systems may employ adaptive access control models capable of dynamically adjusting permissions based on contextual factors such as location, time, and behavior. This flexibility can improve security by ensuring that access rights are constantly aligned with the current context of use.

The implementation of zero-trust principles, which establish a default state of distrust and require continuous verification, will significantly impact the manner in which access control is operationalized and enforced. This approach assumes that threats can exist both inside and outside the network; therefore, every access request must be thoroughly authenticated, authorized, and encrypted before granting access (Edo et al., 2023).

4G and 5G Cellular Networks

4G and 5G cellular networks provide the backbone for mobile data communications, dramatically increasing connectivity and speed. 4G offers speeds of up to

100 Mbps, while 5G, with capabilities of up to 10 Gbps, promises to revolutionize high-bandwidth applications, enabling instant video surveillance and augmented reality for combat training. However, their vulnerabilities include susceptibility to jamming and eavesdropping, potentially compromising sensitive information. Spoofed cell tower attacks are a primary concern, with attackers using rogue base stations to intercept mobile traffic. In addition, 5G's complex network architecture, which relies heavily on software-defined networking and network functions virtualization, presents new attack surfaces. Without rigorous security protocols, these facets could be exploited, compromising data integrity and privacy.

WiFi

As the cornerstone of wireless communications within both stationary and temporary facilities, WiFi enables high-speed data transmission essential for operational planning and logistics. However, WiFi vulnerabilities, such as the susceptibility to eavesdropping and hacking through unsecured networks, pose significant security risks. WiFi networks also face vulnerabilities related to weak encryption protocols and exploits within WiFi Protected Access.

Bluetooth and Bluetooth Low Energy

Bluetooth and Bluetooth Low Energy (BLE) are multi-layer protocols that enable critical short-range secure communications between personal portable devices and mobile devices in the field. Bluetooth is popular with IoT manufacturers, with more than 5 billion devices shipped in 2024 (shown in Figure 11.1), because it is low-cost and easy to integrate. BLE is particularly suitable for applications that require minimal data throughput, such as monitoring vital signs or monitoring

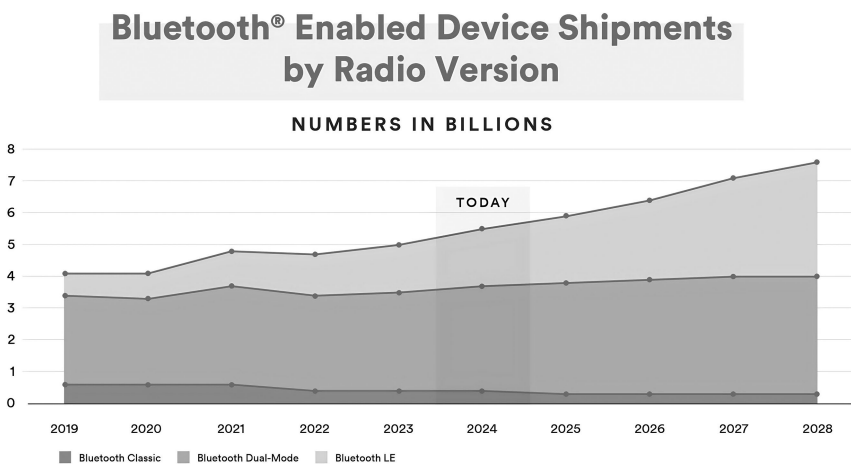


Figure 11.1 Total Bluetooth shipments by radio version (SIG, 2024).

supply chain assets. However, the complexity of the protocol and its closed-source nature make it vulnerable to security flaws.

Bluetooth Vulnerabilities

In 2022, the Bluetooth 5.2 specification approved new BLE audio profiles, namely the Common Audio Profile and the Basic Audio Profile. These profiles open up new possibilities for audio streaming over BLE. However, their deployment is still limited due to the lack of support from many operating systems and hardware. BLE Audio is designed to meet the requirements of low power consumption while offering the high performance required for audio streaming. BLE Audio has the potential to become widely deployed in the next five years, but currently, wireless audio data are mainly sent via Bluetooth Classic, even on devices that support BLE connectivity.

The Bluetooth signal is frequently marketed as a short-range transmission with an effective range of approximately 10 m. However, the use of advanced signal boosters and antennas, along with the potential for sophisticated hacking techniques, can significantly extend the range at which devices can be accessed. Security vulnerabilities in certain Bluetooth headsets and hands-free car kits have enabled malicious actors to exploit these devices as mobile bugging tools, allowing them to covertly monitor conversations. Key weaknesses include vulnerability to man-in-the-middle attacks and device tracking, which can lead to unauthorized access and data leakage. The types of Bluetooth vulnerability are classified as follows:

- **BlueJacking**: sending unsolicited “advertising” messages that look like they’re from a trusted source to get personal information or get people to do something.
- **BlueSnarfing, BlueBugging**: unauthorized device connection to steal data or to spy on the target’s activity.
- **BlueSmacking**: sending more information to the device than it can handle making the device nonoperational.
- **Malware on a Bluetooth device**: malware distribution mechanism.
- **Fuzzing**: looking for 0-day BlueSnarfing and denial-of-service (DoS) vulnerabilities by means of automatic testing the device with random or semi-random test data (the fuzz) in order to test a protocol for unexpected behavior that typically trigger device crashes, memory leaks, and other anomalies.
- **Car Whisperer**: automotive Bluetooth vulnerabilities.
- **DoS**: battery drain, connection interruption, and termination.
- **Pairing Eavesdropping**: key collection during pairing.
- **Secure Simple Pairing**: spoofing an already paired device.

Bluetooth Firmware Security Challenges and Fuzz Testing Limitations

As Bluetooth technology evolves, new versions are constantly being developed to accommodate increasingly sophisticated devices. However, with this evolution also

comes the possibility of previously undisclosed vulnerabilities that could potentially compromise the security of users, their devices, and their data. Bluetooth devices that support legacy peripherals are burdened with high interoperability baggage (protocol-level firmware vulnerabilities). These Bluetooth vulnerabilities allow attackers to trick a device into connecting to a malicious entity, facilitating data theft or malware distribution. In addition, the inherent broadcast nature of Bluetooth signals opens the door to unsolicited location tracking and traffic analysis, despite encrypted communications. The proprietary nature of the various implementations of the Bluetooth protocol contributes to the vulnerabilities of the technology because the implementation and testing do not adhere to established Bluetooth standards and software testing best practices.

Current quality assurance and certification do not adequately and uniformly check for malicious data processing on devices. Hardware manufacturers push to release the latest hardware as quickly and cheaply as possible, and only the largest companies have the financial means to thoroughly test their Bluetooth chips, firmware, and drivers. The security risks associated with Bluetooth can be attributed to implementation errors and configuration issues that lead to vulnerabilities in the firmware and drivers that allow bypassing the security of the entire device operation. It is estimated that over 70% of all vulnerabilities are the result of programming errors, including buffer overflows, incorrect memory management, and inadequately implemented protocol specifications. Bluetooth vulnerabilities registered on the CVE list have grown sixfold since 2016, highlighting the need for systematic security tests. To make matters worse, the very nature of Bluetooth technology makes it difficult or impossible to distribute updates.

The Bluetooth protocol is structured into layers, each layer fulfilling a specific role. The radio layer is responsible for managing access to the physical wireless channel and controlling its operation. The Baseband layer oversees the physical channel, while the Link Manager Protocol handles link coordination and management. The Host Controller Interface provides a standardized interface between the operating system driver software and the hardware software, while the Logical Link Control and Adaptation Protocol allows multiplexing of different logical transmission channels.

Fuzz testing is a methodology that can be used to aid in such tasks, but Bluetooth protocol multi-stage states do not allow immediate testing of all possible paths. To get to the lowest layer of firmware testing, planning is required to adhere to the specific protocol implementation workings on a particular device. In addition, completely invalid data may not be accepted for processing by a high-quality firmware. This depends on the manufacturer's input and quality requirements.

Fuzz testing techniques may be classified according to three main approaches:

- 1 **The generative approach** generates data from scratch in accordance with a specified set of criteria (specifications and documentation). It also uses modeling of protocol behavior and system state transitions, or a formalized Bluetooth message syntax grammar. This approach is designed to identify an unexpected and valid input.

- 2 **The mutational approach**, in contrast, generates data by modifying existing known valid data, making changes at the bit level, and changing the values of certain fields. This approach is intended to identify borderline cases.
- 3 **The hybrid approach** combines the generative and mutational approaches. It uses coverage information to guide the generation of test data targeted at untested phases and uses AI to analyze test results and optimize the generation of test data.

The primary methods for conducting the tests are as follows:

- 1 **Coverage-driven execution** allows for dynamic adjustment of test procedures to ensure complete coverage of all components.
- 2 **Concrete execution** utilizes actual and concrete input data values.
- 3 **Symbolic execution** is a method of analyzing the execution of a program by using symbolic variable values to explore all possible execution paths simultaneously.
- 4 **Concolic execution** is a method that combines symbolic and concrete execution to identify problematic input data paths in a more efficient manner.

Notable fuzzing tools for Bluetooth include *L2Fuzz* (Park et al., 2022), *BrakTooth* (Garbelini et al., 2022), *ToothPicker*, and *Frankenstein*. Each tool targets different layers of the Bluetooth stack and has exposed various vulnerabilities. However, the tools are not immediately usable without specific hardware configuration and software adaptation. During the course of the Latvian cybersecurity project “WearSec” (funded by the Latvian Council of Science, project “Automated wireless security analysis for wearable devices”), a few notable scripts have been created as a way to automate the usage of the aforementioned fuzzing frameworks. The primary issues that were not dependent on the tools or hardware used were identified by fuzzing the Bluetooth protocol implementation in the embedded firmware of various wearables. These included the limited resources of the embedded devices, the divergence in the implementation of the Bluetooth protocol by various manufacturers, and the necessity for high-quality input data. The future of Bluetooth protocol fuzz testing will see the development of hybrid fuzzing, resource-aware fuzzing, and the use of machine learning techniques that will enhance the efficiency and automation of the fuzzing process, thereby streamlining and optimizing the process for greater efficiency and accuracy.

Securing the Bluetooth Environment

The use of an inexpensive ESP32 controller (e.g. ESP32-Cheap-Yellow-Display (Lough, 2024)) in conjunction with various specialized tools, for example, the *ESP32 Marauder* software (JustCallMeKokoLLC, 2024) allows practitioners to exploit a range of Bluetooth vulnerabilities and engage in a variety of offensive and defensive operations on WiFi and Bluetooth devices. This combination provides a compact, portable platform for penetration testing and security analysis, including

the ability to perform Bluetooth sniffing to reveal information about devices communicating, Bluetooth de-authentication to disrupt Bluetooth connections between devices, forcing them to reconnect or fail to communicate, and Bluetooth spamming by sending numerous spam messages or spoofed requests, flooding a Bluetooth device or network, and potentially causing DoS conditions. The portability of the *ESP32 Marauder* makes it an optimal choice for on-site security assessments, as it allows the identification and mitigation of potential threats in real-world settings. Network administrators may utilize the *ESP32 Marauder* to audit their networks for vulnerabilities, thus ensuring the security of their Bluetooth infrastructure through the use of readily available, off-the-shelf hardware and software solutions.

It is evident that the conventional recommendations to improve the gadgets remain relevant. Over the years, a multitude of iterations of the Bluetooth protocol have emerged, spanning from version 1.0 to version 5.4. Each iteration of the Bluetooth protocol is accompanied by its distinctive security vulnerabilities, which can be exploited by adept cybercriminals. Therefore, it is advisable to decommission devices that are older than four years, as they are likely operating on antiquated Bluetooth versions, and replace them with contemporary devices that utilize Bluetooth 5.

In addition, the recommendation to change the default PIN codes (if possible) is still a good one. These PINs are (almost) always “0000” or “1234”, which opens a wide door to attack. If it is not possible to change the default PINs to something harder to guess, then the safest way to protect against Bluetooth exploitation is to keep it turned off when not in use.

Zigbee

Zigbee provides mesh networking capabilities essential for building resilient, self-healing communications networks in the fluid environment of the battlefield, and is particularly suited for low-power sensor networks and IoT applications in military contexts. Zigbee’s security vulnerabilities stem primarily from poor implementation practices. Their vulnerabilities include the potential for attacks on physical devices (Zigbee networks are vulnerable to jamming) and network infiltration, compromising the integrity of sensitive operational data (secret key sniffing compromising).

LoRaWAN

LoRaWAN, also known as LoRa, is an open standard for low-power wide area networks. This technology can transfer data over 10 km long distances with very little power. LoRa is a great way to connect IoT devices and sensors. LoRa devices are small and suitable for prototyping and production systems. However, there are also vulnerabilities to consider. If LoRa authentication and encryption are not done correctly, devices and networks can still be compromised. Some of the reported LoRa vulnerabilities include fixed or easy-to-guess encryption keys, e.g. $\text{AppKey} = \text{device identifier} + \text{app identifier}$ or $\text{AppKey} = \text{app identifier} + \text{device identifier}$. LoRa devices are susceptible to DoS, ACK spoofing, and replay attacks (Bravo, 2021).

Sigfox

Sigfox protocol is used to send up to 140 small messages a day (12 bytes for the uplink and 8 bytes for the downlink). This protocol is useful for transferring data from sensors over long distances at a low cost. Sigfox networks are vulnerable to communication data leaks (data may be sent unencrypted) when bandwidth is low, and communication is susceptible to availability attacks through signal jamming.

Security Considerations

The aforementioned protocols raise several security concerns. However, most of these vulnerabilities can be attributed to shortcomings in their implementation. Generally, there are a few key considerations regarding the overall security of a device (Bravo, 2021):

- Prior to purchasing, it is advisable to conduct research into the device, as it may have inadequate security measures or be using an outdated protocol version.
- Consider the features of the device to ensure that the chosen option optimally meets your specific needs.
- To avoid potential security issues, it is recommended that an expert implement the selected features.
- Be cautious of low-cost devices and sensors, as they may lack essential security features.
- Ensure that the CPS network is kept separate from the main infrastructure to enhance security.

There is no universal solution that fits all scenarios. Each technology has its own set of advantages and disadvantages, which must be carefully evaluated to determine the best fit for a particular situation. Assessing available cybersecurity solutions should be a fundamental part of a comprehensive strategy. In addition, it is crucial to identify the connectivity technology that offers the highest reliability and minimizes the risk of packet loss or disconnection.

Situation in Latvia***Mapping the Cyber-Physical Landscape using Shodan***

The Shodan tool helps security professionals and ethical hackers identify vulnerabilities and improve network security for companies. Shodan identifies Internet-connected devices and services such as webcams, routers, servers, industrial control systems (ICS), infrastructure components, and other IoT and CPS devices that exchange data and provide control capabilities.

It is common for device interfaces, including smart fridges, medical devices, security cameras, and traffic control systems, to lack essential security measures. These include replacing easily guessed or default passwords and implementing robust network connection encryption. Inadequate security protocols can result in the inadvertent disclosure of sensitive information, which could lead to concerns

about privacy and security. Although Shodan may pose cybersecurity risks to careless device users, it also provides a valuable means of inspection for manufacturers, developers, and consumers to prevent unauthorized access and data breaches. Implementing robust password policies, regular software updates, and encryption methods, along with proactive monitoring to identify vulnerabilities before malicious actors do, can significantly improve cyber security posture and ensure that products and services remain secure.

The Shodan security scanning tool is capable of reviewing an extensive array of statistical data points pertaining to CPSs deployed in Latvia, encompassing various IoT and ICS interfaces. Within the “Explore” section of Shodan (n.d.-a; n.d.-b) for IoT and ICS, users can acquire a thorough understanding of the diverse and specific device data available.

To refine search results to encompass devices within a designated country, one may incorporate the “Country:LV” parameter into the search query. This action restricts the results, which can subsequently be further delimited by specifying the relevant IP address range.

To collect data on CPSs, researchers may deploy a variety of keywords available at no cost or opt for an enterprise upgrade to utilize the “tag” parameter. Should “tag” queries be inaccessible, alternative search methodologies can be implemented based on open ports and particular keywords.

The following enumerations exemplify this concept:

- `country:LV "IoT"`
 - Identify and retrieve devices available within Latvia that explicitly reference IoT functionalities in their descriptive profiles. This encompasses but is not limited to, MikroTik routers, Hikvision surveillance cameras, and Xiaomi IoT-enabled devices.
- `country:LV port:502`
 - Modbus is a widely utilized communication protocol within numerous ICS, serving as a standardized interface for the efficient exchange of data.
- `country:LV port:21 "220" "230 Login successful."`
 - Identifies Latvian electronic devices equipped with unsecured FTP access, encompassing unprotected Network-Attached Storage (NAS) systems, routers, and surveillance cameras.
- `country:LV port:23`
 - Network devices endowed with Telnet accessibility (inclusive of routers, gateways, NAS units, and assorted network infrastructure equipment).

Predominant Latvian CPS Systems

In Figure 11.2, the predominant IoT and ICS products within the Latvian Internet landscape, as cataloged by Shodan, are illustrated. The data reveal a substantial prevalence of devices from prominent manufacturers including Google (specifically Chromecast), LG, Philips, Sony, Tuya, and Apple (specifically AirPlay), signifying their use within the Latvian context.

Smart Home Systems

Many households in Latvia and similar countries are adopting smart home systems such as Philips Hue or Xiaomi Smart Home. These systems allow users to control lighting, heating, and security cameras through a mobile application, reducing the need for physical switches and control panels. Systems can be vulnerable to hacking if not properly secured, potentially giving unauthorized users access to home functions and private data. If not adequately secured, these systems are susceptible to cyberattacks, possibly granting unauthorized individuals access to integral home functionality and sensitive personal data. As of the preperation of this analysis, a Shodan search using the query “country:LV product:"Philips Hue","Xiaomi Smart Home" port:80,443” uncovers a total of 77 indexed smart home devices cataloged in Latvia that are exposed on the public Internet and may be susceptible to an attack.

Industrial Automation and Programmable Logic Controllers

Factories in Latvia, like those in other European countries, are increasingly using IoT devices for automation. For example, smart sensors and controllers are used to monitor and control machinery through mobile apps. Unauthorized access could disrupt industrial processes or even physically damage machinery, emphasizing the need for robust cybersecurity measures.

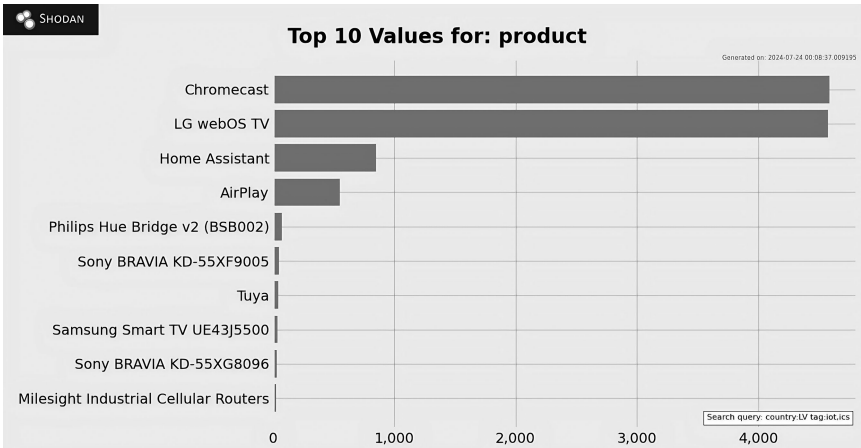


Figure 11.2 Most popular IoT and ICS products in Latvia as indexed by Shodan (2024-07-24).

Shodan search results for Latvia tagged with ICS (illustrated in Figure 11.3) disclose a range of exposed ICS, encompassing those employed in manufacturing, utilities, and building automation. These systems predominantly comprise programmable logic controllers (PLCs), SCADA systems, and other control devices from vendors such as Tridium, Moxa, and 3S-Smart Software Solutions.

A query of “country:LV port:20000,502,102,1911,18245,4911,44818,47808,2404,789,1962,20547,9600,44818,54321” for open ports common with ICS in Latvia returned 2865 instances on Shodan. Ports like 20000 (DNP3 over TCP), 502 (Modbus/TCP), and 102 (Siemens S7) are used for communication in utilities, industrial devices, and PLCs. Ports 1911 (Tridium Niagara Fox) and 4911 (Foxboro FCP280) support building automation, while 18245 (OPC UA TCP) facilitates industrial automation. Ports 44818 (EtherNet/IP), 47808 (BACnet/IP), 54321 (BACnet MS/TP over IP), and 2404 (IEC 60870-5-104) serve various automation needs. Protocol-specific ports like 789 (IEC 60870-6 TASE.2), 1962 (PCWorx), 20547 (ProConOS), and 9600 (OMRON) support device communication in industrial environments. Not all devices are tagged as “ics” in Shodan, but the overall impression of the state of Internet-connected ICS systems is more realistic since not all devices are correctly reported or detected by the information they expose to the Internet.

FTP is one of the most common ICS network protocols, employed by automation solution manufacturers in a multitude of contexts. The fundamental principle of FTP is the transfer of files via an unencrypted channel, which renders the data susceptible to exploitation. Consequently, the process of updating firmware or programmable logic via FTP is often vulnerable to such exploitation. If a file is modified to allow a firmware version to be downgraded to a previously unprotected version, it creates a pathway for previously patched vulnerabilities to be restored in devices (Smith, 2021).

NFS (Network File System) is a dynamic protocol that enables computers in industrial automation, corporate, educational, and data center environments to

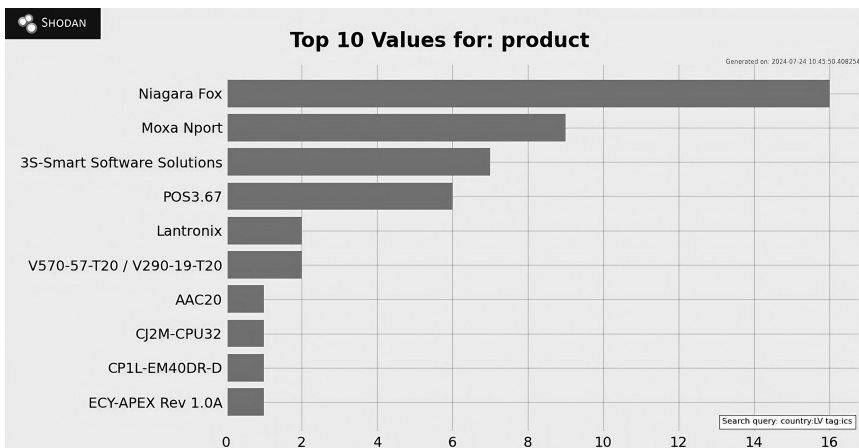


Figure 11.3 Products tagged as ICS by Shodan (2024-07-24).

share files over a network as if they were in the same local storage. While NFS facilitates file sharing, it also introduces several security vulnerabilities, including anonymous authentication, well-documented older version vulnerabilities, and the potential for root access on all devices lacking the “root squashing” security option. NFS servers are not uncommon to be publicly accessible, often with inadequate or absent authentication measures. A simple query on Shodan reveals numerous open NFS resources on the Latvian Internet (“country: LV nfs”). There are a range of industrial systems available, including those for managing cinemas and for automation in data centers and conferences.

Comparable risks are inherent in the deployment of Samba servers for file-sharing applications. The Samba service usually operates on port 445. Executing a Shodan query with the parameters: “country:LV port:445 "Authentication: disabled"” retrieves all instances accessible within Latvia, which can be immediately connected to, thereby facilitating the transfer of data, installation of ransomware, incorporation of persistence mechanisms, among other nefarious activities. At the time of writing, there are 247 identified instances in Latvia susceptible to these vulnerabilities.

Additional inquiries of interest, which are not categorized under “ICS”, disclose the following:

- A query on Shodan for “country:LV hacked-router-help-sos” reveals the existence of compromised network routing equipment. At the time of writing, one such product is identified, namely the Ubiquiti LM2.
- A query on Shodan for “country:LV port:161 SIMATIC” returns two results for potentially exposed Siemens Industrial Automation products.
- A query on Shodan for “country:LV Module:6ES7” returns six results for Siemens Industrial Equipment products.

A comprehensive index of product favorite icon hashes is available on Github (san-satart, 2024). It should be noted that this list may not be exhaustive; however, it provides valuable information about the extent of exposure of various surveillance products to the Internet. By selecting the hashes and applying a country-specific filter for Latvia, we can derive the following data, as illustrated in Figure 11.4.

This query returns 12,925 devices, of which the most notable are products such as Hikvision IP Camera, Ubiquiti AirRouter, Sophos User Portal, various Dahua video cameras, Fortinet FortiGate firewall products, and SonicWall firewall products. Hikvision is a company that is owned by the Chinese government. Similarly to Huawei, both Hikvision and Dahua have been banned from the United States. Nonetheless, their subsidiaries persistently operate across numerous regions in Latvia and other global locations.

It would not be an exaggeration to suggest that home security cameras present a significant privacy challenge. It is not uncommon to find that most of the systems on the market are rebranded or originate from China. It also appears that many companies are encouraging customers to connect their cameras to WiFi, despite the fact that the user interface and code base in question are underdeveloped and shipped with vulnerabilities such as RCE (e.g., CVE-2021-36260 (NIST, 2021)).



Figure 11.4 Common internet-connected devices in Latvia identified by Shodan via favicon hashes (2024-07-24).

Healthcare Devices

Medical devices such as glucose monitors and insulin pumps from brands such as Medtronic are becoming common in Latvian healthcare. These devices can be monitored and controlled through mobile applications, improving patient care and convenience. The compromise of these devices could lead to incorrect dosage administration or unauthorized access to data, which poses significant health risks to patients.

In addition, non-medical health and well-being devices are widely adopted in Latvia, most notably smart watches and sports-related wearables. Direct health risks are much lower with these devices, but privacy-related risks, such as device fingerprinting and tracking, still are a potential concern (Rušīņš et al., 2024).

Public Transportation and Smart Mobility

Riga's public transport system utilizes mobile applications to buy tickets and has started real-time tracking of buses and trams. Systems of Rīgas Satiksme have moved much of their functionality to mobile apps to improve user convenience and operational efficiency. If these mobile applications are compromised, that could lead to disruptions in the public transportation system and unauthorized access to user data.

The road infrastructure in Latvia encompasses a diverse array of roadside monitoring and automation systems, such as speed enforcement radars, average speed enforcement systems, red light cameras, public transport lane enforcement cameras, free parking space monitoring systems, pedestrian and bicycle counters, smart roadside lighting systems, and also some smart traffic lights and traffic signs have appeared in recent years. The biggest threat here is the fact that different city councils and state agencies have been adopting different usually non-compatible systems, sometimes even multiple in parallel at the same time. Thus, it is not transparent what data from roadside sensors goes where, who processes them, and also what potential vulnerabilities might exist in all of these competing solutions. The situation is potentially made worse by the fact that some of the systems are either developed from scratch locally or heavily adopted by local companies, introducing another point where security or privacy issues might arise.

Currently, many of these smart mobility systems in Latvia are either completely standalone systems acquired over many years or integrated in only one of multiple control centers across major Latvian cities, leading to potentially different security and privacy mechanisms for each of them.

Agricultural Automation

Agricultural automation is growing with the use of IoT devices for soil monitoring, irrigation control, and livestock management. Companies like John Deere offer solutions that are controlled via mobile applications. There are also locally developed sensor network solutions usable for agriculture among other fields, such as Aranet by SAF Tehnika JSC which uses a proprietary LoRa based protocol. Vulnerabilities in these systems could result in the loss of crops or livestock, significantly impacting food production and the economy.

Threats to CPS

Mobile Application Threats

A dominant trend in CPSs, industry automation, and consumer IoT devices is to reduce the complexity and cost of physical control by shifting the control of the device to a mobile application linked to the device. This is facilitated by the low cost of embedded wireless controllers compared to the cost of even simple physical controls like switches and dials and means that the device can be controlled remotely, which has both convenience advantages and increased security risks.

These applications represent a potential target for exploitation, as the designed architecture explicitly provides them with the ability to control these connected devices and vehicles. According to the OWASP Mobile Security Project, a global non-profit organization focused on improving software security, the ten most critical mobile controls for the final list of 2024 are as follows (OWASP, 2024):

- **M1: Improper Credential Usage.** This refers to the practice of using credentials such as usernames and passwords in an insecure manner. Examples of such insecure practices include hardcoding credentials in the code, storing them in an improper manner, or failing to employ robust encryption techniques. Such practices make credentials susceptible to theft by malicious actors, thereby facilitating unauthorized access.
- **M2: Inadequate Supply Chain Security.** This refers to the vulnerabilities that arise from the incorporation of third-party components and libraries into an application. If these components are not subjected to adequate vetting and update procedures, they can potentially introduce security risks into the application, increasing the likelihood of exploitation by malicious actors.
- **M3: Insecure Authentication/Authorization.** This refers to the process of ensuring that only authorized users can access specific sections of an application. Insecure methodologies, such as inadequate password policies or flawed authentication mechanisms, can allow malicious actors to circumvent login systems and gain unauthorized access to sensitive data.
- **M4: Insufficient Input/Output Validation.** When applications do not properly check the data that users input or output, it can lead to security vulnerabilities such as SQL injection or cross-site scripting. This means that attackers can manipulate these inputs to execute malicious code or access restricted data.
- **M5: Insecure Communication.** This involves the use of unencrypted or improperly encrypted communications between an application and its server. Without proper encryption, attackers can intercept and read the data being transmitted, potentially stealing sensitive information such as personal data or financial details.
- **M6: Inadequate Privacy Controls.** This covers how well an app protects users' personal information. Inadequate privacy controls may result in the inadvertent exposure or sharing of sensitive data without the requisite consent, thereby placing users' privacy at risk.

- **M7: Insufficient Binary Protections.** Binary protections refer to the process of securing the actual code compiled in an application, with the aim of preventing reverse engineering or tampering. Insufficient protections may allow attackers to decompile the application, comprehend its internal logic, and identify vulnerabilities for exploitation.
- **M8: Security Misconfiguration.** This happens when security settings are not properly configured, leaving an application vulnerable. Such issues may include the use of default passwords, misconfigured security headers, or improperly set permissions.
- **M9: Insecure Data Storage.** This refers to the manner in which data is stored within an application. In the event that sensitive data is stored without the implementation of appropriate encryption or protection measures, it can be readily accessed by malicious actors who gain physical access to the device or exploit other vulnerabilities. Rooting or jailbreaking a mobile device bypasses any encryption protection, and all that is needed to view the data is a specialized set of tools.
- **M10: Insufficient Cryptography.** Cryptography is used to protect data, but if it is implemented poorly or uses outdated methods, it can be ineffective. Insufficient cryptography means that even if data appears to be encrypted, it can still be vulnerable to decryption and theft by attackers.

In addition to the aforementioned controls, the list of OWASP top ten mobile controls identifies several other potential vulnerabilities in mobile security systems. These include data leakage, hardcoded secrets, insecure access control, path overwrite and path traversal, unprotected endpoints, and unsafe sharing.

Data leakage can be defined as the unintentional exposure of sensitive information, which may occur through the use of memory dumps or improper logging practices. It is essential that developers ensure the prompt removal of sensitive data from memory once they are no longer required and guarantee the secure storage of such data. The implementation of appropriate memory management techniques, such as the overwriting of sensitive data with random data prior to its deletion, helps mitigate these risks. Hardcoding secrets such as API keys or passwords directly into the source code is a critical security flaw. It makes it easy for attackers to extract these secrets through reverse engineering or simply examining the code. Instead, secrets should be stored securely, such as in environment variables or in secure storage mechanisms provided by the platform.

Insecure access control refers to a situation in which an application does not effectively regulate who is allowed to access specific data and functionalities. Such deficiencies can result in unauthorized users gaining access to sensitive information or functionality. It is of great importance to ensure that robust authentication and authorization mechanisms are in place to prevent such events. Path overwrite and path traversal vulnerabilities occur when an attacker can manipulate file paths to gain unauthorized access to files outside the intended directory. This can lead to exposure of sensitive files or even system files. Proper validation and sanitization of file paths are essential to mitigate these risks.

An unprotected endpoint is defined as a network interface that lacks the necessary security measures to prevent unauthorized access or data interception. The use of HTTPS to encrypt data in transit and the implementation of endpoint authentication protocols can serve to mitigate the aforementioned vulnerabilities. Unsafe sharing involves exposing sensitive data through shared resources such as clipboard, logs, or shared storage. Developers should minimize the use of shared resources for sensitive data and implement proper data handling practices to ensure that sensitive information is not exposed involuntarily.

A novel form of M2 control's attack targeting mobile applications is the overlay attack. Previously a prevalent form of cybercrime in conventional internet browsers, it has now been found to target sensitive user data in mobile applications as well (Software, 2024; Verimatrix, 2024). The attack has been adapted to mobile devices, making it more difficult to detect. These attacks are typically conducted via applications distributed to users on fraudulent distribution networks with covert functionality, which reside in the background and monitor for the launch of a targeted selection of applications. Overlay attacks are particularly effective against Android devices due to the permissions model that allows apps to draw over other apps. During the attack, the malicious process creates a user interface on top of the legitimate application and harvests user input. These applications are particularly insidious in that they can emulate the behavior of the original application by introducing an intermediate layer that collects sensitive information for malicious actors. The sole means of protection against these applications is to utilize official distribution networks and to compare the application's file hashes with those of the original developer.

A particularly concerning aspect of M8 control is the prevalence of products that have been shipped with Android Debug Bridge (ADB) enabled or rooted for various reasons by owners of these devices, leaving them susceptible to attacks. ADB listens on port 5555, enabling a connection over the Internet to the device (Polop, 2024). A Shodan search query "country:LV "Android Debug Bridge" "Device" port:5555" returns 60 Android devices that are listening on this port at the time of writing, including TV boxes and Android smartphones. These open devices can be exploited by malicious actors for activities such as cryptocurrency mining or malware dissemination without the owners' permission.

OWASP has developed and regularly updates the Mobile Application Security Vulnerability Standard (MASVS), which defines the basic requirements for mobile application security testing scenarios, and the Mobile Security Testing Guide (MSTG), which details the technical processes and tools of the MASVS. These standards help ensure that mobile applications are secure and resilient against various types of threats.

Typical Threat Models for Mobile Apps

It is crucial for businesses to understand the risks associated with mobile applications and implement effective security measures. This requires a clear understanding of the threats and corresponding solutions, as well as regular updates and adherence to standards such as OWASP MASVS and MSTG. The mobile threat

model (Figure 11.5) illustrates the potential vulnerabilities, threats, and attack vectors associated with mobile applications and the mobile environment.

- A. Potential risks to the supply chain, including phishing.
 - Example: Attackers send malicious emails to developers or supply chain partners to gain unauthorized access to development environments.
 - Solution: Implement stringent supply chain security measures, including email filtering and awareness training.
- B. Unauthorized disclosure of data from the test environment or infrastructure.
 - Example: Test data containing personal information being exposed due to inadequate security measures.
 - Solution: Ensure that all test data are anonymized and protected with robust access controls.
- C. Cyberattacks on users of compromised devices.
 - Example: Malware installed on a user's device leads to unauthorized access to the mobile application.
 - Solution: Implementing security measures such as device integrity checks and user awareness training.
- D: Developer-created threats, including smear campaigns.
 - Example: A disgruntled developer inserting malicious code into the application.
 - Solution: Conduct regular code reviews and employ stringent access controls in development environments.
- E: The leakage of sensitive data and the alteration of data.
 - Example: Sensitive information being exposed through improper data storage practices.
 - Solution: Encrypting sensitive data and implementing secure data storage mechanisms.
- F: The alteration of the logic of the app and the unlawful collection of data from devices.
 - Example: Attackers modify the behavior of the app to collect additional data without the consent of the user.
 - Solution: Using code obfuscation and integrity checks to prevent unauthorized modifications.
- G: The interception, modification, and compromise of third-party libraries.
 - Example: A malicious library being included in the app, leading to data leakage.

- Solution: Verify the integrity of third-party libraries and use only trusted sources.
- H: The takeover of infrastructure and the compromise of privileged users, including the use of phishing.
 - Example: Attackers gaining control of the back-end infrastructure via phishing attacks targeting administrators.
 - Solution: Implementing multi-factor authentication and continuous monitoring of privileged accounts.
- I: API interception and leakage of data and compromise of data integrity from API vulnerabilities.
 - Example: An attacker intercepting API calls to exfiltrate sensitive data.
 - Solution: Securing APIs with proper authentication, authorization, and encryption mechanisms.

Wireless Communication Threats

A study of 2023 CVE reports of wireless vulnerabilities (Paikens & Nesenbergs, 2024) demonstrated that proper security review appears to be limited only to a few major platforms which have the resources and motivation to perform a thorough security analysis, while the observed weaknesses for most manufacturers of IoT and CPS systems are “low hanging fruit” of simple weaknesses findable and exploitable by unsophisticated means, indicating that currently the bottleneck for exploiting such systems is mostly in the motivation of attackers to do so.

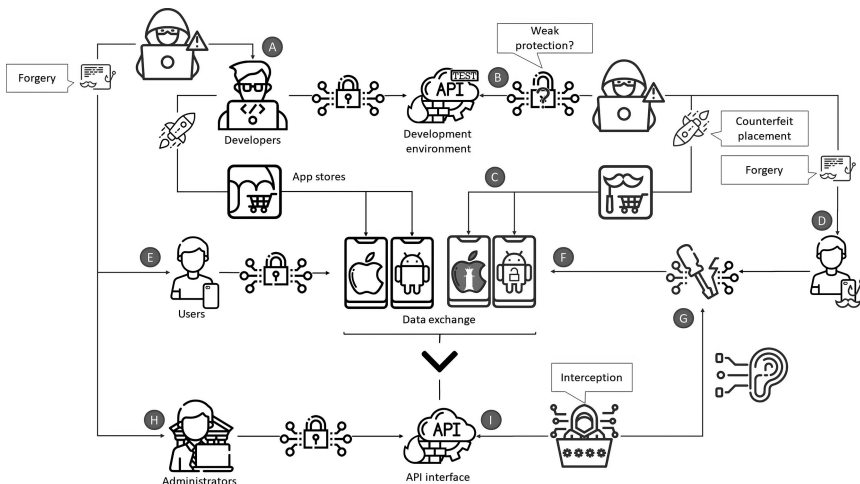


Figure 11.5 Potential mobile vulnerabilities, threats, and attack vectors. Figure by the authors.

The vast majority of the vulnerabilities reported in that study are caused by memory safety issues inherent to common practices of C/C++ usage.

Smart Grid and Industrial Threats

The electrical grid is the primary source of energy for numerous domestic, educational, and urban infrastructure applications. The grid includes both power plants that generate electricity and a complex system of transmission lines that deliver electricity to consumers. As the quantity of smart devices in residential and commercial settings rises, it becomes increasingly necessary to integrate these devices with the grid to satisfy consumer requirements. However, this also presents a potential risk: malicious actors could gain control of these devices and disrupt the power grid. For example, they could initiate a large-scale shutdown or restart of many devices simultaneously.

Hackers could control multiple IoT devices, such as smart thermostats, that are distributed in multiple locations. By modifying the total power consumption of these devices in a coordinated manner, hackers could cause disruptions in the operation of the power grid. The impact of such an attack could be major, possibly causing grid overloads and subsequent power loss in certain areas of the grid. Such actions could result in power outages, increased electricity costs, or even damage to the grid infrastructure.

A 2017 study (Dvorkin & Garg, 2017) identified two different attack strategies:

- **Naive attack strategy:** In this approach, the hacker does not take into account existing defenses. Such an attack is less effective because some security systems are designed to prevent significant damage.
- **Insidious attack strategy:** In this approach, the hacker is aware of the network's defenses and bypasses them. This type of attack is more dangerous because it has the potential to bypass security mechanisms and cause greater damage.

The researchers developed a model to simulate these attacks and analyze their impact. They found that as the number of connected and controlled IoT devices increases, so does the potential for significant damage and disruption to the grid. The study used actual grid data to show how these attacks can spread from smaller local grids (distribution grids) to larger regional grids (transmission grids).

This indicates that the proliferation of IoT devices poses a real risk to the electric grid. It underscores the need for enhanced security protocols to protect against such distributed cyberattacks. The study shows that both naive and insidious attacks can cause significant disruption, with insidious attacks being more damaging due to their ability to bypass existing protection systems.

Existing Threat Classification

Existing threats can be broadly classified as endpoint vulnerabilities, supply chain risks, and network-based attacks.

Endpoint Vulnerabilities

CPS endpoints, such as sensors, actuators, and controllers, are typically the primary targets of attacks due to their physical accessibility and resource constraints. As suggested by Omitola and Wills (2018), IoT endpoints can be classified into three categories: simple, medium-sized, and gateway endpoints. Each of these categories presents a distinct set of security challenges (Omitola & Wills, 2018). Simple endpoints, such as sensors, have limited security features, making them susceptible to tampering and spoofing attacks. Medium-sized endpoints, including devices such as smart household appliances, face risks from persistent connections to backend servers. Finally, gateways, which manage communication between endpoints and backend systems, are vulnerable to complex attacks due to their critical role in the network.

Supply Chain Risks

The sophisticated nature of the CPS supply chain presents a range of significant security challenges. The supply chain includes numerous stakeholders, such as component suppliers, manufacturers, and distributors, all of whom have the potential to contribute to the introduction of vulnerabilities. Omitola and Wills (2018) emphasize that the global nature of supply chains, such as that of the iPhone, expands the attack surface and complicates security management (Omitola & Wills, 2018). Malicious actors pose a significant risk to the integrity of the supply chain by exploiting vulnerabilities in a number of ways, including the insertion of counterfeit components, the introduction of malware during manufacturing processes, and the hijacking (or “compromising” in the technical lexicon) during the distribution of software updates.

Network-Based Attacks

The operation of communication networks plays a pivotal role in the exchange of data and the control of processes within CPS. Network-based attacks, including DDoS, man-in-the-middle (MitM), and eavesdropping, present a considerable threat to the integrity and availability of CPS. Such attacks have the potential to disrupt the normal operation of CPS, resulting in safety hazards and financial losses. It is of critical importance to guarantee the robustness of network security in order to maintain the reliability and resilience that are essential for the continued functioning of CPS.

Future Threats

As CPS technology continues to evolve, the emergence of novel threats is an inevitability, precipitated by advancements in technological innovation and the development of new attack tactics. Therefore, it is necessary to predict these future threats in order to develop effective and proactive security measures.

Advanced Persistent Threats

APTs are sophisticated, targeted attacks that aim to gain prolonged access to CPS networks. These threats present a significant risk to critical infrastructure and high-value targets within CPS.

AI-Driven Attacks

The integration of AI in CPS introduces novel attack vectors. AI-driven attacks leverage machine learning algorithms, resulting in sophisticated attacks that evade detection. AI has the ability to automate and enhance traditional attack methods (Fang et al., 2024), making them more effective and challenging to identify.

Quantum Computing Threats

The advent of quantum computing has the potential to render current cryptographic algorithms insecure, which poses a significant threat to the security of CPS. As quantum computing technology continues to evolve, it is imperative to develop quantum-resistant cryptographic methods to safeguard CPS against future quantum-based attacks.

Future Threats in Latvia: Potential Impact and Mitigation

Although general categories of future threats are quite universal, some more specific CPS/IoT-related problems and threats are identified in Latvia specifically, for some of which attempts have been made to develop mitigations or at least investigate the impacts and potential solutions. In this section, we will list some of the most recent and ongoing related work in the Latvian context.

Security of Smart Wearables

One of the categories of CPS systems with the highest potential privacy risks is smart wearable systems which are becoming more prevalent in the daily life of society, ranging from smartwatches, and fitness bracelets to accessories and head-phones (Blumbers et al., 2022). A key consideration is the fact that wearable devices can gather and transmit sensitive information about the wearer and usually have very limited amount of power thus limiting the complexity of potential solutions. Globally there has been relatively little research on the security of these devices, thus a gap has been identified, where multiple local research groups have initiated research activities.

In order to explore these potential dangers, several Latvian research institutions explored innovative security analysis and automated vulnerability assessment of wearable devices in the research project “Automated wireless security analysis of wearable devices” (WearSec).¹ As a result of this project, a dataset of the most popular wearable device wireless communications was developed and published (Rusins et al., 2024). This dataset includes SDR recordings of communications by

these wearable devices and is meant to be extendable by interested third parties in order to develop and validate different security testing methods, that can later be used to check if any specific wearable device might be vulnerable to some attack vectors. This project also found that the wireless communications of these wearable devices can be used not only to identify the specific model of the device but also a specific device through fingerprinting, allowing attackers to track the user and their habits (Rušņš et al., 2024).

Numerous efforts in Latvia have focused on creating novel solutions for wearable device communication aimed at reducing security and privacy risks.

One ongoing research direction in Latvia is related to wired wearables – clothing with an integrated wired CPS network is not exposed to wireless-related attacks and vulnerabilities, as well as fingerprinting-based tracking, but have disadvantages in usability, such as fragile wiring or water damage due to washing of the smart clothing with integrated wires. Several Latvian research projects have attempted to solve this problem, with two of the latest being “Smart Materials, Photonics, Technologies, and Engineering Ecosystem” (MOTE)² and “Sensorial Clothes for Accurate Physical Exercise and Instant Feedback” (SCAPE-IF),³ the latter of which has also resulted in successful commercialization of washable smart wear with integrated elastic wiring. This solution allows for a network of wired sensors and actuators to be embedded in smart clothing, but unfortunately, this means that each individual sensor or actuator node must be connected to this clothing item.

A different research direction in Latvia is directed toward solving this problem by introducing a completely new type of communication – Body-Coupled Communication (Ormanis & Nesenbergs, 2018). This method allows wearable devices to use the human body as a medium for communication without radiating a wireless communication signature outside the body. Thus, communications in such a wearable CPS can only be intercepted by physical touch of the user’s body, which can be easier to detect than remote wireless monitoring and is also much more prohibitive for successful attacks on this communication channel. Some security-related developments based on this research are unique signature of a person as a communication system, that can be used to authenticate a person of a wearable device or implanted electronics, both for individual use or in a real-life handshake, where two people can exchange secret information through touch without the risk of surveillance. This technology can also be used to authenticate people for physical access instead of existing RFID systems which can be attacked remotely. This technology has been further developed (Ormanis & Elsts, 2020) in Latvia in projects such as “Body-Coupled Communication for Body Area Networks” (BCC)⁴ and “Sustainable and green electronics for circular economy” (Sustronics).⁵

Improved Wireless Protocol Development

The potential insecurities of wireless CPS communications can be partially addressed by the use of appropriate communication protocols. As each existing wireless communication protocol has some potential problems related to security and availability (as some of them are proprietary), there has been a push to develop

the next generation of wireless communication protocols. In Latvia, specifically, there have been two main drivers toward this: public research initiatives and private business interests.

Mentionable public research results in Latvia are related to new wireless protocols for embedded CPS systems (Bae et al., 2022), and WSN/CPS/IoT TestBed environment which allows close to real-life testing of such devices in order to develop them to be safer, more energy-efficient and appropriate for the specific use case (Judvaitis et al., 2023). There is also research related to protocols and methods for data transfer in the previously mentioned Body-Coupled Communication (Ormanis et al., 2023).

From the related private business developments in Latvia, the most notable is Aranet (<https://pro.aranet.com/library>) by SAF Tehnika JSC. This is a proprietary protocol based on LoRA and used for many different types of CPS systems for applications such as smart home, smart farming, and customer tracking. One of the most popular products of this company is Aranet4 CO₂ sensor which was popularized during the pandemic as a useful indicator of potentially dangerous non-ventilated areas. Even though the details of the proprietary protocol are not revealed to the public, it can be inferred that one of the motivators for the development of such proprietary protocol is to protect their CPS devices from known attacks on other existing wireless protocols, although the price for licensing similar protocols such as LoRA might also be a key factor.

Quantum Research

Historically, Latvia has been an epicenter of quantum-related research. Recently, quantum-related technologies have been central to the security discussion, both from the threat perspective (undermining conventional cryptography) and from the solution perspective (quantum-safe encryption, quantum key exchange, etc.). There have been several important quantum-related research projects related to security. In 2019 Latvia joined forces with Switzerland, the United States, China, and South Korea to co-found company ID Quantique, which provides Quantum Key Distribution (QKD) services thus protecting the devices involved in the communication from key tampering. Quantum computing and quantum optimization (Abbas et al., 2023) have been researched in the University of Latvia for more than 20 years, yielding theoretical results, with practical applications, that have allowed researchers to become part of multiple international quantum initiatives, such as the Quantum Community Network and National Quantum Initiatives.

In addition to quantum algorithms, software, and communication security, a research direction related to quantum sensors and devices is directly connected to CPS. One example of such research in Latvia is project “Development of Optical Frequency Comb Generator Based on Whispering Gallery Mod Micro-Resonator and Its Applications in Telecommunications”⁶ where micro-resonators are developed with uses in high precision sensors. Finally, Latvia is currently implementing an EU-funded project “Development of experimental quantum communication infrastructure in Latvia”⁷ the goal of which is to build QKD infrastructure in order to improve cybersecurity and reliability in Latvia and Europe.

Automated and Self-Driving

One of the promises of CPS is automated and self-driving. Due to the fact that such applications are of potentially high risk, they require stringent security solutions. Various automated and self-driving projects have been developed in Latvia, which have led to the development of the 5G Test Environment for Connected and Driverless Cars at Bīķernieki Track in Riga, Latvia, where researchers, Latvijas Mobilais Telefons (LMT) (an innovation technology company), and the Road Traffic Safety Directorate (CSDD) of Latvia have collaborated to establish a safe testing location, as well as participation of Latvian team in The Grand Cooperative Driving Challenge (GCDC), a cooperative and automated driving competition among various European universities and research centers.

Some of the problems that Latvian researchers are trying to solve include fail-safe communication between autonomous vehicles and smart infrastructure, as well as better automated perception and task planning. Recent CPS security-related projects in this field which are implemented in Latvia include “Integrated Components for Complexity Control in Affordable Electrified Cars” (3Ccar),⁸ “Automotive Intelligence for/at Connected Shared Mobility” (AI4CSM),⁹ and “5th Generation connected and automated mobility cross-border EU trials” (5G-Routes).¹⁰ Additionally, Latvian researchers are partnering with European institutions in order to develop Electronic Components and Systems for European Automotive applications thus securing the automotive industry from potential supply-chain risks.¹¹

Smart Traffic Monitoring Solutions

Related to automated driving research, another CPS application that has security implications is smart city/smart traffic monitoring. The benefits of such systems must be balanced with the amount of data gathered by them in order to minimize the unneeded invasion of privacy. Latvian researchers together with company “Dots”. have developed a unified smart traffic monitoring and control back-office system Fits. These systems are deployed in multiple cities in Latvia as well as abroad, ensuring more efficient and privacy-preserving functionality (Skadins et al., 2020).

Radio Signal and Data Security

CPS security is often related to radio signal interception as well as physical compromise of the device. Due to these risks, a research project “Enhanced electromagnetic protection and cybersecurity through field-deployable innovative shielding, monitoring, and data destruction technologies” (EMI-CUBE/EMCField-Shield) has recently developed enhanced radio shielding materials and other CPS data protection methods (Bleija et al., 2023).

Dual use and Military Applications

Due to the physical proximity of Latvia to Russia and the related risks, much effort is invested in research and development in Latvia in dual-use and military

technologies. Specific achievements are not public due to secrecy requirements, but we can mention a published solution, the mobile national defense platform “Viedsargs” with the Internet of Military Things functionality which has been developed by LMT. As part of NATO alliance, Latvia is highly involved in research projects related to security, including CPS/IoT technologies.

Conclusion: Potential Mitigation Strategies

To address both current and prospective threats to CPS, it is advisable to implement a comprehensive array of technical, organizational, and procedural measures. These measures should be continually updated to address new threats and vulnerabilities, thereby maintaining the systems’ resilience and reliability.

Enhanced endpoint security. It is of fundamental importance to implement robust security measures at the endpoint level. This encompasses the use of secure boot mechanisms, hardware-based security modules, and the implementation of regular firmware updates, with the objective of protecting against tampering and malware. Techniques such as fuzzing, similarity detection, and control flow analysis remain effective in uncovering hidden firmware vulnerabilities. However, the diversity in instruction sets and CPU architectures introduces new obstacles that require the creation of proficient reverse engineering tools for mobile apps, PLC binaries, and firmware binaries to decode processing logic (Wang et al., 2021). In addition, the integration of endpoint anomaly detection and response systems can offer ongoing monitoring and quick reaction to threats, thereby improving the overall security stance.

Supply chain security management. To ensure the safety and reliability of the supply chain, it is essential to implement strict procedures for supplier evaluation, enforce secure manufacturing processes, and monitor the integrity of software updates. Technological solutions with the potential to enhance transparency and traceability within the supply chain, such as blockchain, can facilitate early detection and prevention of compromised components. In addition, conducting frequent audits and employing cryptographic verification techniques can enhance the protection of the supply chain from potential threats.

Network security enhancements. The integration of strong network security protocols, such as encryption, intrusion detection systems, and secure communication methods, serves as a robust approach to reducing the likelihood of attacks targeting the network. In addition, implementing a zero-trust security framework, which entails the ongoing validation of all network engagements, can greatly enhance the system’s overall security profile. Using machine learning techniques for anomaly recognition can further strengthen the capacity to detect and counteract advanced network threats.

Notes

- 1 LCS Fundamental and applied research project programme grant No. lzp-2020/1-0395.
- 2 Grant No. VPP-EM-Photonics-2022/1-0001, funded by State Research Programme of Latvia.
- 3 Grant No. KC-PI-2020/42.

- 4 The project is funded by Latvian Councils of Science, Project No: lzp-2020/1-0358.
- 5 Grant No. 101112109.
- 6 Project No. 1.1.1.1/18/A/155.
- 7 LATQN, ID Nr. 101091559.
- 8 Grant agreement no. 662192.
- 9 Grant agreement no. 101007326.
- 10 Grant agreement No. 951867.
- 11 Project “Ensuring European ECS Value Chain Sovereignty through Shaping the Future of ECS for Automotive Applications” (ShapeFuture). Grant agreement No. 101139996.

References

- Abbas, A., Ambainis, A., Augustino, B., Bärtschi, A., Buhrman, H., Coffrin, C., Cortiana, G., Dunjko, V., Egger, D. J., Elmegreen, B. G., et al. (2023). Quantum optimization: Potential, challenges, and the path forward. *arXiv Preprint arXiv:2312.02279*.
- Alotaibi, B. (2023). A survey on industrial internet of things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors*, 23(17), 7470. <https://doi.org/10.3390/s23177470>
- Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, 1(2), 99–109.
- Bae, C., Yang, S., Baddeley, M., Elsts, A., & Haque, I. (2022). Bluetisch: A multi-phy simulation of low-power 6tisch iot networks. *GLOBECOM 2022-2022 IEEE Global Communications Conference*, Rio de Janeiro, Brazil. 4280–4285.
- Bleija, M., Platnieks, O., Macutkevič, J., Banys, J., Starkova, O., Grase, L., & Gaidukovs, S. (2023). Poly (butylene succinate) hybrid multi-walled carbon nanotube/iron oxide nanocomposites: Electromagnetic shielding and thermal properties. *Polymers*, 15(3), 515.
- Blow, F., Hu, Y.-H., & Hoppa, M. (2020). A study on vulnerabilities and threats to wearable devices. *Journal of the Colloquium for Information Systems Security Education*, 7, 7–7.
- Blumbers, B., Dobelis, Ē., Paikens, P., Nesenbergs, K., Solovjovs, K., & Rušņš, A. (2022). WearSec: Towards automated security evaluation of wireless wearable devices. *Nordic Conference on Secure IT Systems*, Reykjavik, Iceland, 2022, 311–325.
- Bravo, C. (2021). *Mastering defensive security: Effective techniques to secure your windows, linux, IoT, and cloud infrastructure* (pp. 287–313). Packt Publishing. <https://www.packt.com>
- Carstens, D., Mahlman, J., Miller, J., & Shaffer, M. (2019). Mobile device espionage. *Journal of Management & Engineering Integration*, 12(2), 86–94.
- D’Mello, O., Gelin, M., Khelil, F. B., Surek, R. E., & Chi, H. (2018). Wearable iot security and privacy: A review from technology and policy perspective. *Future Network Systems and Security: 4th International Conference, FNSS 2018, Paris, France, July 9–11, 2018, Proceedings 4*, 162–177.
- Doshi, K., Yilmaz, Y., & Uludag, S. (2021). Timely detection and mitigation of stealthy DDoS attacks via IoT networks. *IEEE Transactions on Dependable and Secure Computing*, 18(5), 2164–2176.
- Dvorkin, Y., & Garg, S. (2017). *IoT-enabled distributed cyber-attacks on transmission and distribution grids*. 2017 North American Power Symposium (NAPS), 1–6. Morgantown, WV: IEEE. <https://doi.org/10.1109/NAPS.2017.8107363>
- Edo, O., Ang, D., Billakota, P., & Ho, J. C. (2023). A zero trust architecture for health information systems. *Health and Technology*, 14(1). <https://doi.org/10.1007/s12553-023-00809-4>
- Fang, R., Bindu, R., Gupta, A., Zhan, Q., & Kang, D. (2024). *Teams of LLM agents can exploit zero-day vulnerabilities*. <https://arxiv.org/abs/2406.01637>

- Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 101, 55–82.
- Garbelini, M. E., Chattopadhyay, S., Bedi, V., Sun, S., & Kurniawan, E. (2022). *BRAK-TOOTH: Causing havoc on bluetooth link manager*. In *Proceedings of the 31st USENIX Security Symposium* (pp. 1–18). Boston, MA: USENIX Association.
- Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., Robinson, W. H., & Alexis, W. (2016). Securing commercial WiFi-based UAVs from common security attacks. *MILCOM 2016-2016 IEEE Military Communications Conference*, 1213–1218. Baltimore, MD: IEEE.
- Ibarra, J., Jahankhani, H., & Kendzierskyj, S. (2019). Cyber-physical attacks and the value of healthcare data: Facing an era of cyber extortion and organised crime. In H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, & H. Al-Khateeb (Eds.), *Blockchain and clinical trial: Securing patient data*. 115–137. Cham, Switzerland: Springer.
- Judvaitis, J., Abolins, V., Elkenawy, A., Balass, R., Selavo, L., & Ozols, K. (2023). Testbed facilities for iot and wireless sensor networks: A systematic review. *Journal of Sensor and Actuator Networks*, 12(3), 48.
- JustCallMeKoko LLC. (2024). *ESP32Marauder*. <https://github.com/justcallmekoko/ESP32Marauder>.
- Khader, R., & Eleyan, D. (2021). Survey of DoS/DDoS attacks in IoT. *Sustainable Engineering and Innovation*, 3(1), 23–28.
- Kim, Y., Lee, W., Raghunathan, A., Raghunathan, V., & Jha, N. K. (2015). Reliability and security of implantable and wearable medical devices. In S. Bhunia, S. Majerus, & M. Sawan (Eds.) *Implantable biomedical microsystems* (pp. 167–199). Amsterdam, Netherlands: Elsevier.
- Koskosas, I. V., & Asimopoulos, N. (2011). Information system security goals. *International Journal of Advanced Science and Technology*, 27, 15–26.
- Lough, B. (2024). *ESP₃₂-cheap-yellow-display*. <https://github.com/witnessmenow/ESP32-Cheap-Yellow-Display>. <https://github.com/witnessmenow/ESP32-Cheap-Yellow-Display>.
- NIST. (2021). *CVE-2021-36260 Detail*. National Vulnerability Database. <https://nvd.nist.gov/vuln/detail/CVE-2021-36260>
- Odarchenko, R., Gnatyuk, V., Gnatyuk, S., & Abakumova, A. (2018). Security key indicators assessment for modern cellular networks. *2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC)*, 1–7. Kyiv, Ukraine: IEEE.
- Omitola, T., & Wills, G. (2018). Towards mapping the security challenges of the internet of things (IoT) supply chain. *Procedia Computer Science*, 126, 441–450. <https://doi.org/10.1016/j.procs.2018.07.278>
- Ormanis, J., & Elsts, A. (2020). Towards body coupled communication for ehealth: Experimental study of human body frequency response. *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, 1–7. Dublin, Ireland: IEEE.
- Ormanis, J., Medvedevs, V., & Judvaitis, J. (2023). *BEAM: Body coupled communication enabled amplitude modulation for skinput application*. *EWSN*, 380–384.
- Ormanis, J., & Nesenbergs, K. (2018). Human skin as data transmission medium for improved privacy and usability in wearable electronics. *2018 IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, 1–6. Rome, Italy: IEEE.
- OWASP. (2024). *OWASP mobile top 10 2024- final release*. <https://owasp.org/www-project-mobile-top-10>
- Paikens, P., & Nesenbergs, K. (2024). Resilience and vulnerability of consumer wireless devices to cyber attacks. In C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, & D. Štrucl (Eds.), *16th international conference on cyber conflict: Over the horizon* (pp. 47–62). Tallinn, Estonia: CCDCOE Publications.

- Pao, W. (2021). *Common access control vulnerabilities and ways to tackle them*. <https://www.asmag.com/showpost/32127.aspx>.
- Park, H., Nkuba, C. K., Woo, S., & Lee, H. (2022). L2Fuzz: Discovering Bluetooth L2CAP Vulnerabilities Using Stateful Fuzz Testing. *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2022)*, 343–354. Baltimore, MD: IEEE. <https://doi.org/10.1109/DSN53405.2022.00043>
- Peng, H. (2012). WIFI network information security analysis research. *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 2243–2245. Yichang, Hubei, China: IEEE.
- Polop, C. (2024). *Android debug bridge - HackTricks*. <https://book.hacktricks.xyz/network-services-pentesting/5555-android-debug-bridge>.
- Rusins, A., Tiscenko, D., Dobelis, E., Blumbergs, E., Nesenbergs, K., & Paikens, P. (2024). Wearable device bluetooth/BLE physical layer dataset. *Data*, 9(4), 53.
- Rušņš, A., Nesenbergs, K., Tiščenko, D., & Paikens, P. (2024). An experimental study: RF fingerprinting of bluetooth devices. *arXiv Preprint arXiv:2402.06250*.
- Sagers, G., Hosack, B., Rowley, R., Twitchell, D., & Nagaraj, R. (2015). Where's the security in WiFi? An argument for industry awareness. *Proceedings of the 2015 48th Hawaii International Conference on System Sciences*, 5453–5461. Koloa, Kauai, Hawaii: IEEE.
- sansartart. (2024). *Shodan-favicon-hashes.csv*. <https://github.com/sansartart/scraps/blob/master/shodan-favicon-hashes.csv>
- Schmidt, M. B. (2006). *Development and analysis of a model for assessing perceived security threats and characteristics of innovating for wireless networks* [PhD thesis]. Mississippi State University.
- Shodan (n.d.-a). *Explore: tags:iot*. Retrieved July 24, 2024, from <https://shodan.io/explore/search?query=tags:iot>
- Shodan (n.d.-b). *Explore: tags:ics*. Retrieved July 24, 2024, from <https://shodan.io/explore/search?query=tags:ics>
- SIG, B. (2024). *2024 bluetooth market update*.; Bluetooth Special Interest Group (SIG). <https://www.bluetooth.com/2024-market-update/>
- Skadins, A., Ivanovs, M., Rava, R., & Nesenbergs, K. (2020). Edge pre-processing of traffic surveillance video for bandwidth and privacy optimization in smart cities. *2020 17th Biennial Baltic Electronics Conference (BEC)*, 1–6. Tallinn, Estonia: IEEE.
- Smith, P. (2021). *Pentesting industrial control systems: An ethical hacker's guide to analyzing, compromising, mitigating, and securing industrial processes* (p. 162). Packt Publishing. <https://www.packt.com>
- Software, I. S. (2024). *Mobile overlay attacks on android*. <https://www.ikarussecurity.com/en/mobile-device-management-en/mobile-overlay-attacks-on-android/>.
- Verimatrix. (2024). *Deconstructing a mobile banking app overlay heist*. <https://www.verimatrix.com/cybersecurity/cybersecurity-insights/deconstructing-a-mobile-banking-app-overlay-heist/>.
- Wang, H.-M., Zheng, T.-X., Yuan, J., Towsley, D., & Lee, M. H. (2016). Physical layer security in heterogeneous cellular networks. *IEEE Transactions on Communications*, 64(3), 1204–1219.
- Wang, Z., Xie, W., Wang, B., Tao, J., & Wang, E. (2021). A survey on recent advanced research of CPS security. *Applied Sciences*, 11(9). <https://doi.org/10.3390/app11093751>
- Xu, Q., Zheng, R., Saad, W., & Han, Z. (2015). Device fingerprinting in wireless networks: Challenges and opportunities. *IEEE Communications Surveys & Tutorials*, 18(1), 94–104.
- Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for internet-of-things security: A review. *Sensors*, 21(18), 6163. <https://doi.org/10.3390/s21186163>

12 Cyber Threats of Tomorrow

Kate E. Kanasta

Introduction

Cyber, space, and emerging technologies have transformed the strategic environment, but only one question remains – to what extent? This chapter explores the transformative impact of cyber capabilities on modern military strategies, examining whether these changes constitute a Revolution in Military Affairs (RMAs). It delves into the historical context of military revolutions and the specific role of cyber technologies in reshaping warfare. The analysis focuses on three key components: ground-breaking technological developments, significant operational changes, and shifts in organizational structures. By investigating case studies, including Russia's cyber operations in Ukraine, this article highlights the integration of cyber capabilities into military doctrines and strategies. It also discusses the implications for international alliances like NATO and the EU, emphasizing the need for continuous adaptation to emerging threats. The findings suggest that while cyber capabilities have revolutionized modern warfare, ongoing advancements in artificial intelligence (AI) and Internet of Things (IoT) will further influence military strategies and require comprehensive defence approaches.

Vive La Revolution as Long as Nobody Nukes us

Throughout the military history, technology has consistently emerged as the pivotal factor, often defining the superior side in changing balance of power system. Nation-states and non-state groups have always aimed to be the first ones (or at least not the last ones) to acquire the newest cutting-edge military advancements. The nuclear arms race during the 1960s is a prime illustration of how the utilization of new military technologies can influence the power dynamics. Instances such as these have contributed to the emergence of the concept known as RMA. The RMA posits that at certain junctures in history, new military doctrines, strategies, tactics, and the development of new technologies have brought about irreversible changes in the conduct of warfare. Furthermore, these transformations necessitate an accelerated adaption of novel defence policies and strategies (Charles Fissel, 2023). RMAs can be seen as pre or after “shocks” of military revolutions and military revolutions do not only affect military organizations, but also they recast the nature

of society and the state as well. Due to this impact, they alter the capacities of states to project military power. In the process of developing RMAs, military organizations must comprehend fundamental changes in the political, social, and military landscape. Successful application of RMA to national strategies will combine lessons learned carried over into an evidentiary-based analysis of current exercises and capabilities, both in peacetime and war (Murray, 1997).

So far, we have experienced multiple revolutions in military strategy throughout history, such as the innovation of the longbow (14th century), the introduction of gunpowder and artillery (the 15th century), the Napoleonic *levée en masse* – the first compulsory military service and the communications revolution brought by telegraphy, as well as mechanization in the late 19th and early 20th century. In the 20th century, three important science-based innovations led to significant technological progress, but also to new military capabilities: (1) nuclear weapons, (2) biotechnology, and (3) information and communication technologies. In addition, the distinction between military and non-military activities is becoming more and more blurred (Götz, 2008). As Gray (2006) points out, factors such as poor leadership, bad luck, or normal friction could cause one to lose a war, but when no major changes in the warfare are happening, the defence planner is not in serious danger of preparing for the wrong war.

Most authors distinguish three main prerequisites of RMA – (1) **a ground-breaking technological development**, (2) **a significant change of operation followed by a change in military doctrine**, and (3) **consequential changes in the organizational structures** (Yogev, Cohen, & Lewin, 2022). This means that the technology itself (e.g., AI) and the ability of the militaries to recognize its potential and capitalize on the opportunities are inherent in novel weapons systems. Even more, the militaries have to have the capacity (or the skill) to re-organize structures throughout the whole strategical, operational, and tactical chain (Gray, 2006).

Are Cyber Capabilities (R)evolutionary?

When it comes to cyber capabilities, researchers are divided in their views on the long-term implications of development in cyber domain to warfare. Some researchers argue that while it is undeniable that cyber capabilities enhance existing military operations, the implications do not fundamentally alter the very nature of warfare itself. This would suggest that it is a simply evolutionary change rather than a revolutionary shift. A decade ago, it was suggested that the warfare is not only changing but also is transferring from the physical world (conventional warfare) to cyber world. If we follow this assumption, we would currently live in a world where most conflicts occur in a cyber realm, almost limiting actors to engage in traditional warfare with soldiers dying on a battlefield. If we examine the world today, we know that does not reflect reality. Major conflicts, such as Russia's war against Ukraine, elucidate that cyber is definitely a component of military strategies but it has not replaced tanks, howitzers, and missile attacks.

So, is the warfare fundamentally changing? Or is this just a stepping stone in the evolutionary technological development of military capabilities? To further

develop this debate, the first part of this chapter will focus on the three components of RMA outlined above. The aim is to closely examine specific and concrete cyber capabilities that might be categorized as ground-breaking or even disruptive technologies and whether this technological development has triggered both a significant change of operation and consequential change in military doctrine and organizational structures.

A ground-breaking technological development. One of the most noticeable changes is the development and use of independent, kinetic cyber effects such as sophisticated malware. Attacks by malwares like *Stuxnet* and *NotPetya* have gathered the most attention over the years. These highly cited and referenced malware attacks illustrate the high level of sophistication, the targeted nature, and the ability to disrupt the work of critical infrastructure objects, such as nuclear facilities or major power grids. These cyber tools enable actors to achieve strategic objectives without traditional military force as in the case of targeted use of *Stuxnet* against Iranian nuclear centrifuges. Malware can cause very real and physical consequences, something that might have seemed so plausible few decades ago, today benchmarking the sort of capabilities modern militaries should acquire.

Another break-through is what can be described as cyber enablers. Enablers usually share the same level of sophistication and targeted nature as kinetic cyber effects but lack the independent characteristic of the attack. The enabling cyber capabilities have one main task – to ensure that conventional capabilities, such as military force, can deliver the intended effect and reach strategic objectives. An illustrative example is the 2007 Israeli Operation Orchard. While still publicly unconfirmed, the assumption is that the intrusion into the Syrian air defence system enabled the Israel Defence Forces to effectively manipulate the radars to hide incoming planes (Clarke & Knake, 2010). Cyber effects have clawed its way into electronic and information warfare, in particular on tactical-level. Russia in its war against Ukraine has used this approach repeatedly. For example, Russian forces jammed classified communication channels while simultaneously exploited vulnerabilities in commercial software on private phones to send targeted messages to soldiers on the front lines. The attack aimed to lower the morale and will to fight of Ukrainian forces (Brantly, Cal, & Winkelstein, 2017). Similarly, the rise of social media and use of advanced algorithms allows rapid spread of misinformation that can create wide impact. In recent years, we have witnessed campaigns that manipulate public opinions and destabilize governments, even elections of Western countries.

Less sophisticated methods, such as distributed denial-of-service (DDoS) attacks might not be a new tactic, but in recent years have been used more and more frequently to operate under the threshold of military conflict, draining resources and causing general confusion and doubt (Jacobsen, 2021). A less noticeable but occasionally even more impactful dimension is cyber espionage – advanced cyber capabilities that are used for gathering intelligence and conducting surveillance missions with techniques like phishing, zero-day exploits, and cyber reconnaissance. This technical development touches upon the change of operation – this has significantly increased the role of individuals

in countering such threats. If traditional military counter measures are mostly in the hands of armed forces, cybersecurity requires much more comprehensive and whole-of-society approach.

A significant change of operation followed by a change in military doctrine. Novel cyber capabilities have introduced new dimensions and strategies that differ from conventional military tactics. These developments reshape the strategic landscape and enable states to conduct operations in a way that is less visible, more adaptable, and potentially more impactful even on a global scale. The integration of cyber dimension into traditional military strategies has led states to apply hybrid approach where the actors utilize a combination of conventional forces and cyber operations to achieve objectives. Both defensive and offensive cyber capabilities are playing increasingly bigger role in defence strategies. Actors are investing in threat hunting, real-time monitoring, and increasing the resilience of their infrastructure. Cyber capabilities are becoming an integrated part of traditional military operations, enhancing situational awareness and operational effectiveness (Bendett, 2020).

Ability to conduct various cyber operations is accessible to a wide range of actors, including state and non-state structures, creating asymmetric nature of threats in the cyberspace. Disparity of resources and capabilities between different actors enables smaller entities to exploit vulnerabilities and engage in cyber warfare effectively against larger and even more established adversaries (Hecker, 2018). This disparity in resources and capabilities creates a complex asymmetry, particularly between attackers and defenders – attackers can exploit system vulnerabilities with minimal resources, while defenders face the daunting challenges in ensuring absolute security (Friedman, 2016). Consequently, this environment necessitates effective risk management within a multifaceted and resilient framework (NATO, Cyber Defence: Policy and Strategy, 2020).

Another change of operation is the increasing role of individuals and society in the realm of cybersecurity. The human element can significantly influence the effectiveness of cyber defence strategies while it is hard to imagine that the classic conventional military tactics is as greatly impacted by everyday citizens. Individuals often serve as the first line of defence against cyber threats – the behaviours and awareness can either mitigate or exacerbate vulnerabilities. As cyber threats evolve, fostering an informed and vigilant populace becomes paramount – education and training initiatives can empower individuals to recognize potential threats, practice safe online behaviours, and understand the importance of basic cyber hygiene. In this way, the regular citizen not only becomes a target but also an active participant in the defence against cyberattacks (Hadnagy, 2018). Moreover, societal norms and expectations play a pivotal role in shaping the cybersecurity environment. The civilian nature of cybersecurity emphasizes the necessity for collaboration between government entities, private sectors, and the general public to create a robust defence ecosystem. Cybersecurity and therefore cyber defence cannot solely rely on technical solutions and military capabilities: it requires a collective effort to develop policies, share threat intelligence, and establish best practices that enhance national resilience (Bertot, Jaeger, & Grimes, 2016).

Russia's full-scale invasion of Ukraine in 2022 was accompanied by a massive campaign of cyberattacks directed towards Ukrainian society, and one of the largest instances of the use of cyber operations in a conflict to date (Lund, 2024). Cyber dimension in Russia's war against Ukraine, to some extent – first of its kind – far exceeds the cyber dimension of any prior conflict. To be fair, the shift in warfare is not as dramatic or science fiction inspired as one might imagine few years ago. The actual impact of cyberattack can be viewed as both objective and subjective, greatly depending on the perception and context (Brantly & Brantly, 2024). Information warfare and cyberoperations have become an integral part of the Russian government's view of conflict (Lund, 2024). The operations and activities target both – the classical military targets, particularly the critical infrastructure objects, and civilian domain.

Consequential changes in the organizational structures. NATO's Cooperative Cyber Defence Centre of Excellence's (CCDCOE) research conducted in 2019 indicated that a significant number of NATO member states began to take military cyber operations more seriously from started to more seriously 2008 onwards, while some states had already started significant organizational efforts in the 1990s. Yet, majority of were and still are at the early stages of organizational development when it comes to cyber structures. Member states have different strategic objectives that require different approaches and have to be based on different legal and organizational prerequisites resulting in a widely diverse picture. It can vary from cyber structure being authorized to direct and control full spectrum of cyber operations to only having a narrow authority to execute a small set of missions. Some states have fully military cyber structures while others have responsibilities and roles in defence and resiliency efforts in the civilian sector (Smeets, 2019).

Regardless of variations of the process and outcome, it is clear that NATO member states are integrating changes in their respective organizational structures to accommodate to the changes of warfare. At the Warsaw summit in 2016, NATO for the first time ever declared cyberspace to be a military domain, consequentially NATO established a Cyber Defence Policy, emphasizing the need for collective defence against cyber threats. This policy is underpinned by the recognition that cyberattacks can potentially trigger Article 5 of the North Atlantic Treaty, which commits member states to collective defence (NATO, 2016). Only a year later Secretary-General at the time, Jens Stoltenberg, introduced the NATO Cyber Operations Centre (CYOC) which serves as a focal point for coordinating cyber defence efforts among member nations, facilitating information sharing, and enhancing collective resilience against cyber threats. The centre is an entity responsible for requesting cyber efforts from Allied nations and integrating them into NATO operations. Former Secretary-General described the centre as another tool to NATO's operational toolbox to address the threats and deter the adversaries of Alliance (Stoltenberg, 2019). An example of this is SCEPVA – specific tool of integration of sovereign cyber effects in NATO operations.

NATO has taken multiple significant steps to integrate cyber into its organizational structures and doctrines through several key initiatives. The framework for cooperation itself and information sharing among member states is established with

the Cyber Defence Policy. It emphasizes collective defence against cyber threats. Central to this effort is the Cyber Defence Operations Centre, which provides real-time situational awareness and incident response capabilities, consequentially enhancing Alliance's operational readiness in cyberspaces. Additionally, the Cyber Security Centre of Excellence plays a role in developing training and research activities. The incorporation of Cyber Enabled Operations into military strategies further elucidates NATO's recognition of cyber as a critical component of modern warfare. The role of Cyber Defence Committee is to oversee abovementioned efforts, ensuring a coordinated and strategic approach to cyber defence across the alliance (NATO, 2016).

Similarly, the European Union has taken significant strides in integrating cyber capabilities into its governance structures. The establishment of the European Union Agency for Cybersecurity (ENISA) in 2004 marks a pivotal moment, evolving to become a central hotspot for cyber defence policy and strategy (ENISA, 2020). The EU's Cybersecurity Act (enacted in 2019), further solidified the agency's key role in enhancing cybersecurity across the Union, promoting a unified approach to threat intelligence and incident response (Parliament, 2019).

Both organizations have recognized the importance of collaboration, not only among their member states but also with the private sector and international partners. NATO CCDCOE, founded in 2008, exemplifies this collaborative approach, focusing on research, training, and exercise programs to bolster cyber defence capabilities (CCDCOE, 2021). The EU's emphasis on public-private partnerships is evident in initiatives like the EU Cybersecurity Strategy, which aims to enhance cooperation with industry stakeholders to improve resilience against cyber threats (European Commission, 2020). Moreover, the increasing interdependence between cyber defence and traditional security necessitates the continuous adaptation of both NATO and EU structures. The growing threat landscape, characterized by state-sponsored cyberattacks and sophisticated cybercriminal activities, demands a proactive and cohesive response (SIPRI, 2021). As both NATO and the EU seek to refine their cyber strategies, ongoing investment in research, capacity building, and cross-border collaboration will be essential to addressing the multifaceted challenges posed by cyber threats in the contemporary security environment.

What Happens Tomorrow?

Keeping in mind the three requirements for an RMA (a ground-breaking technological development, a significant change of operation followed by a change in military doctrine, and consequential changes in the organizational structures), it is quite certain that cyber has indeed brought revolutionary change to modern warfare. Change has happened and states have strived to adapt to the new reality with various level of success. But what happens now? Have we arrived at the point in time where the speed of changes halts and states have time to catch up? Or we can expect new ground-breaking technological developments in near future, especially when it comes to cyber realm?

As we look towards the future, understanding the potential cyber threats that may emerge is critical for nations, military organizations, and international alliances such as NATO and the EU, to ensure readiness to defend and attack with whatever new technology in the military field. This section will discuss the most likely cyber threats of tomorrow, how military strategies may evolve in response, and the proactive measures that NATO, the EU, and individual nations can undertake to adapt to an ever-changing threat landscape.

Several key threats are anticipated to shape the cyber landscape in the coming years. One of the most significant is the rise of AI and machine learning (ML) technologies in cyberattacks. As these technologies become more sophisticated, malicious actors can leverage them to execute attacks with unprecedented speed and precision. For instance, AI can be used to automate phishing attacks, enabling adversaries to craft highly personalized messages that increase the likelihood of successful breaches (Bertino & Islam, 2019). Additionally, AI-driven malware could adapt and evolve in real time, making it more challenging for traditional defences to detect and mitigate threats. According to researchers, AI is poised to significantly alter the landscape of military operations, enhancing both strategic planning and battlefield execution. The advantage of AI-enhanced technologies, such as ML and autonomous systems, will enable militaries to process vast amounts of data far more efficiently than human operators. For instance, the U.S. Department of Defence has already explored AI applications in predictive maintenance for military equipment, which ultimately minimizes downtime and optimizes resource allocation (Association, 2020). Furthermore, AI-enhanced systems most likely will facilitate the development of more sophisticated cyber warfare tactics – algorithms might anticipate and counteract adversarial cyber threats, reshaping the dynamics in cyber realm (Heath, 2021).

Moreover, the development and use potential for autonomous weapon systems raises significant ethical and operational challenges. While these systems might promise increased efficiency and even reduced risk to human lives, they also introduce complexities related to accountability and risk of potential unintended escalation. Even more heated debates have been triggered by the idea of the deployment of AI in lethal autonomous weapons – there is no consensus on the moral implications of removing human judgment from life-and-death decisions (Sharkey, 2019). Arguments against the use of the systems are focused on the fear that reliance on the systems could lead to conflicts being initiated or escalated without direct human oversight, potentially destabilizing international relations (Asaro, 2019). Key element of future use of these technologies will be establishment of frameworks that govern the ethical use of them, ensuring that warfare remains a domain where human oversight and accountability paramount.

The impact of emerging threats goes beyond military applications, affecting civilian infrastructure and societal resilience. The increasing reliance on interconnected systems means that vulnerabilities in the civilian sector can have cascading effects on national security. For example, the proliferation of IoT devices can serve as entry points for cyberattacks. With billions of IoT devices projected to be connected to the internet, many of which lack adequate security measures,

the adversary could hit the vulnerability jackpot and the potential for large-scale attacks is significant. For example, the *Mirai* botnet attack in 2016, which compromised IoT devices to execute a massive DDoS attack, highlighted the vulnerabilities inherent in this rapidly growing sector (Krebs, 2016). As the number of IoT devices continues to rise, attackers may increasingly target these systems to disrupt services or gain access to more secure networks.

In response to evolving cyber threats, military strategies must continue to adapt to incorporate cyber capabilities as integral components of national and collective defence. Traditional military doctrines, which primarily emphasize kinetic operations, will likely even further shift towards hybrid warfare strategies that blend conventional forces with cyber capabilities. This hybrid approach enables states to conduct operations that are less visible and more adaptive, leveraging the element of surprise in cyber engagements (Bendett, 2020). The blurring of lines between military and civilian domains complicates the establishment of clear thresholds for response, raising questions about how to define an act of war in the cyber realm.

Furthermore, military organizations will need to invest in enhancing their cyber defence capabilities. This includes not only acquiring advanced technologies but also developing a skilled workforce capable of operating in cyber environments. Training programs focused on cyber warfare tactics, threat intelligence analysis, and incident response will be critical to ensuring military readiness in future conflicts. The interplay between technological advancements and military strategies becomes increasingly important. The integration of AI and ML into cyber operations can enhance both offensive and defensive capabilities. For example, AI can be used to detect anomalies in network traffic, enabling quicker responses to potential breaches. However, these technologies also present risks; adversaries may employ AI to automate attacks, making them more sophisticated and harder to counter (Bertino & Islam, 2019). Therefore, military organizations must adapt their operational and technical behaviours to address the dual-use nature of these technologies, recognizing that they can be employed for both defensive and offensive purposes.

The evolution of cyber capabilities signifies a transformative period in modern warfare, meeting the criteria for RMA. The concept of RMA refers to a significant change in the conduct of warfare that alters the nature of conflict, often driven by technological advancements. As demonstrated through historical and contemporary examples, cyber technologies have introduced profound changes in military operations, doctrines, and organizational structures. The blurred lines between military and civilian domains necessitate a comprehensive approach to cybersecurity, involving not just military entities but entire societies. The ongoing cyber conflicts, especially highlighted by Russia's actions in Ukraine, underscore the critical role of cyber capabilities in achieving strategic objectives. However, as the cyber landscape continues to evolve with advancements in AI and IoT, military organizations and international alliances like NATO and the EU must remain vigilant and adaptive. As we look to the near future, it is increasingly likely that we will witness another RMA, primarily fueled by advancements in AI, cyber capabilities, and unmanned systems. By investing in technology, fostering collaboration, and

enhancing workforce skills, they can better navigate the complexities of future cyber threats and maintain a robust defence posture. Countries such as the United States and China are investing heavily in AI technologies to develop advanced command-and-control systems that can analyse data from various sources, enabling faster and more informed tactical decisions (Binnendijk & Libicki, 2019).

However, the anticipated next RMA does not only revolve around technological developments, but it also involves new operational concepts and strategies that encompass these technologies and leverage they provide. Thus, while a new RMA is likely on the horizon while we are still catching up with the previous one, it definitely will involve not only the technologies themselves but also a transformative shift in how military power is conceptualized and employed.

References

- Asaro, P. (2019). The Ethics of Autonomous Weapons Systems. *Journal of Military Ethics*, 18(1), 1–21.
- US Department of Defense (2024). Defense Department Tests AI Software, Advances to Improve Physical Security Posture. <https://www.defense.gov/News/News-Stories/Article/Article/3946607/defense-department-tests-ai-software-advances-to-improve-physical-security-post/>
- Bendett, S. (2020). *Cyber Operations and the Future of Warfare*. Center for a New American Security.
- Bertino, E., & Islam, N. (2019). Cybersecurity of the Internet of Things: A survey. *Computer Networks*, 148, 1–12.
- Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2016). Big Data and Public Policy: A New Frontier for Public Administration Research. *Public Administration Review*, 76(3), 385–396.
- Binnendijk, H., & Libicki, M. C. (2019). *The Future of Artificial Intelligence and Military Operations*. RAND.
- Brantly, A., & Brantly, N. (2024). The Bitskrieg That Was and Wasn't: The Military and Intelligence Implications of Cyber Operations During Russia's War on Ukraine. *Intelligence and National Security*, 39(3), 475–495.
- Brantly, A. F., Cal, N. M., & Winkelstein, D. P. (2017). *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*. Army Cyber Institute.
- CCDCOE. (2021). Cooperative Cyber Defence Centre of Excellence. <https://ccdcoc.org>.
- Charles Fissel, M. (2023). *The Military Revolution and Revolutions in Military Affairs*, Berlin, Boston: De Gruyter Oldenbourg. De Gruyter Oldenbourg.
- Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco.
- ENISA. (2020). *About ENISA*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/about-enisa/what-we-do>.
- Friedman, G. (2016). *The Future of War: A History*. Crown Publishing.
- Götz, N. (2008). *The Revolution in Military Affairs: Its Driving Forces, Elements, and Complexity*. Complexity.
- Gray, C. S. (2006). *Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context*. Strategic Studies Institute.
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*, 2nd edition. Wiley.

- Heath, T. (2021). AI and Cyber Warfare: The New Frontier. *International Journal of Cyber Warfare and Terrorism*, 11(2), 15–30.
- Hecker, M. (2018). *Asymmetric Warfare in the Cyber Age*. Journal of Cyber Policy.
- Jacobsen, J. T. (2021). *Cyber Offense in NATO: Challenges and Opportunities*. International Affairs.
- Krebs, B. (2016). *Inside the Mirai Botnet: A Look into the Biggest DDoS Attack in History. Krebs on Security*.
- Lund, M. S. (2024). *Hybrid Threats in Cyberspace. What Do Russia's Cyberspace Operations in Ukraine Tell Us?* Routledge.
- NATO. (2016). NATO Cyber Defence Policy.
- NATO. (2020). *Cyber Defence: Policy and Strategy*. NATO Communications and Information Agency.
- Parliament, E. (2019). Cybersecurity Act: New EU Cybersecurity Agency. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>.
- Sharkey, N. (2019). The Ethical Landscape of Autonomous Weapons. *Journal of Military Ethics*, 18(2), 123–139.
- SIPRI. (2021). *Cybersecurity and International Relations: The Evolving Threat Landscape*. SIPRI.
- Smeets, M. (2019). NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis. *2019 11th International Conference on Cyber Conflict: Silent battle*. Tallinn: NATO CCD COE Publications.
- Stoltenberg, J. (2019, gada 23. May). *Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge conference*, London.
- Yogev, H., Cohen, R. A., & Lewin, E. (2022). Revolution in Military Affairs - The Operation Mole Cricket 19 as a Case Study for the Technological Race During the Cold War. *International Area Studies Review*, 25.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Index

Note: **Bold** page numbers refer to tables and *italic* page numbers refer to figures.

- Abazi, B. 12
Abrahams, T. O. 179
advanced persistent threats (APTs) 41, 166, 235, 256; *see also* threats
Android Debug Bridge (ADB) 251
artificial intelligence (AI) 102, 176, 180, 196, 236; cyber-physical security 256; Revolution in Military Affairs 270–272
Association of Higher Education and Science Information Technology Shared Services Center (VPC) 184–185
attacks: denial-of-service 112, 238; distributed denial-of-service *see* distributed denial-of-service (DDoS)
attacks; Mirai botnet attack 271; network-based 255; overlay 251; strategies 254; *see also* cyberattacks
attribution 65, 153, 163
authentication 12; insecure 249; multi-factor 188, 189
automated data processing system (ADPS) 99, 100, 104, 106; arbitrary access 108–109; civil law 124; criminal procedure law 118; data stored in 120; fraud in 115; intentional act 113; jurisdiction 121; security requirements 110; technological neutrality and sustainability 103; territorial affiliation 121
automation 12; agricultural 248; and big data processing 188; industrial 244–247
Ayuthaya, S. D. N. 179
Baerbock, A. 167
balance-of-power systems 9
Baltic Cybersecurity Innovation Forum 140
Baltijas Datoru Akadēmija (BDA) 212
Barrinha, A. 151, 152
Bederna, Z. 13
Benetis, V. 13, 20
Blažič, B. J. 204
blockchain technology 236
BlueJacking 238
BlueSnarfing 238
Bluetooth: firmware security challenges 238–240; fuzzing tools for 240; securing environment 240–241; security risks with 239; vulnerabilities 238, 239
Bluetooth Low Energy (BLE) 237–238
Boas, T. C. 34
Bodas, M. 79
Body-Coupled Communication 257, 258
boundary spanner image 153
Brinkmann, S. 77
Burton, J. 74, 80
business goals 18, 19
capacity-building 138–141, 143, **144**; “one-size-fits-all” approach in 160; resilience 177
capture the flag (CTF) 211–212
centralization 39, 47, 176; balancing 185; benefits of 183; vs. decentralization 38–39, 176, 195; economical measure and quality enhancer 183; loss of control 183; monopolization 183; organizations 184–185; risks associated with 183–184; semi-centralised model 35, 39, 46, 136; single point of failure 183
CERT.LV 5, 13, 20, 37, 39; assets and configurations 62; audit and feedback process 65–66; authority 58; capacity-building 138–140; case study 57–68; classification 59, 60, **60**;

- code of conduct/practice/ethics 60;
- communication training programme 62; comprehensive incident resolution framework 65; consolidated messaging system(s) 63; constituency 58; detection capabilities 64; email services 63; emergency reachability 66; escalation to governance level 64; extensive incident resolution toolset 64; flagship event in 139; governance reporting 67; handling sensitive information 66; human maturity 60–62, 69; incident classification matrix 59; incident detection process/prevention measures 65; incident statistics 122; information sources 62–63, 66; internal and interagency meeting processes 67; job description 61; knowledge transfer and technical support 143; legal escalation process 65; mandate of 57–58; mandatory technical training 61–62; Memorandums of Understanding 62; organisational maturity 57–60, 68–69; outreach programme 67; participation in CSIRT systems 59; peer collaboration 67–68; policy recommendations 70–71; prevention toolset 63–64; process maturity 64–68, 70; public disclosure procedures 65; public media policy 58; resilience and effectiveness 71; responsibilities 58; security policy 59; service description 58; service-level description 58–59; staff resilience 61; structure and operational framework 59; structured and comprehensive evaluation 57; structured onboarding process 61; tools maturity 62–64, 69–70; voice communication method 63; website and public engagement 66
- Chang, S. E. 80
- chief information security officer (CISO) responsibilities 36
- Civil Protection Plan 84, 94; Aluksne region's 86; Latvia—Daugavpils and Rezekne 87; Liepaja and Dienvidkurzemes region's 84–85; local 84; Riga City Council's 85
- Claire-Bazy, M. 102
- combating cybercrime 6, 100, 108, 121
- Common Foreign and Security Policy (CFSP) 133
- Common Security and Defence Policy (CSDP) 133
- community resilience 83–90; *see also* resilience
- competences 205, 221, 229–230; classification 217; frameworks 203; future 221, 222, 223; gaps 221, 222; leadership 217, **229**; operational 217, **229**; professional 217, **229**; roles and 201; technical 217, **229**
- Computer Emergency Response Team (CERT) 16, 53
- computer-related fraud 114–116, 123
- Computer Security Incident Response Team (CSIRT) 5, 36, 52, 133; core responsibilities 55; cybersecurity governance 53–56; emergence of 53; in European Union 55–56; government-led 54; hybrid 54; independent 54; maturity assessment 52–71; Network and Information Systems directive 55–56; operational effectiveness 56; operational scope 53; organisational models of 54–55; practitioner-centric approach 57; proactive functions 53; reactive functions 53; tasks 55–56
- Concordia project 202, 204
- conformity assessment bodies (CABs) 137
- conspiracy theories 91
- Constitutional Council of France 102
- Constitutional Court 100–101
- Constitution Protection Bureau (SAB) 43–44, 167
- content analysis: legal/policy documents 76
- Convention on Cybercrime (CC) 99–100, 102, 104, 107
- corporate social responsibility models 88
- COVID-19 pandemic 91, 176
- Creswell, J. W. 76
- crime: definitions 101; object 112–113; *see also* cybercrime
- criminal law 118–121; components 104; fundamental principle of 100–101, 125; public official 105; rule of law notion 101; Section 177 115; Section 241 114; Section 243 111
- criminal liability 101, 102, 113, 125
- criminal offence 101, 102; causal link 107; characteristic 103; classification 104; computer-related fraud 114–116; construction 104; data interference 111; factors 107; General Safety and Public Order 108; illegal device 113; illegal interception 105–107; against information system security 104–105,

- 108; Information Technology Security Law 52, 109, 110; interception process 107; liability 114, 124; objective element 111; repercussions 107; subject 105; system interference 111, 112; unauthorized manipulation 111
- Cross-Sector Cybersecurity Performance Goals (CPGs) model 15
- CrowdStrike case 183–184
- cryptoviruses 189
- cyberattacks 130, 150; Baltic states
 - 1; cognitive perspectives 80; on compromised devices users 252; escalation in 179; in Estonia 151, 156; *see also* attacks
- CyberBazaar 140
- cyber capabilities 9, 265–269
- CyberChess 29, 139
- cybercrime 6, 99, 175; challenges
 - 6; combating 6, 100, 108, 121; computer-related fraud 114–116; concept of 100–104; in conventional internet browsers 251; criminal law and 118–121; jurisdiction 6, 7; legal certainty 103–104; legal framework 100–116; offences *see* criminal offence; principles 103–104; scientific research method 100; technological neutrality 103; transnational nature 163
- Cybercrimes Committee 102
- cyber defence 133, 140–141, 143–145, **144**, 146, 268–269
- Cyber Defence Policy 268, 269
- Cyber Defence Unit (CDU) 37–38
- cyber diplomacy *see* diplomacy
- Cyber Incident Response Institution 122
- Cyber Operations Centre (CYOC) 268
- cyber-physical security (CPS) 8–9; access control systems 235–236; agricultural automation 248; agriculture 233; artificial intelligence 256; automated and self-driving 259; autonomous vehicles 233; Bluetooth Low Energy 237–238; categories 233; challenges 234; civil infrastructure and transportation 233; communication security challenges 235–242; dual use and military applications 259–260; endpoint 255; 4G and 5G cellular networks 236–237; fuzz testing 239–240; hashes and country-specific filter 246, 247; healthcare devices 248; industrial automation 244–247; LoRaWAN 241; mobile and wearable systems 233; mobile application threats 249–251; network-based attacks 255; programmable logic controllers 244–247; public transportation and smart mobility 248; quantum-related research 258; radio signal and data security 259; robotics and manufacturing 233; security concerns 242; security-related projects 259; Shodan tool 242–243; Sigfox protocol 242; smart grids and industrial control 233; smart home systems 244; smart traffic monitoring solutions 259; of smart wearables 256–257; supply chain risks 255; threats to 249–260; WiFi 237; wireless communication protocol 257–258; Zigbee 241
- Cyber Resilience Act 137, 142, 145, 169
- CyberSec4Europe project 202–203
- CyberSecPro project 203, 205
- cybersecurity (CS) 7; authorities 134; awareness and collaboration 3; case studies 176–177; challenges and opportunities 4; community clusters in 26, 28; competence frameworks 203; in digital age 74, 176; ecosystem *see* ecosystem; events **22**, 23, 25–26, **27**, 28, 29; financial and healthcare sector 176–177; future skills 204–206, 225, 229; policy documents 75; public policy 32; responsibilities 41; roles 217, **218–219**, 220, 220; skills gaps 203; smaller nations 3; societal resilience *see* societal resilience; specialists of organizations 220, 221; stakeholder group **226–228**; threats *see* threats
- cybersecurity awareness 18, 66, 86, 89–93, 95, 138
- cybersecurity governance 4, 129, 135; centralised model 39, 47, 176; collaborative 32; Computer Security Incident Response Teams 53–56; critical factors 33; decentralised model 38–39, 176; digital revolution 32; under eIDAS 38; enforcement and compliance mechanisms 48; evolution 35–44; geopolitical instability 38; institutional and legal evolution 4; institutional foundation for 94; IT Security Law (2010) 36–37, 40, 44; lack of oversight and accountability 41; modernisation 35–36, 41–44; national 154; Network and Information Systems directive 40; path dependence *see* path dependence;

- policy evolution 44; public trust in 96; responsibilities of supervisory institutions 48; semi-centralised model 35, 39, 46, 136; state information systems 36
- Cybersecurity Higher Education Database (CyberHEAD) 202
- The Cybersecurity Strategy of Latvia* 155, 157
- cybersecurity transformation 7–8, 175–196;
 - case studies 186–194; centralization *see* centralization; compliance landscape and legislative initiatives 181–182; direct observations 178; document analysis 178; landscape 178–179; Latvia State Radio and Television Centre 138, 177, 184, 192–193; Latvia University of Life Sciences and Technologies 177, 189–191; Latvijas Mobilais Telefons 177, 191–192; literature review 176–177; methods and approach 177–178; multiple-case study design 177; organizations 177, 186, 193–194, 196; Riga Technical University 177, 188–189; semi-structured interviews 178; strategic directions 180–182; Tet 177, 186–187
- cybersecurity workforce development
 - 8, 200–201; design science problem-solving method 205–206; future skills 204–205; literature review 201–205; methods and approach 205–207
- Cybersecurity Workforce Framework (CWF) 203
- Dahua 246
- Dante, A. D. 79
- D’Arcy, J. 12
- Das, S. 17
- data leakage 250
- data preservation 119
- data privacy analyst/data protection officer **219**
- Dawson, J. 204
- decentralised governance model 38–39, 176; *see also* cybersecurity governance
- denial-of-service (DoS) attacks 112, 238
- digital diplomacy 151–152; *see also* diplomacy
- digital ecosystem 11, 13; *see also* ecosystem
- Digital Europe Programme 133, 139, 143, 146
- Digital Operational Resilience Act (DORA) 187
- Digital Security Supervisory Committee (DDUK) 39, 40, 43, 47, 137
- Digital Services Act (DSA) 102
- digital sovereignty 6, 7, 130, 142, 145
- diplomacy 7, 133, 150; across political formats 158–159; capacity-building methods 160; collective responsibility 159, 164; definition and dimensions 151–154; digital diplomacy vs. 151–152; dimensions 151–154; Estonian cyberattacks 151, 156; implications for policy interventions 153; incident attribution procedures 163; intelligence sharing 153; international and regional political formats 166; international norms 155, 160, 165; international relations 152; landscape of 154–158; legislative and policy initiatives 155; nations approaches 154; Open-ended Working Group 155, 159–160, 168; private sector organisations 153; scope 152; skills requirement 153; types 150, 151
- Directives on Security of Network and Information System 16
- Directorate-General for Communications Networks, Content and Technology (DG CNECT) 132
- distributed denial-of-service (DDoS)
 - attacks 112, 116, 150, 167, 180, 266, 271; mitigation strategies 193, 194; Riga Technical University 188; Tet 187
- ecosystem 4–5, 46; aggregation 21; analysis 22–29; capacity-building 138–140, 143, **144**; collaboration mechanisms 13, 16; composition and motivation of entities 11; conceptual model 131, *132*; customer and end-user role 21; cyber defence 140–141, 143–145, **144**; Driver role 21; education 200, 201, 206, 207–215; enterprise modelling 11, 12, 29; European Union 6–7, 129–146; generic roles 22, 23, **24–25**, 30; goals *17*, 17–20; governance of *see* cybersecurity governance; governmental institutions and regulations 13; graph 23, 25–26, 26, 27, 29; human goals 16; informal representation 13; key building blocks 12; keystone and niche players 17; legislation and literature analysis 20;

- macro-level and micro-level players 16; mapping 13; modelling approach 13–14; notation used to model **15**; organisational entities through events 26, **27**, 28, 29; organisational roles and actors in 17; organisational units **24**; personal and national security 18; perspective 13, 16; policy and legislation 135, 136–137, 142, **142**; policy recommendations 145–146; practitioner-centric approach 134; practitioner-oriented approach 135; qualitative case study 134; resilience 16–17; roles **19**, 20, 20–22, 21; science-for-policy 46; with sectoral legislation 131; thematic dimensions 135–141; theoretical and practical interest 29; well-functioning 47
- education 8; challenges 200, 204; ecosystem 200–201, 206–215; effective communication in 92; future 204; general basic 207–211, 223–224; higher 213, 213–215, 225; institutions, business goals 18, 19; non-formal 211–213, 224, 230; offering and provision 201; primary 201–203, 208, **209**; professional standards, requirements for 215–221; providers **227**; provision 223–225; research methodology 206; research questions 201; secondary 201–203, 208, **210**, 211, 224; skill gap 200; workforce and student-oriented 200
- eIDAS 38
- Elburz, Z. 79
- Electronic Communications Law 107, 119
- electronic information system 119
- Elran, M. 79
- endpoint 255; implement robust security measures 260; unprotected 251; vulnerabilities 255
- ENISA *see* European Union Agency for Cybersecurity (ENISA)
- enterprise modelling 11, 12, 29
- e-PINE (Enhanced Partnership in Northern Europe) 165
- ESP32 Marauder* software 240, 241
- Estonian cyberattacks 151, 156
- EU Cybersecurity Act 16, 137, 176, 181, 194, 202, 269
- EU Cybersecurity Strategy 82, 182, 269
- Eurobarometer (2021) survey: cybercrime 99, 122; societal resilience 88, 91
- European Convention on Human Rights 102
- European Court of Human Rights 107
- European Cybercrime Centre (EC3) 134, 140
- European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) 133, 141
- European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) 133, 139
- European Cybersecurity Organisation (ECSO) 134, 205
- European Cybersecurity Skills Framework (ECSF) 143, 145, 203
- European Defence Agency (EDA) 133
- European External Action Service (EEAS) 133
- European Security and Defence College (ESDC) 140
- European Social Fund project 212
- European Space Agency 152
- European Telecommunications Standards Institute (ETSI) 13, 22
- European Union (EU): Computer Security Incident Response Team in 55–56; conventional armed conflicts in 1; Cybercrime Directive 103; Cyber Diplomacy Toolbox 7, 155, 157, 162–163, 168; cybersecurity ecosystem 6–7, 129–146; and NATO 2, 3; policies 135, 136; wake-up call for 1–2
- European Union Agency for Cybersecurity (ENISA) 16, 53–54, 131–132, 179, 200, 202, 269; roles in organizations 220, 220; threat group 150; three-tier approach 57
- existing threats 254; endpoint vulnerabilities 255; *see also* threats
- Explanatory Report to Convention on Cybercrime (ER CC) 100, 105, 106, 112, 114, 116, 117
- Farmer, L. 101
- financial support through third-party (FSTP) funding 139, 143
- focus group discussions 76–77, 96
- Ford, C. A. 153
- foreign policy 7, 150, 166; implementation 157; instrument 151, 152; long-term objectives 161; multilateral formats 155; national perspective 168; Russia's 167
- Forum of Incident Response and Security Teams (FIRST) 53
- 4G and 5G cellular networks 236–237

- fraud: in automated data processing system 115; computer-related 114–116, 123
 fuzz testing 239; generative approach 239; hybrid approach 240; mutational approach 240; techniques 239–240; tools for Bluetooth 240
- gatekeeper image 153
- General Data Protection Regulation 102
- General Safety and Public Order 108
- Gercke, M. 103
- German Constitutional Court 106, 111
- Global Cybersecurity Index 180, 194
- goals: business 18, 19; collaborative security 16; components 15; information security 14–15; resilience 18–20
- governance *see* cybersecurity governance
- government-led CSIRT 54
- Gundu, T. 179
- Güngör, M. 79
- Haavik, T. K. 79
- hacker tools 114
- Hajny, J. 217, 225
- Hamkova, D. 124
- Harvard Research Draft Convention 116
- higher education programmes 213, 213–215, 225; *see also* education
- Hikvision 246
- Hocking, B. 153
- Horizon Europe programmes 133, 139, 143, 146, 202
- Horizontal Working Party on Cyber Issues (HWPCI) 133, 162
- Hovav, A. 12
- illegal interception 105; computer data 106–107; confidentiality and privacy 106; criminal offence, objective side 107; location data 107; Section 144 105–107; stored data 107
- incident response: effective 52; reactive model 69; requirements 40; 24/7 operations 71
- independent Computer Security Incident Response Team (CSIRT) 54
- industrial automation 244–247; *see also* automation
- industrial control systems (ICS): Internet of Things and 244, 244; products tagged as 245, 245
- information and communication technology (ICT) 5, 11, 74, 150; service providers 21–22, 26; universal security requirements 40
- information security: ecosystem 12; goals 14–15
- Information Society Agency 12
- information system security (ISS) 99, 111, 123; criminal offence 104–105, 108; manager 217, **218**
- Information Technology (IT) Security Law 36–37, 40, 44, 52, 109, 110
- innovation 35, 46, 47, 133, 139, 143, 233, 265
- insidious attack strategy 254
- Interinstitutional Working Group 161
- International Conference of the Constitutional Court 102
- international cooperation 154, 156
- international norms 155, 160, 165
- international relations (IR) 130; collective security perspective 130; cyber diplomacy 152; digital sovereignty 130–131
- International Telecommunication Union (ITU) 53, 110
- Internet of Things (IoT) 8–9, 236; agricultural automation 248; electric grid 254; endpoint 255; and industrial control systems 244, 244; proliferation 270
- interoperability 12, 61, 142
- Joinson, A. N. 80
- jurisdiction: and criminal procedure law 118–121; cybercrime 6, 7; doctrine of consequences 117; electronic evidence 118; fundamental principles 116–118; geographical 116; Harvard Research Draft Convention 116; nationality 117; passive personal/victims 118; principle of defence/consequences 117; subjective 117; territorial principle 116–117
- Kaktiņa, K. 164
- Kasper, A. 152
- Kellos, L. 160
- Krippendorff, K. 76
- Kvale, S. 77
- Lain, C. 74, 80
- Lancelot, J. F. 154
- Latvian Academic Data Transmission Network 184, 185

- Latvian Information and Communications Technology Association (LIKTA) 90
- Latvian National Library (LNB) data center incident 184
- Latvia State Radio and Television Centre (LVRTC) 138, 177, 184, 192–194; data centre standards 192–193; high-security services 193; service level agreements (SLAs) 192; State Electronic Communications Service Centre (VESPC) 192
- Latvia University of Life Sciences and Technologies (LBTU) 177, 189–191, 193–194; challenges 190, 191; diverse cybersecurity measures 190; early warning system (EWS) 190; extensive VPN and remote access 191; in-depth analysis 190; private optical network 190
- Latvijas Mobilais Telefons (LMT) 177, 191–194; collaborative efforts with military 192; global trends 194; Internet Guard Service 191; physical security and IT 191; proactive strategy regarding sanctions 191–192; technological advancements 192
- legal certainty: principle of 103–104
- Les, W. 79
- Linkov, I. 80
- LoRaWAN 241
- Maastricht Treaty 130
- machine learning (ML) 176, 180, 196, 236, 270; Revolution in Military Affairs (RMAs) 270, 271; techniques 240
- Marčinauskaitė, R. 106
- Mathias, E. 117
- maturity model, CERT.LV 56–57; human maturity 60–62, 69; organisational maturity 57–60, 68–69; process maturity 64–68, 70; tools maturity 62–64, 69–70
- Melbarde, D. 158
- Metsola, R. 140
- MICNET Category A project 134
- Military Computer Emergency Response Team (MilCERT) 40–41, 140–141
- Ministry of Foreign Affairs (MFA/MoFA) 151, 155; cyber diplomacy 166, 169; cyber incident attribution 163; malicious cyber activities 164; representatives 158, 159; stakeholders role 155; traditional position of 153; UNSC membership and foreign policy 161
- Mirai botnet attack 271
- misuse of devices 114
- Mobile Application Security Vulnerability Standard (MASVS) 251
- mobile application threats 249–253, 253; *see also* threats
- mobile data communications 236–237
- Mobile Security Testing Guide (MSTG) 251
- modernisation 35–36, 41–44
- Molnár, A. 152
- Morgan, D. L. 77
- Morgus, R. 54
- Morris Worm incident 53
- multi-factor authentication (MFA) 188, 189
- naive attack strategy 254
- National Armed Forces 140
- National Centre of Education 208
- National Civil Protection Plan 84
- National Coordination Centre in Latvia (NCC-LV) 139, 140
- National Coordination Centres (NCCs) 133
- national CSIRT *see* Computer Security Incident Response Team (CSIRT)
- National Cyber Security Centre (NCSC) 4, 20, 29, 42, 46, 54, 82, 89, 156, 182; centralised cybersecurity governance model 47; CERT.LV's and 48; consolidating responsibilities under 47; as executive agency 42; hybrid model 42–44, 47; as ministry department 42
- national cybersecurity governance 154; *see also* cybersecurity governance
- National Cyber Security Index (NC SI) 180
- National Cybersecurity Law (NCL) 20, 29, 46, 47, 57, 58, 81–82, 110, 137, 155, 163, 176, 182; *see also* CERT.LV
- National Cybersecurity Strategy 22, 82, 83, 154
- National Defence Concept 81
- National Development Plan 161
- National Institute of Standards and Technology (NIST) 203
- National Liaison Officers (NLO) Network 132
- National Scientific Activity Information System 185
- National Security Law (2000) 37
- national sovereignty 130–131
- NATO 145; Cooperative Cyber Defence Centre of Excellence (CCDCOE) 141, 268, 269; European Union and 2, 3

- network analysis techniques 29
- Network and Information Systems (NIS)
 - directive 40, 55, 110, 136; Computer Security Incident Response Team in 55–56; digital service providers 40, 43; entity designation under 40; ICTs security requirements 40; incident response requirements 40; operators of essential services 40, 43
- network-based attacks 255; *see also* attacks
- network security enhancements 260
- NFS (Network File System) 245–246
- non-formal education 211–213, 230; adults 212–213, 224; children and teenagers 211–212
- non-governmental organisation (NGO) 134
- Norris, F. H. 83
- NotPetya 266
- nulla poena sine lege* 101
- Obama, B. 156
- offence *see* criminal offence
- Omitola, T. 255
- Open-ended Working Group (OEWG) 155, 159–160, 168
- Ostrom, E. 76
- Osula, A.-M. 152
- overlay attacks 251
- OWASP Mobile Security Project 249;
 - binary protections 250; cryptography 250; improper credential usage 249; inadequate privacy controls 249; inadequate supply chain security 249; input/output validation 249; insecure authentication/authorization 249; insecure communication 249; security misconfiguration 250; sensitive data 250
- Page, S. E. 33, 34
- participants 12; in CSIRT systems 59; resilient cyber ecosystem 16–17
- path dependence 33; composite-standard model 34; decision-making approach 34; dynamic system 34; evolutionary periods and 34; factors analysis 35; increasing returns 34, **45**; lock-in **45**; policy coordination tools 35; policymakers 33–34; positive feedback 33, **45**; self-reinforcement **45**; types of 33, 35, 44, **45**; uncertainties 35
- Pavluta-Deslandes, S. 159, 165
- Pedersen, D. B. 46
- PESCO projects 134
- Pierson, P. 33
- policy documents 75; content analysis of 76
- policy makers **226**, **228**
- practitioner-centric approach 57, 134
- practitioner-oriented approach 135
- primary education 201–203, 208, **209**; *see also* education
- principle of legality 101
- procedure law 118–121
- professional education programmes 211, 215–221, **216**, **217**; *see also* education
- programmable logic controllers (PLCs) 244–247
- Programme of Action (PoA) 159, 168
- Programming and Design & Technology 208
- Public Administration Modernization Plan 183
- public-private partnerships (PPPs) 90, 137; societal resilience 90, 95; for supply chain security 48
- quantum computing technology 256
- quasi-cybercrime 114
- Radanliev, P. 152, 153
- Rajnai, Z. 13
- Rattanapong, P. 179
- Renard, T. 152
- resilience 2–3, 177; capacity building 177; CERT.LV 71; ecosystem 11–12, 16–17; goals 18–20; roles 21, **21**; *see also specific resilience*
- Revolution in Military Affairs (RMAs) 264–265; artificial intelligence (AI) 270–272; autonomous weapon systems 270; conventional military tactics 267–268; criteria for 271; cyber capabilities 265–269; ground-breaking technological development 266–267; machine learning 270, 271; requirements for 269
- RIGA COMM 2023 conference 26
- Riga Technical University (RTU) 177, 188–189, 193–194; automated security management solutions 188; automation and big data processing 188; cloud service vulnerabilities 189; cryptovirus evolution 189; distributed denial-of-service attacks 188; email security challenges 189; global trends 194; multi-factor authentication (MFA) 189; security perimeters 188; system aging and vulnerability management 189; user acceptance of security measures 188
- Rinkēvičs, E. 157, 164
- Riordan, S. 151–153, 169

- Rosen, J. 102
 Russian invasion of Ukraine 1–2, 157
- Sadik, S. 47
 science-for-policy ecosystem 46
 secondary education 201–203, **210**, 211;
 awareness and hygiene **209**; levels 208;
 professional (vocational) 211, 224; skills
 208; *see also* education
- Security Incident Management Maturity
 Model (SIM3) 5, 52, 57
 security risk management specialist **219**
 semi-centralised governance model 35, 39,
 46, 136
 semi-structured interviews 178; societal
 resilience 77, 85
 Shinozuka, M. 80
 Shodan tool 242–243
 Sigfox protocol 242
 smaller nations cybersecurity 3
 smart grid 254
 smart home systems 244
 Smith, G. 151
 social capital 80, 89
 social cohesion 80
 societal resilience 5–6, 75; assessment of
 84; business perspectives on 88; Civil
 Protection Plans 84–86; community
 perspective 83–90; comprehensive
 analysis of 94; conspiracy theories 91;
 content analysis of legal and policy
 documents 76; crisis-resistant and 79;
 critical indicator of 90; Elran's definition
 79; essential actors 79; Eurobarometer
 (2021) survey 88, 91; focus group
 discussions 76–77, 96; fundamental
 pillars of 75; fundamental strategy
 for 92; government initiatives 77–78;
 Haavik's definition 79; holistic approach
 to 80; individual perspective 90–93;
 institutional and national mechanisms
 87–88; institutional trust 89; Luminor
 Bank (2024) survey 88; mixed-research
 methods 77; municipality's approach
 86–87; one-stop cyber agencies 85–86;
 perspective 79–81; preparedness
 mechanisms 86; private sector and
 citizens 86; psychosocial 85; public
 opinion polls 77; public-private
 partnerships 90, 95; research methods
 76–78, 78; semi-structured interviews
 77, 85; small-state model 96; *vs.*
 state-centric paradigm 74; state
 perspective 81–83; strengthening 95–96;
 trust 89; well-defined participatory
 mechanisms 89–90; *see also* resilience
- socio-technical systems 11
 software-defined radios (SDRs) 235
 sovereignty: digital 6, 7, 130, 142, 145;
 jurisdiction 117; territorial 121;
 traditional notions of 130
- Special Investigative Actions 120
 Special Part of Latvian Criminal Law 103,
 104, 108, 117, 124
 Sprüds, A. 156
 stakeholder: collaborative approach 5;
 economic 94; ecosystem of 3–4, 134;
 focus group discussions 76–77; group,
 recommendation for 225, **226–228**;
 micro 16; role 155
- Stake, R. E. 177
 state-centric paradigm: societal resilience
 vs. 74
 State Civil Protection Plan 82
 state information systems 36
 State Security Service 109
 Steinmetz, K. F. 101
 Stikvoort, D. 56
 Stoltenberg, J. 268
 stored data 119; in automated data
 processing system (ADPS) 120;
 electronic information system 119
- Stuxnet 266
 substantial harm 111, 123–125
 supply chain: OWASP Mobile
 Security Project 249; public-private
 partnerships for 48; risks 255; security
 management 260
 system interference 111, 112
- Tallinn Manual 120
 technological neutrality 103
 Tet 177, 186–187, 193–194; dependence
 on reliable IT resources 187; distributed
 denial-of-service attacks 187; enhanced
 update frequency 187; global trends
 194; regulatory compliance and audit
 routines 187; team evolution 186;
 transition to zero trust architecture 186;
 vulnerability monitoring and testing
 187; web application firewall 187
- Thomson, R. 204
 threats 19, 36, 41, 91, 169, 192; awareness
 88; critical infrastructure against
 159–160; to cyber-physical security
 249–260; existing 254–256; financial
 and non-financial effects 125; future
 256–260; military strategies 271; mobile

- application 249–253, 253; protection against 99; quantum computing 256; smart grid and industrial 254; wireless communication 253–254
- Trojan horses 235
- trust 21–22
- Tsai, C. H. 12
- Ukraine: Russian invasion of 1–2, 157
- United Nations Security Council (UNSC) 159, 161
- UN Programme of Action (PoA) 159, 168
- vocational education programme 211, 224; *see also* education
- Walker, B. 78
- WearSec project 240, 256
- web application firewall (WAF) 187
- Whites, B. 102
- whole-of-society and whole-of-government approach 3
- WiFi 237
- Wight, M. 150
- Wills, G. 255
- Windle, G. 85
- wireless communication 235, 237; threats 253–254
- World Economic Forum and Accenture (2024) 179
- Yar, M. 101
- Zdravkovic, J. 12
- zero-trust principles 35, 236
- Zigbee 241