CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

The evolution of cyber forces in NATO countries

Dr. Aleksander Olech

Visiting scholar

Dr. Damjan Štrucl

NATO CCDCOE Strategy Researcher

Tallinn 2025

About the author

Dr. Aleksander Olech is the Head of International Cooperation at Defence24, where he leads strategic initiatives and fosters crucial global partnerships. He is a distinguished lecturer at both national and international universities, sharing his deep expertise in international relations and security studies. As a NATO associate, analyst, and publicist, Dr. Olech contributes significantly to discussions and policy development in global defence and diplomacy. His previous role as Deputy Director of the Department of Africa and the Middle East at the Ministry of Foreign Affairs allowed him to shape regional policies and influence international relations. Over recent years, Dr. Olech has been actively collaborating with various NATO centres of excellence (COEs), including the NATO ENSEC COE in Vilnius, NATO StratCom in Riga, NATO CCD COE in Tallinn, and NATO COE DAT in Ankara. With these elite centres, he focuses on enhancing security measures, strategic communications, counterterrorism, and defence technologies. He holds degrees from the European Academy of Diplomacy and the War Studies University. He specialised in Franco-Russian relations, hybrid warfare, and NATO's security policy. Dr. Olech's research and professional contributions continue to shape global security dynamics and diplomatic strategies, establishing him as a prominent young voice in these critical areas.

Dr. Damjan Štrucl is a Lieutenant Colonel (OF-4) in the Slovenian Armed Forces and is currently a researcher in the Strategy Branch at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). He has been working in the field of communications and information systems since 2004. During his career, he was the commander of the signal unit and an INFOSEC officer in several units of the Slovenian Army. From 2015 to 2020, he served as a senior officer of cyber defence and as the head of the Cyber Defence Department of the General Staff of the Slovenian Army. His research focuses on the comparative analysis of the legal and institutional regulations of cybersecurity and defence between various countries, and specifically between NATO and the European Union (EU). He has completed several educational programmes and training courses on information and cybersecurity at home and abroad, holds a Master's degree in Governmental and European studies and a Doctorate in law from the New University, Slovenia.

Acknowledgements

The author would like to express sincere gratitude to Dr. Damjan Štrucl for his invaluable supervision throughout this research. I am deeply thankful to the many experts who generously shared their knowledge and insights, including Dr. Sven Herpig, Dr. Athanasios Staveris-Polykalas, Prof. Plamen Pantev and Dr. Velko Attanassoff. I am equally grateful for the dedicated support of my colleagues at CyberDefence24, including Konrad Markiewicz, Gabriela Urbańska, Paweł Makowiec, Dorota Kwaśniewska, Zuzanna Sadowska and Mieszko Kucharski, as well as the wider community of independent researchers who contributed to this work. I particularly appreciate the input of individuals affiliated with national institutions, whose identities cannot be disclosed due to the nature of their roles. Finally, I would like to thank the CCD COE community for their outstanding work and for the many valuable analyses they continue to provide to the field. My thanks go especially to the researchers at CCD COE, including Piret Pernik, Major Battista Magurno, Nick Womba, Major Frédéric Lambrix and Otakar Horák, for their generous insights and collaborative spirit.

This research on the evolution of cyber forces is an ongoing effort. Its progress would not be possible without the valuable support and contributions of researchers, experts, practitioners, and North Atlantic

Treaty Organisation (NATO) representatives. Their insights and dedication continue to play a crucial role in shaping and advancing this important field.[1]

CCDCOE

The NATO CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the *Tallinn Manual*, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring the Centre hosts the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. Since January 2018, CCDCOE has been responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by the following NATO nations and partners of the Alliance: Albania, Austria, Australia, Belgium, Bulgaria, Canada, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Montenegro, North Macedonia the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom (UK) and the United States (US). NATO-accredited COEs are however not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

[1] Any observations regarding potential errors or suggestions for improving this research are welcome and may be directed to the author at: a.olech@defence24.pl

Table of Contents

1. Abstract

The emergence of cyberspace as a realm of strategic competition has fundamentally transformed the global security environment, necessitating that NATO and its member states continuously reassess the frameworks, doctrines, and capabilities required for effective defence. As cyber threats increase in frequency, complexity, and severity—spanning critical infrastructure sabotage to hybrid disinformation campaigns—NATO allies are expediting the establishment of specialised cyber units within their national armed forces. These advancements address national security requirements and significantly enhance the Alliance's collective resilience.

This study provides a thorough analysis of cyber force development across all 32 NATO member states, emphasising their distinct methodologies for establishing, organising, and integrating cyber units within their respective military and defence structures. Each nation is evaluated based on its cybersecurity environment, the historical development of its cyber units, and the present organisation and competencies of its cyber forces. The research indicates a robust and escalating trend wherein, although states may initially develop cyber capabilities for national interests, the aggregate impact of these concurrent endeavours substantially bolsters NATO's collective security framework in cyberspace.

Through this detailed comparative analysis, the paper identifies both common patterns and national distinctions in how cyber forces are conceptualised, funded, and deployed. Despite variations in maturity and structure, from highly advanced commands to newly forming units, every member state is increasingly recognising cyberspace as a domain where a military presence is essential. The study highlights the strategic convergence between national sovereignty in cyber defence and the interdependence required for effective NATO coordination, especially in light of evolving threats from adversarial actors such as the Russian Federation.

By mapping the evolution of cyber forces across the Alliance, this research not only documents current capabilities but also underscores the necessity of deeper cooperation, standardisation, and shared strategic vision. The growing role of cyber forces is not an isolated national trend, but rather a cornerstone of NATO's modern deterrence strategy, and a prerequisite for credible defence in the digital era. The findings serve as a basis for further discussion on how to align national efforts with Alliance-level objectives and how to ensure that cyber forces, though nationally controlled, operate as a unified component of NATO's broader defence ecosystem.

2. Introduction

NATO has achieved numerous milestones in the cyber domain since the advent of the digital revolution. The rapid development of the Internet (originally a military enterprise),[2] computing technologies, and innovative communication methods—culminating in the rise of virtual reality—has given rise to unprecedented security challenges.[3] Recognising that the Alliance is not immune to cyber threats, NATO has continuously developed its capabilities to strengthen responses and deter malicious activities from both state and non-state actors.[4] This proactive stance has led to the creation of cyber-related entities and the integration of cybersecurity initiatives as foundational pillars of NATO's overall operations.[5]

Events and incidents are occurring more frequently, and malicious activities in the information environment through and in cyberspace are becoming more complex, damaging, and forceful, thereby endangering the security of the Alliance. As a constant battlefield, cyberspace is exploited daily by malevolent cyber activities to support information operations (InfOps) and psychological operations (PsyOps) across a broad spectrum of technological attacks, ranging from minor disruptions to sophisticated strikes. In response, NATO and its allies are strengthening their capacity to spot, stop, and neutralise these cyber-related threats. Effective execution of NATO's main missions—which include crisis prevention and management, deterrence and defence, and cooperative security—is dependent on strong and resilient cyber defence. The Alliance must remain prepared to protect its communication and information systems (CIS) and operations against the rising sophistication of cyber-related threats.[6]

In recent years, significant emphasis has been placed on cyber capabilities. NATO allies, among others, have adopted a Comprehensive Cyber Defence Policy to support the Alliance's core tasks and strengthen its deterrence and defence posture.[7] The allies have since reaffirmed NATO's defensive mandate and pledged to use all available tools—political, diplomatic, and military—to deter, defend against, and counter cyber threats, including potential collective responses. Significant cyberattacks could, in some cases, trigger Article 5 of the North Atlantic Treaty. This policy promotes unified political, military, and technical efforts to address the evolving cyber threat landscape.[8] The allies have introduced a new concept to better integrate NATO's political, military, and technical cyber defence efforts, ensuring constant civil-military cooperation (CIMIC) and private sector engagement.[9]

---

[2] V. Brustolin, *Comparative Analysis of Regulations for Cybersecurity and Cyber Defence in the United States and Brazil*, Rev. Bras. Est. Def. v. 6, nº 2, jul./dez. 2019, p. 94.

[3] M. Pfannenstiel, D. Cox, *NATO's Cyber Era (1999–2024) Implications for Multidomain Operations,* Military Review Online Exclusive, October 2024, Army University Press.

[4] P. Fritz*, Estland war der Vorgeschmack auf das, was Europa blüht*, Welt 03.09.2024, https://www.welt.de/politik/ausland/plus253302868/Russische-Cyberattacken-Estland-war-der-Vorgeschmack-auf-das-was-Europa-blueht.html, accessed: 13.01.2025.

[5] M. Efthymiopoulos, *NATO's approach to cyber defense: Strategic foundations, challenges, and opportunities*, Journal of Innovation and Entrepreneurship, 2019, 8:12.

[6] NATO, *Cyber defence,* 30.07.2024, https://www.nato.int/cps/uk/natohq/topics_78170.htm, accessed: 12.01.2025.

[7] A. Dyner, *Russia Continuing Cyberthreats Against NATO Countries*, https://pism.pl/publications/russia-continuing-cyberthreats-against-nato-countries, PISM 21.11.2023, accessed: 13.01.2025

[8] C. Stupp, *NATO Funds Startups Aiming to Solve Cyber Problems in Infrastructure*, WSJ 10,07.2024, https://www.wsj.com/articles/nato-funds-startups-aiming-to-solve-cyber-problems-in-infrastructure-2b6aaf24?, accessed: 13.01.2025.

[9] J. Gotkowska, J. Graca, *NATO Summit in Vilnius: breakthroughs and unfulfilled hopes,*

It is imperative to enhance cyber resilience in order to mitigate the effects of cyber threats. NATO's Cyber Defence Pledge was reaffirmed by allies, who established new national objectives to safeguard critical infrastructure. Moreover, NATO's Virtual Cyber Incident Support Capability (VCISC)[10] was launched to assist national responses to major cyber incidents and is committed to building partnerships with countries, organisations, industry, and academia to enhance global cybersecurity. The growing importance of cybersecurity for NATO member states has never been more significant than it is today.[11]

The basis for the conducted research is the successive development by NATO member states of the cyber components within their armed forces or to support the cyber defence domain. Such an approach indicates the identification of challenges and threats in the field of cybersecurity, which necessitates a response at the national level; but at the same time, the element of a bigger picture where more and more NATO member states aim to develop their own cyber capabilities and, to some extent, cyber forces. We are in a time when current military development in NATO is the prelude to the development of similar cyber units or separate teams in the armies of countries belonging to the Alliance. The idea of "Cyber-profiled troops" will be crucial for competition in the coming years. NATO's hostile countries, mainly led by the Russian Federation,[12] regularly carry out harmful operations against Alliance states.

For the countries associated with NATO's CCDCOE, a questionnaire on cyber forces in individual nations was submitted.[13] Notably, only eight countries—Croatia, Greece, Latvia, Slovenia, Spain, and Sweden—provided responses, while two others chose to remain anonymous. Despite the critical importance of addressing cyber threats and advancing cyber capabilities within the NATO Alliance, many member states remain reluctant to disclose their strategies for improving cyber defence initiatives or developing NATO cyber forces. This selective participation allows for a detailed and nuanced analysis of the complexities surrounding NATO's evolving role in cybersecurity and the development of national cyber forces.

In 2016, during the summit in Warsaw, NATO officially recognised cyberspace as one of the operational domains alongside land, air, sea, and space. This was a breakthrough in the process of developing defence capabilities. However, importantly, this initiative placed a responsible task before many member states. Allies were encouraged to establish, if they hadn't already, new (cyber) components within their armed forces. Each country made an official declaration that it would build its competencies to operate in cyberspace in order to effectively defend not only itself, but also its allies.[14]

---

https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-07-13/nato-summit-vilnius-breakthroughs-and-unfulfilled-hopes, OSW 13.07.2023, accessed: 13.01.2024

[10] Cyber Express, *NATO to Bolster Cybersecurity Measures to Combat Threats for Alliance Countries*, https://thecyberexpress.com/nato-cybersecurity-threats-alliance-countries/, accessed: 13.01.2024.

[11] P. McFadden, *Putin is harnessing AI against us, minister tells Nato*, The Times 24.11.2024, https://www.thetimes.com/uk/politics/article/putin-is-harnessing-ai-against-us-minister-tells-nato-l29hjsvwz, accessed: 14.01.2024.

[12] Carnegie, *Cyber Conflict in the Russia-Ukraine War*, https://carnegieendowment.org/programs/technology-and-international-affairs/cyber-conflict-in-the-russia-ukraine-war, accessed: 23.01.2024.

[13] The Survey on NATO Cyber Forces (with the questionnaire attached) was designed to gather insights into NATO member states' cyber forces, focusing on their structure, resources, cooperation, threats, and future plans. While standardised, its open-ended questions allowed for detailed responses, making it similar to a semi-structured interview. The answers were submitted to the NATO CCD COE Strategy Branch via e-mail.

[14] This decision also placed a responsibility on NATO member states to develop or enhance their cyber defence capabilities. Member states were encouraged to establish or expand specialised components within their armed forces to operate effectively in cyberspace. The goal was to ensure that individual nations, as well as NATO as a collective organisation, could defend

Despite recognising cyberspace as a distinct operational domain, NATO member states lack a unified approach to cyber defence, with strategies varying based on national priorities, resources, and levels of technological advancement.[15] Perceiving cyberspace as an isolated fifth domain poses a risk to effective cyber deterrence and defence.[16] This divergence highlights the need for greater coordination to ensure collective security in the face of evolving cyber threats, which also includes the notion of the development of cyber forces.

2.1 Limits and constraints

As part of the research conducted, the author acknowledges the inextricable intertwining of the information and cyber environments. However, the scope of this paper is limited to the cyber component, with a focus on the development of units, divisions, departments, staffs, and branches of the armed forces whose primary responsibility is to support cybersecurity efforts. These entities fall under the broader category of cyber forces and are organised within the 32 member states of the NATO. As J. Blessing points out [17], cyber forces are active duty military units with the authority and capability to conduct strategic operations in cyberspace, with an overarching goal of influencing diplomatic or military outcomes. These operations include a wide range of activities, such as defence, exploitation, and attacks. At the same time, this definition explicitly excludes civilian intelligence services, reservist components, and military emergency readiness teams.

According to P. Pernik, the term "cyber force" typically refers to an independent entity, branch, or service within the armed forces tasked with overseeing and managing the three primary categories of cyberspace operations, specifically defence, exploitation, and attack.[18] In this regard, and after analysing the different approaches of NATO member states, it can be stated that cyber forces are organised, government-sanctioned military or paramilitary components specialising in conducting defensive and offensive operations in the cyber domain, which are aimed at protecting national security and achieving strategic objectives. Nevertheless, they may also include officially tasked civilian or volunteer groups operating under government authority during specific missions.

Ultimately, in most NATO nations, cyber forces constitute a specialised and distinct element within the military. Although structures may differ, it is generally accepted that cyber forces are military entities, functioning as specialised units within national armed forces.

---

against and respond to cyber threats, which could potentially impact critical infrastructure, military operations, and national security.

[15] A. Marrone, E. Sabatino, *Cyber Defence in NATO Countries: Comparing Models*, Istituto Affari Internazionali (IAI), February 2021, p. 2.

[16] A. Ertan, K. Floyd, P. Pernik, T. Stevens, *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, NATO CCDCOE, 2020, s. 127-128.

[17] J. Blessing, *The Global Spread of Cyber Forces, 2000–2018*, 13th International Conference on Cyber Conflict Going Viral T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.) 2021, NATO CCDCOE Publications, Tallinn, pp. 235-237.

[18] P. Pernik, *NATO's Cyber Deterrence: Policy and Capability in the Context of Collective Defence*, International Centre for Defence and Security, June 2016, https://icds.ee/wp-content/uploads/2016/Piret_Pernik_-_NATO_s_Cyber_Deterrence__June_2016.pdf, accessed: 21.01.2025.

There is a clear lack of consistency between how states and organisations define and approach cyber defence and cybersecurity. States often do not follow the frameworks or standards used by organisations, which can seriously impact the effectiveness of coordinated cyber defence efforts.[19]

It is important to note that NATO distinguishes between national defensive and offensive cyber capabilities, which remain under national control during peace and war. Instead of exercising direct control, NATO plays a crucial role in coordinating efforts and establishing standards to ensure interoperability and collective defence. Additionally, member states voluntarily contribute their offensive cyber capabilities to NATO when required, while retaining command-and-control (C2) over these units. At the same time, international law, the security of national systems, and coordination with allies remain essential considerations. This article focuses on how NATO member states are developing their cyber components, which, depending on the definition, can be referred to as cyber forces. It also assesses the current stage of development in individual countries and examines the expansion of entities that are, or may eventually be, classified as cyber forces.

The author limits the scope to a general description of each country, focusing on the development and evolution of entities responsible for the cyber domain, to highlight the growing importance of cyber forces for both NATO member states and their adversaries. The extant literature lacks up-to-date materials that comprehensively cover all 32 NATO member states and examine the opportunities and challenges related to the organisation of cyber forces. Additionally, the study explores the development of the cyber domain and the command-and-control system (C2 System) within the Alliance, providing conclusions that serve as a foundation for further research on the development of cyber forces. However, the author does not address the detailed cooperation between NATO member states in the framework of cyber exercises or analyse NATO–EU collaboration, and the typology of cyber force structures, based on the organisational models of each country, is only partially discussed.[20] The review of the current level of development of cyber capabilities serves as a starting point for further research, especially as cyberspace has become a domain of rivalry where conflicts can take place.

Moreover, the author intentionally constrained the research's scope, opting not to investigate the roles and responsibilities of the public and private sectors, nor the activities of cyber forces in both wartime and peacetime. Furthermore, accurate information regarding the composition of cyber forces in each nation, encompassing their distinct roles and responsibilities, could not be acquired. The concept of CIMIC, the roles of industry and academia, and the nature of cooperation with other governmental entities could not be defined in a granular manner. These elements are to be examined in subsequent research.

Regrettably, it is important to highlight that much of the data crucial for the development of cyber forces within NATO countries—such as decisions regarding force development, personnel, budgets, operating costs, doctrine, capability acquisitions, the scale of hostile attacks, cooperation with other member countries, political support, information on defensive and offensive actions, partnerships with the private sector, and future improvement goals—remains unpublished, inconsistently documented, or otherwise classified. This analysis is grounded in systematic

[19] D. Štrucl, *Comparative study on the cyber defence of NATO Member States*, Tallinn 2021, p. 23.

[20] More about typology of cyber force structures with regards to: Subordinated Branch, Subordinated Service, Subordinated Joint, Sub-Unified Branch, Sub-Unified Service, Sub-Unified Joint, Unified Branch, Unified Service, Unified Joint. More: J. Blessing, *The Global Spread of Cyber Forces, 2000–2018*, 13th International Conference on Cyber Conflict Going Viral T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.) 2021, NATO CCDCOE Publications, Tallinn, pp. 238-239.

and empirical analysis, drawing from a diverse range of sources, including online publications, media reports, peer-reviewed studies, official government documents, and institutional reports, as well as consultations with experts in cybersecurity and defence. It is important to note that such open-source data may contain errors. Further, the author analysed cyber forces in each of the 32 NATO member states, utilising national sources to validate their development, where the language barrier also posed a challenge.

2.2 Research approach

Currently, with ongoing geopolitical tensions, the need to develop military capabilities in the cyber domain is germane. Cyberspace has become an arena of conflict with its own battles and wars. Observing the situation in Ukraine or the Gaza Strip, it is evident how significant a role cyber operations play in contemporary state rivalries. NATO countries have entered a stage where, in cyberspace, it is more common to experience rivalry, conflict, and the possibility of war rather than lasting peace.

The line between an 'act of war' and 'active influence' is often blurred and perceived as hybrid warfare, which includes political warfare and activities in so-called "grey zones" (*i.e.*, those falling below the threshold of war). As such, these are difficult to define, further complicating any discussion about the roles of military force within cyberspace. At times, kinetic warfare is concurrently supported in cyberspace.[21] Various states, and Russia in particular, are attempting to use this to tip the international balance of power to their advantage. What this means for future warfare is unclear, and international actors still appear to be configuring how this new technology changes the dynamics.[22] Some affirm that strict informational attacks cannot rise to the level of an armed attack, since they lack "the physical characteristics traditionally associated with military coercion,"[23] despite the impact such attacks have on the physical domain. Therefore, the majority do not support this approach "as dangerously outdated, because cyber attacks have the potential to cause catastrophic harm without employing traditional military weapons."[24]

In the context of national security development and, concurrently, the evolution of cyber forces, it is imperative to focus on additional elements that serve as foundational pillars for enhancing resilience in cyberspace. Consequently, this research provides a concise overview of national cybersecurity frameworks, focusing on their structural configurations, developments, and key future objectives. The primary aim of this study is to examine the cyber forces of specific NATO member states, focusing on their history, evolution, current structure, and responsibilities, with regard to the challenges they face, given that the use and creation of cyber forces will undoubtedly continue to increase.[25]

The research hypothesis will assume the following characteristics: *Growing numbers of NATO members are improving their cyber-capability by establishing specialised cyber forces among other aspects.*

[21] A. Olech, *Izrael-Palestyna. Rywalizacja w cyberprzestrzeni zaognia się*, https://cyberdefence24.pl/cyberbezpieczenstwo/izrael-palestyna-rywalizacja-w-cyberprzestrzeni-zaognia-sie, accessed: 17.03.2025.

[22] G. Noel, M. Reith, *Cyber Warfare Evolution and Role in Modern Conflict*, Journal of Information Warfare, 20th Anniversary Edition, Peregrine Technical Solutions, Vol. 20, No. 4 (Fall 2021), p. 30–44.

[23] D. Hollis, *Why States Need an International Law for Information Operations*, Lewis & Clark Law Review 11, no. 4 (2007), pp. 1023–1061.

[24] Oona A. Hathaway et al., *The Law of Cyber-Attack*, California Law Review 100, no. 4 (2012), pp. 817–885.

[25] U. Pagallo, *Cyber Force and the Role of Sovereign States in Informational Warfare*, Springer Science+Business Media, received 31 March 2014, accepted 7 October 2014, p. 9.

Although not every member state has established such units, there is a clear trend toward expansion, especially in the wake of Russia's invasion of Ukraine. The continued strengthening of cyber forces will significantly contribute to their evolution within NATO countries, enhancing their ability to address emerging threats. This, in turn, reinforces cyberspace as a vital domain of modern conflict and cooperation, as challenges in this sphere grow increasingly complex.

The research problems in this study are formulated as follows: *What is the structure and role of entities responsible for cyber defence in NATO member states that are crucial to the development of cyber forces? Which NATO member states have developed dedicated cyber forces? Has the number of hostile cyberattacks increased in recent years? How do NATO member states with established cyber forces differ in their approaches and capabilities compared to those without?*

To address these questions, a qualitative research method has been employed, focusing on the structure and role of entities responsible for cyber defence within NATO member states. This approach examines how these entities contribute to the development of cyber forces and assesses the differences between NATO member states that have established cyber forces and those that have not. The study also explores the impact of hostile cyberattacks on the evolution of cyber defence strategies. Using an interdisciplinary approach, the research evaluates the varying capabilities and strategies of NATO countries, analysing the development of their cyber forces in response to emerging threats. The analysis includes a comparative review of cyber defence structures and strategies across NATO nations, identifying best practices and challenges in the context of global cybersecurity dynamics.

3. Historical context of NATO cyber initiatives

As the digital and electronic landscape advanced with the rise of the Internet, computing technologies, and CIS, NATO consistently evolved to address the increasing cybersecurity threats posed by both state and non-state actors. Aware of its own infrastructure's vulnerabilities, the Alliance took proactive steps to establish specialised cyber defence capabilities to safeguard its operations and collective security. Examining the historical development of NATO's cyber initiatives offers valuable perspective on how the organisation has tackled the complexities of cyberspace, laying the groundwork for the creation of dedicated cyber forces and integrated defence strategies.[26]

NATO has achieved numerous groundbreaking accomplishments in the field of cybersecurity over the years. The rapid development of the Internet, computing technologies, and innovative communication and information methods—culminating in the emergence of virtual reality—has led to unprecedented security challenges. In particular, the latest technological breakthrough in the form of artificial intelligence (AI) raises concerns about its potential use for combat purposes.[27] NATO has continuously developed its cyber capabilities through the establishment of specialised entities, such as the NATO Communications and Information Agency (NCIA), and the integration of cybersecurity initiatives as fundamental pillars of NATO's operational areas.[28]

3.1 Early cyber threats and NATO's initial responses

A significant early example of NATO encountering cyber conflict occurred during the 1999 Kosovo Operation. Activists and hackers sympathetic to Serbia targeted NATO's digital infrastructure through website defacements, virus-laden emails, and distributed denial-of-service (DDoS) attacks. These actions, which aimed to disrupt NATO's operations, highlighted the vulnerabilities of military communication systems in the digital age.[29] This experience underscored the necessity for robust cyber defences and laid the groundwork for NATO's commitment to improving cybersecurity across the Alliance.[30]

NATO has always prioritised the security of CIS, but it was during the Prague Summit in 2002 that cybersecurity was formally recognised as an emerging political priority for the Alliance.[31] This strategic focus was reinforced at the Riga Summit in 2006, where Alliance leaders highlighted the urgent need to strengthen NATO's information

[26] J. Healey, K. T. Jordan, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow,* Atlantic Council, Brent Scowcroft Center on International Security, 2014, https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf, accessed: 13.01.2025.
[27] C. Caruso, *The Risks of Artificial Intelligence in Weapons Design, Harvard Medical School*, https://hms.harvard.edu/news/risks-artificial-intelligence-weapons-design, accessed: 13.01.2025.
[28] R. Mariano, *L'OTAN va bâtir un immense centre de cybersécurité : voici le projet*, 17.07.2024, https://www.lebigdata.fr/l-otan-va-batir-un-immense-centre-de-cybersecurite-voici-le-projet, accessed: 13.01.2025.
[29] J. Healey, *Cyber Attacks Against NATO, Then and Now,* Atlantic Council, 06.09.2011, https://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now, accessed: 20.12.2024.
[30] D. Deschaux-Dutard, *Is NATO ready for cyber war?*, https://frstrategie.org/en/publications/nato-briefs-series/nato-ready-cyber-war-2021, accessed: 10.12.2024.
[31] NATO Press Releases, *Prague Summit Declaration*, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague on 21 November 2002, https://www.nato.int/docu/pr/2002/p02-127e.htm, accessed:10.12.2024.

infrastructure against increasingly sophisticated digital threats.[32] The necessity for decisive action became evident after the large-scale cyberattacks on Estonia in 2007, which targeted both government institutions and private sectors.[33] This incident marked the beginning of NATO's intensified focus on cybersecurity, leading to the adoption of the first Cyber Defence Policy in January 2008.[34] This policy initiated a more unified and proactive approach to mitigating cyber threats across the Alliance.

3.2 From Estonia to the CCDCOE: Building cyber resilience

In the aftermath of the 2007 cyberattacks on Estonia, in 2008 NATO accredited the Cooperative Cyber Centre (CCDCOE) in Tallinn, Estonia, with the tasks of strengthening expertise in cyber defence and enhancing the Alliance's collective resilience against cyber threats.[35] In addition, the Russo-Georgian war underscored the need to enhance cyber capabilities, as conventional military operations were supported by cyber actions.

The CCDCOE has since become a critical hub for advancing NATO's cybersecurity efforts, offering expertise through research, training, and live cyber defence exercises. The Centre supports NATO in developing strategic frameworks, legal, operations, strategic and technical research, and through education, training and exercises.[36] Notably, the CCDCOE initiatives, including Locked Shields[37] (the world's largest live-fire cyber defence exercise) and the compilation of the *Tallinn Manual*[38] (a leading reference on how international law applies to cyber operations), have significantly contributed to strengthening NATO's collective cyber resilience.[39]

Over 16 years, the Centre has grown from an initial seven members[40] to thirty-two sponsoring nations and seven contributing participants. CCDCOE hosts annual exercises such as Locked Shields and Crossed Swords, which bring together NATO members and partner countries to enhance their collective cyber defence capabilities. Another recurring training operation under the CCDCOE's supervision is NATO Cyber Coalition Exercise, which focuses on improving coordination and preparedness for cyber incidents

[32] Eesti NATO Ühing, *Cyber defence*, https://www.eata.ee/en/nato/cyber-defence, accessed: 10.12.2024.
[33] R. Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, NATO CCD COE, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, accessed:10.12.2024.
[34] European Parliament, *NATO's Approach to Cyber Defence: Policy and Strategy, SEDE Committee Meeting Document,* 25.10.2010, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf, accessed: 12.10.2024.
[35] NATO, *NATO opens new centre of excellence on cyber defence*, 14.05.2008, https://www.nato.int/docu/update/2008/05-may/e0514a.html, accessed: 12.12.2024.
[36] More about the NATO CCD COE: https://ccdcoe.org/about-us
[37] ERR News, *Locked Shields cyber defense exercise kicks off in Tallinn*, https://news.err.ee/1609322628/locked-shields-cyber-defense-exercise-kicks-off-in-tallinn, accessed: 12.12.2024.
[38] CCD COE, *The Tallinn Manual*, https://ccdcoe.org/research/tallinn-manual, accessed: 13.12.2024.
[39] Wojsko Polskie, *Locked Shields 2024*, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2024-04-243-locked-shields-2024/, accessed: 13.12.2024.
[40] The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established on 14 May 2008 by seven founding nations: Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, and Spain.

across member states. Additional, CCDCOE organises an annual Cyber Conference (CyCon), which brings together global cyber-related experts.

The evolving nature of cyber threats was further highlighted during the 2008 Russia-Georgia conflict, where cyberattacks were effectively used alongside conventional military tactics. This event underscored the role of cyber warfare as a critical element of hybrid conflict.[41] NATO responded by embedding cybersecurity with its strategic framework through the 2010 Lisbon Summit's Strategic Concept, which explicitly recognised cyberattacks as a potential threat to national and Euro-Atlantic security. This policy direction was solidified in June 2011 when NATO Defence Ministers approved a second Cyber Defence Policy, emphasising coordinated cyber defence across the Alliance.[42] By April 2012, cybersecurity had been fully integrated into NATO's Defence Planning Process, ensuring that cyber capabilities are prioritised alongside traditional defence measures.

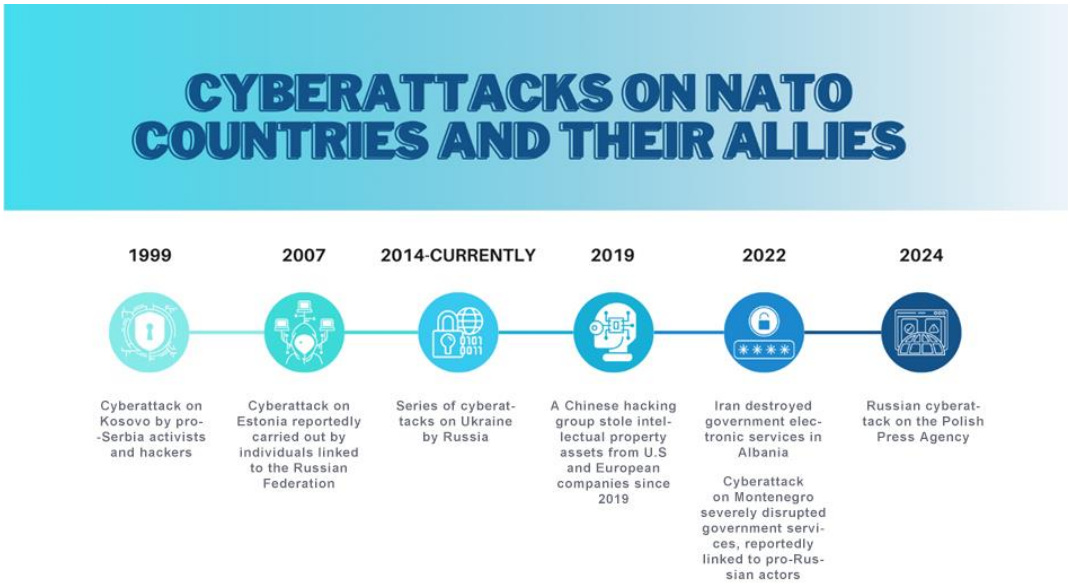


FIGURE 1. KNOWN CYBERATTACKS ON NATO COUNTRIES AND THEIR ALLIES

3.3 Cyberspace as a critical operational domain

This strategic evolution was further cemented at the 2012 Chicago Summit, at which allied leaders committed to centralising network protection and enhancing NATO's cyber defence capabilities.[43] The establishment of the NCIA in 2012 streamlined cyber and communication operations, enabling the Alliance to better manage emerging cyber threats.[44] A landmark moment occurred at the 2014 Wales Summit, where NATO formally recognised cyber defence as a core component of collective defence. This

[41] S. White, *Understanding Cyberwarfare: Lessons from the Russia-Georgia War*, Modern War Institute 20.03.2018, accessed: 14.12.2024.
[42] NATO, *NATO Defence Ministers adopt new cyber defence policy*, https://www.nato.int/cps/en/natohq/news_75195.htm, accessed: 14.12.2024.
[43] NATO, *Chicago Summit Declaration*, https://www.nato.int/cps/en/natohq/official_texts_87593.htm, accessed: 14.12.2024.
[44] NATO, *NATO Communications and Information Agency (NCI Agency)*, https://www.nato.int/cps/en/natohq/topics_69332.htm, accessed: 14.12.2024.

critical decision meant that severe cyber attacks could now trigger Article 5 of NATO's founding treaty, placing cyber threats on par with conventional military threats.[45] Additionally, allies affirmed that existing international law (*lex lata*) fully applies to cyberspace. Recognising the value of public-private collaboration, NATO launched the NATO Industry Cyber Partnership (NICP) in 2014 to strengthen ties with industry in addressing cyber challenges,[46] notably information sharing, cyber threat landscape analysis, standards development, R&D, PUB-PRI cooperation, malware information sharing platform (MISP), and industry engagement, etc.

International collaboration remained central to NATO's cybersecurity strategy. In 2016, NATO and the European Union formalised their partnership[47] through a technical arrangement between the NATO Computer Incident Response Capability (NCIRC) and the EU's Computer Emergency Response Team (CERT-EU), enhancing joint cyber incident responses.[48] At the 2016 Warsaw Summit, NATO declared cyberspace an operational domain, aligning it with land, air, and sea operations. This recognition was complemented by the Cyber Defence Pledge, in which allies committed to strengthening national cyber defences, protecting critical infrastructures, and improving resilience against hybrid threats.[49]

3.4 Strengthening partnerships and collaboration

The Berlin Plus Agreement, formalised in 2003, must also be mentioned. It was a security arrangement between the EU and NATO, establishing a framework for NATO to provide the EU with access to its military assets and capabilities for EU-led operations in cases where NATO chooses not to act. Later, the 2016, 2018 and 2023 EU-NATO joint declarations further emphasised the importance of tackling cyber threats collaboratively.

NATO has since strengthened its efforts to counter cyber threats through close cooperation with the EU Hybrid Centre of Excellence (Hybrid COE),[50] addressing the interconnected nature of hybrid and cyber threats across virtual and physical domains. Both NATO and the EU rely on each other for security, as the EU needs NATO for military deterrence, while NATO benefits from the EU's contributions to European defence capabilities. The EU's broader competencies help tackle hybrid threats, while NATO's military power is complemented by the EU's diplomatic and economic tools for stabilising the Euro-Atlantic region. Both organisations also recognise the importance of working with non-member states to ensure regional and global security. In response to the evolving security environment, NATO and the EU have repeatedly reaffirmed their commitment to strengthening resilience against hybrid and cyber threats, as illustrated in Figure 2.

[45] NATO, *Wales Summit Declaration*, https://www.nato.int/cps/en/natohq/official_texts_112964.htm, accessed: 14.12.2024.
[46] NCIA, *NATO Industry Cyber Partnership*, https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership, accessed: 15.12.2024.
[47] A. Olech, *Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism*, https://ine.org.pl/wp-content/uploads/2021/03/Cooperation-between-NATO-and-the-European-Union-against-hybrid-threats-with-a-particular-emphasis-on-terrorism.pdf, accessed: 15.12.2024.
[48] NATO, *NATO and the European Union enhance cyber defence cooperation*, https://www.nato.int/cps/en/natohq/news_127836.htm, accessed: 15.12.2024.
[49] NATO, *Warsaw Summit Communiqué*, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, accessed: 15.12.2024.
[50] Hybrid COE, *EU and NATO welcome Hybrid CoE*, https://www.hybridcoe.fi/news/eu-and-nato-welcome-hybrid-coe, accessed: 20.12.2024.

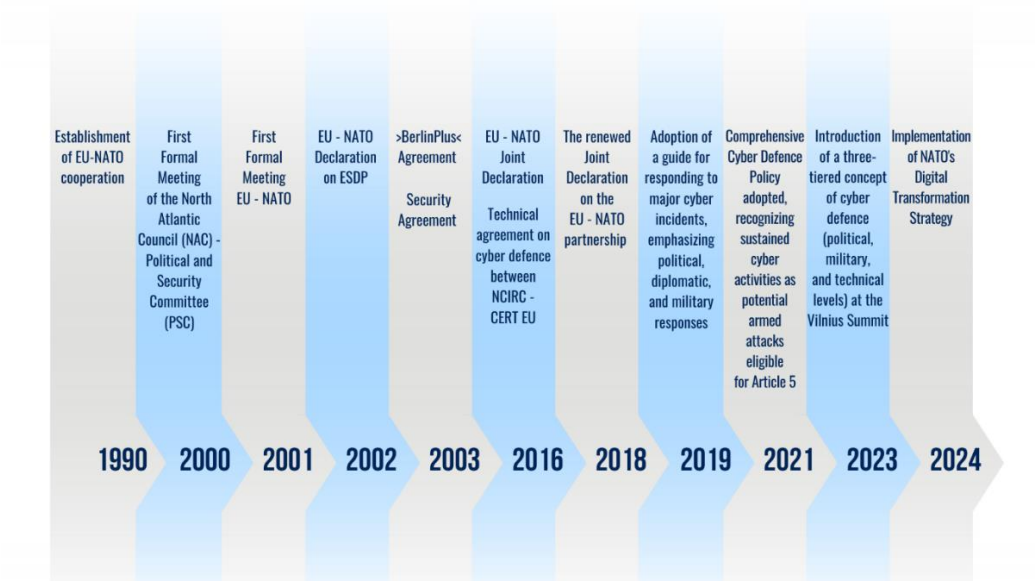


FIGURE 2. EVOLUTION OF THE EU-NATO PARTNERSHIP.[51]

In February 2017, NATO approved an updated Cyber Defence Action Plan and roadmap to operationalise cyberspace as a defence domain.[52] That same year, NATO signed a Political Framework Arrangement on cyber defence cooperation with Finland, strengthening network security—a partnership that deepened when Finland joined NATO in 2023. Sweden also bolstered its cyber collaboration by joining NATO's CCDCOE in 2015 and further integrating into NATO's cyber defence framework upon becoming a full member in 2024.[53]

The 2018 Brussels Summit introduced the NATO Cyberspace Operations Centre, designed to improve situational awareness and coordinate cyber operations across the Alliance.[54] NATO's cyber strategy continued to evolve, notably with the 2019 adoption of a guide outlining tools for responding to major cyber incidents, emphasising the need to use political, diplomatic, and military responses.[55]

3.5 Recent cybersecurity milestones: 2021–2024

In summary, NATO's 2021 Brussels Summit marked a pivotal advancement in the Alliance's approach to cyber defence. By adopting a Comprehensive Cyber Defence Policy, NATO acknowledged that significant malicious cyber activities could, under certain circumstances, be considered equivalent to an armed

[51] Adapted from D. Štrucl, The EU-NATO partnership and ensuring information security and cybersecurity: theory and practice, Sodobni vojaški izzivi/Contemporary Military Challenges, Vol. 23(issue 2), p. 33.
[52] Lillian Ablon et al., *Operationalizing Cyberspace as a Military Domain: Lessons for NATO*, RAND Corporation, 2019, https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND_PE329.pdf, p. 42, accessed:: 15.12.2024.
[53] M. Pfannenstiel, D. Cox, *NATO's Cyber Era (1999–2024) Implications for Multidomain Operations*, Military Review Online Exclusive · October 2024, Army University Press.
[54] NATO CCD COE, *Cyber defence at the 28th NATO Summit in Brussels*, 11-12 July 2018, https://ccdcoe.org/incyder-articles/cyber-defence-at-the-28th-nato-summit-in-brussels-11-12-july-2018, accessed: 16.12.2024.
[55] M. Maigre, *NATO's Role in Global Cyber Security*, GMF 06.04.2022, https://www.gmfus.org/news/natos-role-global-cyber-security, accessed: 16.12.2024.

attack, potentially triggering Article 5 of the North Atlantic Treaty.[56] This policy also emphasised the importance of enhanced political consultations among allies to address and respond to cyber threats collectively. Additionally, the establishment of the Defence Innovation Accelerator for the North Atlantic (DIANA) underscored NATO's commitment to fostering innovation by supporting early-stage companies developing dual-use technologies in areas such as energy, cybersecurity, and communications systems.[57]

In September 2021, the North Atlantic Council appointed NATO's first Chief Information Officer (CIO).[58] North Macedonia signed a key memorandum of understanding (MoU) that will improve cyber defence cooperation and assistance between NATO and Skopje.[59] A programme to enhance Mongolia's cyber defence capabilities has been successfully completed.[60] It was assured that NATO will support Ukraine's cyber defence,[61] and Ukraine is taking part in various events organised by NATO in the field of cyber defence, including integration within the framework of the NATO CCDCOE.

At the 2023 Vilnius Summit, it was agreed to introduce a three-tiered concept of cyber defence, namely establishing political, military and technical levels. The war in Ukraine and hostile actions by the Russian Federation against NATO member states after 2022 led to ambitious goals for strengthening national cyber defence systems. The leaders also announced the first comprehensive NATO Cyber Defence Conference in Berlin in November 2023.

The Alliance also expanded the Cyber Defence Pledge, focusing on ambitious goals for protecting national critical infrastructure. Recognising the need for rapid support, NATO launched the VCISC to assist member states in managing significant cyber incidents.[62] NATO capped the year with its first Comprehensive Cyber Defence Conference in Berlin, uniting political, military, and technical leaders to enhance collaborative defence strategies.[63]

Culminating these efforts, the 2024 Washington Summit marked a turning point with the establishment of the NATO Integrated Cyber Defence Centre (NICC) at the Supreme Headquarters Allied Powers Europe (SHAPE). This state-of-the-art facility enhances network security, improves situational awareness, and fully integrates cyberspace as an operational domain.[64] NATO has since agreed to establish the NICC at SHAPE in Belgium. The new Centre will focus on providing relevant threat information to improve military decision-making, as well as “enhancing our situational awareness in cyberspace and strengthening collective resilience and defence”.[65]

---

[56] NATO, *Brussels Summit Communiqué*, https://www.nato.int/cps/en/natohq/news_185000.htm, accessed: 16.12.2024.
[57] DIANA, *Defence Innovation Accelerator for the North Atlantic Uniting disruptors to shape a peaceful future*, https://www.diana.nato.int/, accessed: 08.01.2025.
[58] NATO, *Cyber defence*, July 30, 2024, https://www.nato.int/cps/de/natohq/topics_78170.htm, accessed: 08.01.2025.
[59] NATO, *NATO and North Macedonia strengthen responses to cyber threats*, July 2, 2021, https://www.nato.int/cps/en/natohq/news_181656.htm, accessed: 08.01.2025.
[60] NATO, *NATO helps to strengthen Mongolia’s cyber defence capacity*, January 18, 2021, https://www.nato.int/cps/en/natohq/news_180697.htm, accessed: 08.01.2025.
[61] NATO, *Deputy Secretary General stresses NATO will continue to increase Ukraine’s cyber defences*, January 25, 2022, https://www.nato.int/cps/en/natohq/news_191143.htm, accessed: 08.01.2025.
[62] NATO, *Vilnius Summit Communiqué*, https://www.nato.int/cps/ge/natohq/official_texts_217320.htm, accessed: 17.12.2024.
[63] NATO, Secretary General: Through NATO, we can build a secure cyberspace for all, https://www.nato.int/cps/en/natohq/news_219850.htm, accessed: 18.12.2024.
[64] NATO, *Allies agree new NATO Integrated Cyber Defence Centre*, https://www.nato.int/cps/en/natohq/news_227647.htm, accessed: 18.12.2024.
[65] NATO, *Cyber defence*...

NATO published its first Quantum Technology Strategy, detailing its ambitions to become an "Alliance ready for quantum technologies". On November 13, 2024, a plenary meeting of NATO's Transatlantic Quantum Community concluded in Copenhagen.[66]

NATO's cyber defence capability now includes 24/7 Cyber Rapid Reaction Teams and hands-on training facilitated through exercises like Locked Shields and Cyber Coalition, supported by the NATO CCDCOE in Estonia. Education is provided through advanced programmes at the NATO Communications and Information Academy in Portugal, the NATO School in Germany, the NATO Defence College in Italy, and the NATO CCDCOE in Estonia. These initiatives ensure that NATO's strategic, operational, tactical/technical and policy development in cybersecurity remains strong and adaptable.[67]

The EU and NATO held their first structured dialogue on cybersecurity on October 4, 2024, which was aimed at strengthening cooperation on cyber defence.[68] This was followed by the annual Cyber Coalition exercise, whose 2024 edition emphasised advanced threat scenarios such as ransomware attacks, state-sponsored cyber intrusions, and breaches of critical infrastructure, many of which were based on lessons learned from the war in Ukraine.[69] During these exercises, Allied Command Transformation, in cooperation with Allied Command Operations and Joint Force Command Naples, led an experimental campaign on Cyberspace Situational Awareness. This initiative is crucial, as it enhances NATO's cognitive advantage in responding to cyberattacks while complementing other ongoing exercises such as Locked Shields.

A set of measures was agreed upon to counter Russia's hostile and cyber activities,[70] including increased intelligence sharing, more exercises, better protection of critical infrastructure, improved cyber defence and tougher action against Russian oil-exporting vessels,[71] yielding fresh opportunities for cooperation.[72]

On the 31st of July, 2024, NATO marked the launch of a $2.5 million project under which the Alliance plans to reroute data to space, fearing that Russia could cut undersea Internet cables. This initiative is partially funded by NATO's Science for Peace and Security (SPS) programme. The project aims to produce a working prototype within two years, with a demonstration planned at the Blekinge Institute of Technology. Leading the project, the Hybrid Space/Submarine Architecture Ensuring INFOSEC of Telecommunications (HEIST) consortium aims to develop a hybrid network combining submarine cables and satellite communications to ensure

[66] NATO, *NATO quantum experts gather in Copenhagen for annual conference*, November 14, 2024, https://www.nato.int/cps/de/natohq/news_230539.htm?selectedLocale=en, accessed: 08.01.2025.
[67] NATO, *Cyber defence*, 30.07.2024, https://www.nato.int/cps/uk/natohq/topics_78170.htm, accessed: 13.01.2025.
[68] The Diplomatic Service of the European Union, *European Union and NATO hold the first Structured Dialogue on Cyber*, October 4, 2024, accessed: 08.01.2025.
[69] Joint Force Command Brunssum, *Cyber Coalition 2024: Strengthening NATO's Cyber Defence*, December 6, 2024, https://jfcbs.nato.int/page5964943/2024/cyber-coalition-2024--strengthening-natocyber-defence, accessed: 08.01.2025.
[70] D. Strucl, *Russian aggression on Ukraine: cyber operations and the influence of cyberspace on modern warfare*, Sodobni vojaški izzivi/ Contemporary Military Challenges, June 2022 – 24/No. 2.
[71] NATO, *NATO Foreign Ministers chart way forward in addressing Russian sabotage*, December 4, 2024, https://www.nato.int/cps/de/natohq/news_231006.htm?selectedLocale=en, accessed: 08.01.2025.
[72] NATO, *NATO Allies and Indo-Pacific Partners discuss cybersecurity cooperation*, September 5, 2024, https://www.nato.int/cps/de/natohq/news_228454.htm?selectedLocale=en, accessed: 08.01.2025.

a continuous flow of data. It will bring together existing technologies, in addition to addressing legal and jurisdictional challenges.[73]

It must be underscored that key milestones in NATO's cybersecurity evolution include the full implementation of NATO's Digital Transformation Strategy in 2024.[74] Through continuous adaptation, strategic partnerships, and robust policy frameworks, NATO remains steadfast in defending the Alliance against the increasingly complex cyber threats of the modern era.

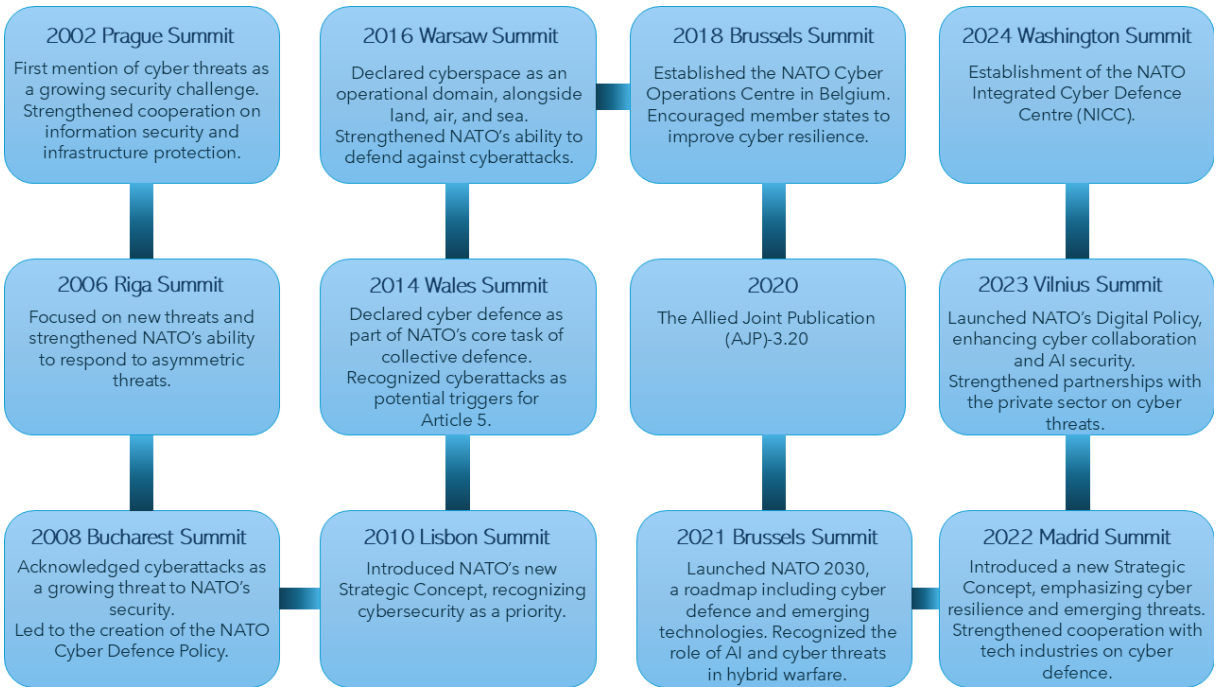


FIGURE 3. NATO CYBER INITIATIVES.

Concurrently, NATO oversees various international activities being developed by individual nations. These include strengthening national armed forces and building cyber forces, and these have become a crucial element of cooperation between NATO and its partners. While responding to cyber threats is one aspect, developing independent defence cyber capabilities within each nation is also a key part of NATO's evolving cyber strategy. This shift reflects the challenges NATO faces in the new cyber era as it confronts malicious actors,[75] prompting reflection on how cyber forces are becoming increasingly crucial for countries in enhancing their ability to respond.

[73] NATO, *NATO-funded project to reroute internet to space in case of disruption to critical infrastructure*, July 31, 2024, https://www.nato.int/cps/en/natohq/news_228257.htm, accessed: 08.01.2025.
[74] NATO, *NATO's strategy for digital transformation,* https://www.nato.int/cps/en/natohq/news_229985.htm, accessed: 13.01.2025.
[75] D. Michaels, A. Cullison, *As Russia and China Rewrite Rules of War, NATO Adapts Its Game Plan*, WSJ 8.12.2024, https://wsj.com/world/europe/as-russia-and-china-rewrite-rules-of-war-nato-adapts-its-game-plan-76432a2e, accessed: 19.12.2024.

4. NATO's command-and-control in cyber forces coordination

NATO does not directly command or manage the cyber forces of individual member countries; instead, it plays a pivotal role in coordinating and setting standards to ensure interoperability and collective defence. Each member nation is responsible for organising, equipping, and managing its own cyber forces, developed based on national priorities, resources, and threat assessments. To facilitate effective collaboration, NATO has established frameworks, doctrines, and policies for collective cyber defence. For instance, the Cyber Defence Pledge commits member states to enhancing their national cyber defences.[76]

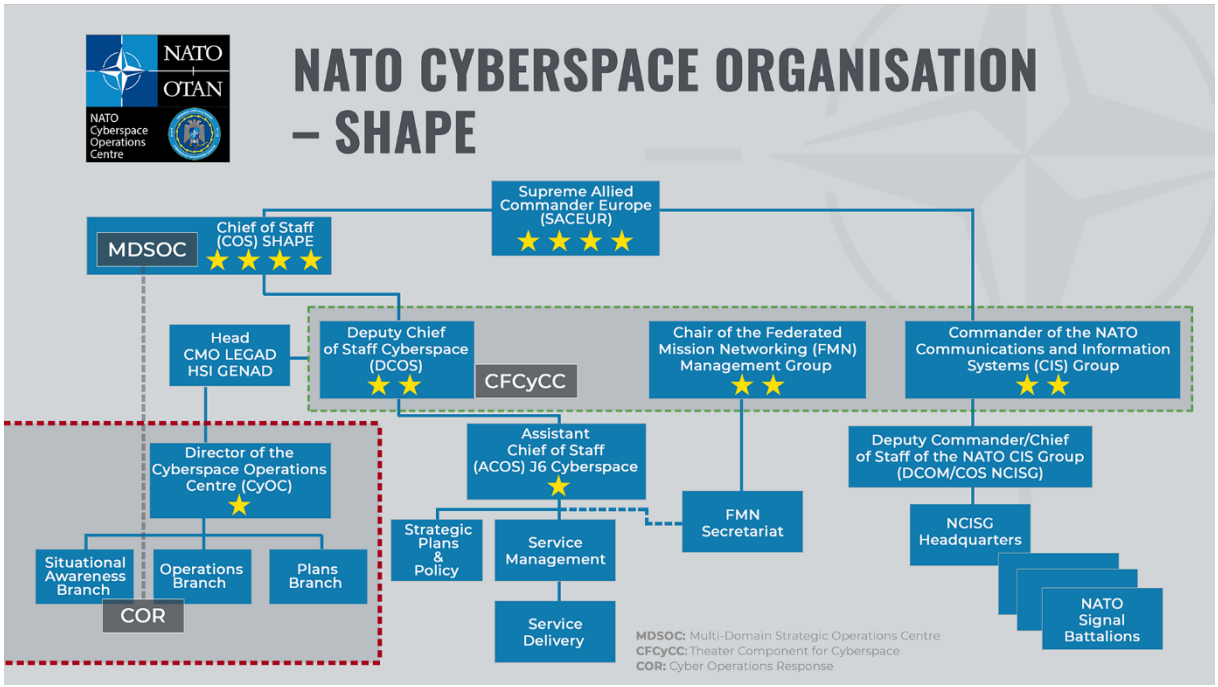


FIGURE 4. ORGANISATION OF NATO CYBERSPACE – SHAPE[77]

NATO's C2 System[78] framework enables effective coordination and synchronisation of national cyber forces, ensuring cohesive responses to cyber threats across member nations. Such exercises as Cyber Coalition provide a vital platform for testing and enhancing the interoperability of national cyber forces. By simulating real-world scenarios, these exercises refine NATO's C2 systems and align national efforts with broader Alliance missions.[79] Such initiatives ensure cohesive and effective responses to cyber threats

[76] NATO, *Cyber Defence Pledge*, https://www.nato.int/cps/en/natohq/official_texts_133177.htm, accessed: 12.12.2024.
[77] NATO's perspective on Cyberspace Operations, NIC Nikos FOUGIAS, CyOC PLANS RDN, 2/6/2025, p. 18
[78] Refers to the systems, processes, and structures through which NATO coordinates, directs, and synchronises military operations across its member nations. It enables the effective planning, execution, and monitoring of multinational operations to achieve NATO's strategic objectives.
[79] NATO, *NATO Cyber Operation Centre*, https://nrdc-ita.nato.int/operations/allied-reaction-force/nato-cyber-operation-centre, accessed: 12.12.2024.

while respecting the sovereignty of member states.[80] The integration of cyber-specific protocols within C2 processes further highlights NATO's commitment to addressing the unique challenges posed by cyberspace.[81]

C2 within NATO's framework is crucial for coordinating and directing military operations across member nations. It encompasses the processes by which forces are synchronised, managed, and controlled to achieve strategic objectives. By focusing on optimising processes, organisational structures, and knowledge management, while addressing the critical role of leadership, the C2COE strengthens NATO's ability to adapt its command structures to evolving operational challenges.[82]

While NATO's cyber capabilities enhance combat effectiveness, adversaries can exploit vulnerabilities in military platforms, networks, and supply chains through cyber espionage and manipulation. In 2019, NATO recognised (outer) space as an operational domain. This decision has significant implications for cyberspace, as the two domains increasingly overlap.[83] C2 systems rely heavily on space assets for data collection and distribution, making cyber or physical attacks on satellites and ground stations a significant threat to strategic weapon systems and early warning mechanisms. Adversaries such as Russia, China, and Iran employ asymmetric tactics to operate below the threshold of armed conflict, posing complex challenges for NATO. A critical issue is the systematisation of multi-domain operations (MDOs), as political differences deepen divides in legal frameworks, strategic cultures, threat perceptions, and resources among allies.

Additionally, defining the scope of cooperation between member states and the US in cyber architecture remains contentious, as EU countries seek to balance reliance on American systems, domestic solutions, and broader international collaboration. Smaller states also face the challenge of influencing larger allies while addressing their own capability gaps within the cyber domain. As of 2025, researchers and policy experts still encounter difficulties accessing certain unclassified NATO data, despite its importance for informed analysis and for strengthening societal resilience across the Alliance.[84]

Individual NATO member states develop and maintain their own cyber forces tailored to their specific national security needs and resources. However, with NATO's support, these national cyber forces benefit from shared expertise, training, and frameworks that enhance their capabilities and ensure they can operate effectively as part of the Alliance.[85] This collaborative approach allows NATO to leverage the strengths of individual member nations while providing a unified defence posture against cyber threats. Through its robust C2 framework and collaborative initiatives, NATO not only strengthens the cyber

[80] NATO, *Strengthening Cyber Resilience: NATO's Cyber Coalition and Collective Defence*, 29.11.2024, NATO ACT, accessed: 13.12.2024.
[81] NATO, *Command and Control Services*, https://www.ncia.nato.int/about-us/service-portfolio/command-and-control-services, NATO NCI, accessed: 13.12.2024.
[82] NATO C2COE, *About the centre*, https://c2coe.org/about-the-centre, accessed: 13.12.2024.
[83] A. Ertan, K. Floyd, P. Pernik, T. Stevens, *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, NATO CCDCOE, 2020, pp. 127-138.
[84] NATO CCD COE, *NATO Cyberspace Exercises: Moving Ahead CyCon 2022 Workshop Summary*, https://ccdcoe.org/uploads/2022/12/CyCon-2022-Workshop-NATO-Cyberspace-Exercises-Moving-Ahead-Summary-Paper.pdf, December 2022, accessed: 17.10.2024.
[85] NATO, *Allies agree new NATO Integrated Cyber Defence Centre*, https://www.nato.int/cps/en/natohq/news_227647.htm, accessed: 13.12.2024.

capabilities of individual member states but also fortifies the collective defence posture of the Alliance in an increasingly contested cyberspace.

In NATO's cyber operations framework, it is essential to distinguish between peacetime and wartime activities, as well as between defensive and offensive actions. Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) pertain specifically to offensive cyber operations. These operations are conducted by individual member nations and are not under NATO's direct C2. Instead, they are offered voluntarily by allies to support NATO missions, with the providing nation retaining full control over the execution and oversight of these operations. This approach ensures that while NATO can benefit from offensive cyber capabilities during its missions, the sovereignty and decision-making authority of each member state are preserved.[86]

NATO's cyber defence framework relies on a coordinated approach, with distinct roles assigned to various commands and entities to ensure strategic planning, operational execution, capability development, and collaboration across member states.

The Allied Command Transformation (ACT) leads NATO's efforts in cyber defence transformation, ensuring that the Alliance is equipped to address evolving cyber threats. ACT focuses on innovation, research, and the development of cyber capabilities, thereby enhancing interoperability across member states. It promotes training, exercises, and new operational concepts to strengthen NATO's collective cyber resilience. Additionally, ACT collaborates closely with COEs to support cyber strategy development and the enhancement of defensive and offensive capabilities.

The CCDCOE, located in Tallinn, Estonia, is a NATO-accredited organisation that supports the Alliance by providing expertise in cyber defence research, training, and education. The CCDCOE is renowned for its annual "Locked Shields" cyber exercise and its legal and policy research contributions. It serves as a hub for sharing knowledge among NATO members and partners, advancing both technical and strategic cyber capabilities. The CCDCOE is part of a broader network of NATO-accredited COEs, which support NATO efforts by enhancing expertise and capabilities across various domains, including cyber defence. In summary, CCDCOE provides expertise, training, and research to strengthen the cyber capabilities of member states.[87]

SHAPE is NATO's strategic command and is responsible for overseeing the development and execution of strategies and policies, including those related to cyber defence. SHAPE coordinates NATO's strategic planning efforts to enhance the Alliance's readiness against cyber and hybrid threats. Its role includes formulating long-term defence strategies that align with NATO's collective security objectives.

The Allied Command Operations (ACO) is responsible for the operational execution of NATO's defence strategies, including cyber operations. The Cyberspace Operations Centre (CyOC) provides strategic coordination of cyber activities with attached electronic warfare capability, while the Joint Force Commands (JFCs) handle operational command, integrating cyber capabilities into broader missions. Supporting units, such as the NCIA and the NCIRC, maintain interoperability and provide strategic

[86] NATO, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20)*, https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf, accessed: 03.02.2025.

[87] NATO, *Cyber defence*, 30.07.2024, https://www.nato.int/cps/uk/natohq/topics_78170.htm, accessed: 13.01.2025.

direction for secure communications and cyber incident response. Together, these entities ensure that NATO's cyber infrastructure and operations remain resilient and secure.

The advancement of cyber capabilities across thirty-two member states represents a substantial asset for NATO, enhancing the Alliance's overall strength. However, this also introduces significant challenges in tracking rapid technological changes and ensuring effective coordination to implement cohesive actions. The cyber domain has now emerged as a pivotal and strategic area, requiring NATO to integrate and address its complexities at multiple levels, particularly as each member state remains at a different stage of development with respect to its cyber forces.

5. The role and evolution of cyber forces in NATO

NATO's Cyber Defence Policy highlights the critical role of cyber threats in contemporary warfare, requiring member states to establish and sustain robust cyber defence capabilities. These cyber forces—most of which are military units—belong to individual NATO member countries and not to NATO as a collective organisation. Often referred to as "Cyberspace Operations Forces" or "Cyber Defence Forces," they are specialised national military units tasked with achieving military objectives both in and through cyberspace. These forces are responsible for conducting both defensive and offensive cyber operations, safeguarding critical military networks and infrastructure, supporting conventional military operations through cyber capabilities, and conducting cyber intelligence, surveillance, and reconnaissance (ISR). Originally organised to respond rapidly to cyber incidents and attacks on NATO assets, these units collectively play a vital role in protecting NATO. Depending on the cyber capabilities of individual member states, these forces may operate within NATO's military structure or be independently managed by its respective member states.

In the majority of NATO countries, cyber forces are a distinct, specialised component within the armed forces. While structures may vary, we can generally agree on the definition that cyber forces are military in nature, as they operate as specialised units within national armed forces. Their responsibility is to maintain and ensure security in one of the operational domains, which, with the rapid advancement of technology, has become known as cyberspace. Cyber forces undertake a broad range of tasks, including defensive measures, ISR, and, sometimes, offensive operations. These forces are entrusted with ensuring telecommunication security, conducting research, designing, constructing, and protecting technology. This branch of the military is also involved in scientific, educational, and advisory activities. Experts in cyber forces develop methods for detecting incidents in cyberspace, design solutions for protecting and securing information, and organise, maintain, and monitor networks and systems, both classified and unclassified, in real-time. Moreover, cyber forces support the efforts of other military branches across land, air, and sea domains. Unlike conventional armed forces, cyber units do not engage in physical confrontations with adversaries, as their operational area is restricted to digital space and the Internet.[88]

When it comes to the deployment of cyber forces, they must also be perceived as an integral part of the armed forces. For instance, their integration into planning and operations ensures the security and defence of critical networks and systems while achieving operational objectives. Joint force commanders operate in an increasingly complex environment, one that must integrate cyberspace as a critical fifth operational domain alongside land, air, maritime, and space. While mission command principles emphasise decentralised execution and disciplined initiative, cyberspace operations often challenge traditional notions of delegation and decentralisation due to the strategic implications of employing national-level cyber capabilities. Commanders must navigate unique challenges such as

[88] *Wojska Obrony Cyberprzestrzeni*, Ministerstwo Obrony Narodowej, https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni, accessed: 14.01.2025; *Cyber forces*, Bundesheer.at, https://www.bundesheer.at/en/the-forces/cyber-forces, accessed: 14.01.2025; *Mission and Vision*, U.S. Cyber Command, https://www.cybercom.mil/About/Mission-and-Vision, accessed: 14.01.2025.

the need for shared understanding, intense coordination, and situational awareness in a contested digital environment.[89]

Advancements in information and communication technology (ICT) based on the electromagnetic spectrum (EMS) have fundamentally reshaped the contemporary security environment, particularly within the information environment (IE). This interconnected and dynamic landscape blurs distinctions between civilian and military domains and among different components of the armed forces, requiring a comprehensive and adaptive approach to address threats that transcend traditional boundaries.[90] The development of cyber forces in NATO countries reflects an acute recognition of these challenges, as member states bolster their capabilities to secure and dominate within the IE. As cyberspace evolves into an independent domain and a cross-domain enabler, serving civilian and military purposes, a holistic strategy, one that considers its multifaceted dimensions and inherent vulnerabilities, is indispensable to ensuring resilience, strategic readiness, and operational superiority within this complex and rapidly evolving domain.

A common trend is emerging among the thirty-two NATO member states in the establishment of national cyber forces, whose genesis is propelled by the collective acknowledgement that cyber defence is a crucial element of national security. Still, there is no consensus on the obligations of military cyber forces during peacetime, especially in relation to their interactions with civilian institutions and private sector players. In most allied countries, the use of cyber forces remains limited mostly to the protection of their own systems, especially industrial control systems (ICS), without being fully integrated into a larger, holistic Cyber Defence Strategy. Many NATO nations still lack clear roles, coordination systems, and cooperative frameworks, especially with relation to the efficient deployment of military cyber forces, which would close this gap. Developing thorough national cyber resilience thus depends on establishing these links.

The significance of an integrated approach is highlighted by actual occurrences, such as those documented in Poland, where industrial systems have faced escalating cyberattacks.[91] These cases underline the increasing threat environment all NATO members face and the need to extend the military's cyber involvement beyond internal defence. NATO countries can more successfully handle changing cyber threats by encouraging cooperation across sectors, thereby enhancing civil-military relationships and methodically building national cyber forces. By doing this, they not only improve their own resilience but also help the whole Alliance to become more secure and stronger online.

This report aims to highlight the evolution of cyber forces across all thirty-two NATO member states by examining their unique cyber challenges, the development of national cybersecurity strategies, and the concept and eventual establishment of cyber forces. Each nation is examined independently, concentrating on three fundamental aspects: the comprehensive cybersecurity environment, the historical evolution of cyber units, and the present organisation and resources. The development of cyber forces is given great importance, stressing differences in organisation,

[89] V. Delacruz, *Mission Command In and Through Cyberspace: A Primer for Army Commanders*, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136047/mission-command-in-and-through-cyberspace-a-primer-for-army-commanders/, accessed: 10.12.2024.

[90] D. Strucl, *Cyber and Space are two "new" domains in the concept of "Multi-Domain Operations: "The influence of the Space-Cyber domain on future warfare*, Kranj 2024.

[91] K. Paslawski, *Ataki na przemysłowe systemy sterowania w Polsce*, https://crn.pl/aktualnosci/ataki-na-przemyslowe-systemy-sterowania-w-polsce-ataki-na-systemy-przemyslowe, accessed: 17.03.2025.

from advanced systems to countries just beginning to acquire their own capabilities. Eventually, improving the cyber capacity of every member state directly increases the Alliance's overall security and resilience.

5.1 Albania

5.1.1 Overview of the state's cybersecurity situation

Cyber terrorists linked to Iran carried out Operation 'Homeland Justice' in 2022,[92] which led to the destruction of government electronic services. Several companies fell victim to cyber piracy, but the exact number remains unknown. Nevertheless, the attack resulted in the severing of diplomatic relations between Albania and Iran[93] and the preparation of NATO's first defensive cyber operation, 'Hunt Operation'.[94] This event also contributed to the establishment of the National Cyber Security Agency (alb. Agjencia Kombëtare për Sigurinë Kibernetike - AKSK), functioning under the supervision of the Ministry of Infrastructure and Energy of Albania. It acts as the national Computer Security Incident Response Team (CSIRT). AKSK is responsible for cooperation with international organisations such as Europol and NATO.[95]

After the 2022 attacks, the country's cybersecurity ecosystem underwent a drastic change, including an increase in budget and expansion of the Responsible Authority for Electronic Certification and Cyber Security's (AKCESK) personnel, activities and projects. The law regulating cyberspace in Albania is Law No. 2/2017 on cybersecurity, which introduced key institutions for managing this sphere, such as the AKCESK, the CSIRT. Despite the Albanian Ministry of Defence's adoption of a proactive role in the field of cyber defence, through the establishment of a cyber unit within the armed forces, the EU's cybersecurity policy has been expanded and focused on close CIMIC in cyberspace. Despite this fact, Albanians continue to be victims of surveillance by their own government and politicians, making civil society a victim of cyber attacks controlled by centres linked to the government.[96]

Albania is currently the 5th largest source of cybercrime in Europe and experiences at least 1.3 million cyberattacks per year. The country is also a signatory to the Budapest Convention on Cybercrime, ratified by its parliament in 2002. The latest five-year National Cyber Security Strategy states that 'cybersecurity legislation should be harmonised with EU law, thus creating a complete and codified mechanism to adequately address and resolve problems'. Albanian law enforcement has also cooperated with Europol

---

[92] "Homeland Justice Operations Against Albania (2022)", *Cyber Law Toolkit, NATO CCDCOE*, https://cyberlaw.ccdcoe.org/wiki/Homeland_Justice_operations_against_Albania_(2022), accessed: 17.03.2025.

[93] M. Beqa, *Albania Must up its Game to Meet Growing Cybersecurity Challenges*, Balkan Insight, 2 March 2023, https://balkaninsight.com/2023/03/02/albania-must-up-its-game-to-meet-growing-cybersecurity-challenges/ accessed: 17.03.2025.

[94] "Committed Partners in Cyberspace: Following Cyberattack, U.S. Conducts First Defensive Hunt Operation in Albania," *U.S. Cyber Command*, 23 March 2023, https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/., accessed: 17.03.2025.

[95] "About Us", *National Authority for Electronic Certification and Cyber Security (AKSK)*, https://aksk.gov.al/en/about-us/. accessed: 17.03.2025.

[96] "*We are fighting against a 'digital army': Albania's Citizens Channel faces cyberattacks'*, Civil Rights Defenders, 12 April 2024, https://crd.org/2024/04/12/we-are-fighting-against-a-digital-army-albanias-citizens-channel-faces-cyber-attacks/ accessed: 17.03.2025.

in coordinated action against cyber fraud, as well as through the launch of the awareness campaign 'Sell Safe'.[97]

5.1.2 History and evolution of cyber units

Cybersecurity and cyber defence key points on the agenda of Albanian defence-related institutions. The 2014 National Security Strategy promoted the adoption and implementation of the National Cyber Security Strategy (NSC) as one of its objectives. The document itself emphasised the protection and safeguarding of information in all forms of its existence, focusing its efforts on the direction of protection against cyber attacks. Accordingly, cyber defence was high on the agenda of the Albanian Ministry of Defence and the Air Force, and the reason for this was the NSC's classification of cyber attacks as a type one risk (i.e., of highest importance).

The Ministry of Defence has developed the concept of cyber defence by initiating its own Cyber Defence Strategy (2014-2017). It was designed to provide orientation, coherence and focus on a comprehensive approach to developing military capabilities in cyberspace.

A second version of the document was prepared in 2018-2020 for the Ministry of Defence and the Air Force. As a NATO member, Albania signed the 2013 MoU with the NATO Computer Incident Response Capability [98](NCIRC) on strengthening cyber defence. Since 2016, the country has also actively participated in NATO's largest annual cyber exercise, the Cyber Coalition.

In 2024, with the support and coordination of the US, Albania established the 'Military Cyber Security Unit'. This unit is part of the General Staff of the Armed Forces and aims to monitor and protect Ministry of Defence information systems from unauthorised access and other cyber threats around the clock. Its staff is comprised of military and civilians, with a foreign (presumably US) adviser overseeing its operation for three years. The unit is expected to cost the US 50 billion USD.[99]

5.1.3 Current structure and resources

The Ministry of Defence is the institution responsible for handling cyber incidents related to the Ministry of Defence and the Air Force. It also oversees the implementation of the National Cyber Defence Strategy. In the NCSI Index, Albania received a score of zero in the 'Cyber Operations Unit' category, failing to meet the following requirements:

1. The armed forces should have a Cyber Command that specialises in planning and executing cyber operations;
2. The armed forces have conducted cyber operations exercises or exercises with a cyber operations component in the country in the last 3 years.[100]

---

[97] EU Cyber Direct: *Albania*, https://eucyberdirect.eu/atlas/country/albania accessed: 17.03.2025.

[98] sometimes referred to as the NATO Cyber Incident Response Centre—to enhance cooperation and capability in cyber defence

[99] "Military Cyber Security Unit is Inaugurated", *Ministry of Defence of Albania*, 14 January 2024, https://www.mod.gov.al/eng/newsroom/1600-military-cyber-security-unit-is-inaugurated. accessed: 17.03.2025.

[100] I. Dedja, A. Dyrmishi, J. Çipa, *Cyber Governance Challenges for Albania: Addressing policy choice dilemmas*, Center for the Study of Democracy and Governance, September 2023, pp. 51-60.

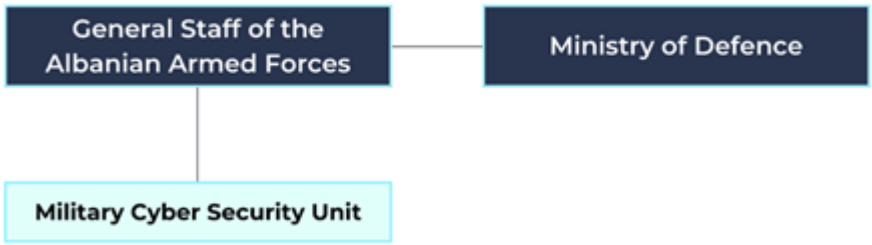


FIGURE 5. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN ALBANIA.

5.2 Belgium

5.2.1 Overview of the state's cybersecurity situation

Belgium first implemented specific cybercrime legislation as early as 2000, and in 2012, the government adopted a National Cyber Security Strategy to address growing cyber threats.[101] Compared to the total number of crimes in Belgium, cybercrime is not the dominant category in the target region. Nevertheless, the number of cyber incidents has increased rapidly since 2017, resulting in the Belgian National Risk Assessment (nl. Belgische Nationale Risico Analyse - BNRA) identifying cyber threats as one of the greatest risks that could significantly affect the country's security.[102]

By 2020, the number of recorded cybercrime incidents exceeded 44,000 and, in 2022 alone, the Belgian Federal Police reported more than 58,400 cases of cybercrime.[103] A report by the Belgian Cyber Security Centre (nl. Centrum voor Cybersecurity België - CCB) identified Ransomware and DDoS attacks as the most common threats.[104]

Only 20% of companies are protected by a security specialist, while 80% leave IT security to their managers or have not designated an appropriate person. Only 8% of companies have encrypted computer data, which makes confidential data and passwords vulnerable to attacks by hackers.[105] Due to Belgium's support for Ukraine since 2022 and the strategic importance of Brussels as the headquarters of NATO's Western Command and many EU institutions,[106] the Russian Federation has been committing

[101] "Belgium," Octopus Cybercrime Community, Council of Europe, 10 February 2025, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/belgium accessed: 17.03.2025.
[102] Belgian National Risk Assessment, 2025, https://crisiscenter.be/sites/default/files/documents/files/Belgian%20National%20Risk%20Assessment_EN.pdf. accessed: 17.03.2025.
[103] *Registered cases of cybercrime in Belgium from 2008 to 2022*, Statista, https://www.statista.com/statistics/534977/cybercrime-in-belgium/, accessed: 17.03.2025.
[104] Belgian Cyber Security Centre, CCB Report 2023, 2023, https://ccb.belgium.be/sites/default/files/CCB%20REPORT%202023_EN.pdf. accessed: 17.03.2025.
[105] *What is the state of cybersecurity in Belgium and the world?*, Digital Dives, https://www.dnsbelgium.be/en/digital-dives/cyberwar/cybersecurity-belgium-and-world accessed: 17.03.2025.
[106] "Cyber-attacks on the rise, Belgium an increasingly popular target," VRT NWS, 26 November 2024, https://www.vrt.be/vrtnws/en/2024/11/26/_cyber-attacks-on-the-rise-belgium-an-increasingly-popular-tar/. accessed: 17.03.2025.

hostile cyber acts against Belgium, such as interfering in national elections.[107] The CCB confirmed a cyber attack on the municipalities of Enghien, Comines-Warneton, Mouscron, Flobecq, Amblève, Colfontaine and Malmedy. The attack was claimed by a pro-Russian hacking group called NoName057.[108]

5.2.2 History and evolution of cyber units

A landmark step towards organising cyber defence was the establishment of the Belgian Cyber Security Centre in 2014. This institution is responsible for coordinating cybersecurity activities at a national level, including the protection of government networks and cooperation with international partners such as NATO and the EU. In 2024, it played a key role in negotiating the Cyber Solidarity Act and the amendment of the Cyber Security Act during the Belgian Presidency of the Council of the EU. It chaired the EU-CyCLONe and NIS networks, organised the Brussels Cyber Security Summit and led the implementation of the NIS2 Directive, making Belgium the first EU country to fully implement it. The CCB is also strengthening international cooperation by contributing to NATO and OSCE initiatives and is preparing Belgium's new Cyber Security Strategy for 2025-2030.[109]

The CCB also has a CERT.be team which is responsible for analysing cyber attacks in Belgium and provides technical support and assistance to other government departments.[110] In 2017, Belgium adopted its first Cyber Defence Strategy in response to growing cyber threats from state actors and criminal groups. The strategy included strengthening Belgium's capacity to defend itself against cyber attacks and creating special military units in charge of cyber operations.

Based on the STAR Plan 2022 (Security & Service – Technology – Ambition – Resilience), a Belgian Cyber Command (BECYBERCOM) was created to coordinate with the armed forces and to collect information for the General Intelligence and Security Service (nl. Algemene Dienst Inlichting en Veiligheid – ADIV; fr. Service Général du Renseignement et de la Sécurité - SGRS) and to conduct operations in cyberspace. The cyber component, known as Cyber Force, is organised similarly to a brigade (Bde) comprising several entities, akin to battalions (Bn), each specialising in different aspects of cyber operations. The Belgian Cyber Command is one of these entities within the Cyber Force structure, focusing specifically on military cyber defence and offensive operations.

On 19 October 2022, the Belgian Ministry of Defence announced the initial operational capability of its new Cyber Command,[111] which constitutes the fifth component of the Belgian Armed Forces, alongside the Land, Maritime, Air and Medical Forces.[112] The essence of Belgium's commitment to developing its

[107] Ciara Carolan, "Pro-Russian cyber-attacks in Belgium: What impact on local elections?", The Brussels Times, 12 October 2024, https://www.brusselstimes.com/1264870/pro-russian-cyber-attacks-in-belgium-what-impact-on-local-elections, accessed: 17.03.2025.
[108] *Belgium hit by pro-Russian cyberattacks for third consecutive day*, Belga News Agency, 9 October 2024, https://www.belganewsagency.eu/belgium-hit-by-pro-russian-cyber-attacks-for-third-consecutive-day accessed: 17.03.2025.
[109] Centre for Cybersecurity Belgium, "Protect, Strengthen, Prepare," Centre for Cybersecurity Belgium, 2024, https://ccb.belgium.be/en/protect-strenghten-prepare?utm_source. accessed: 17.03.2025.
[110] Centre for Cybersecurity Belgium, "Organisation," Centre for Cybersecurity Belgium, 2024, https://ccb.belgium.be/en/organisation?utm_source. accessed: 17.03.2025.

[111] *STARPlan 2022 Security & Service, Technology, Ambition, Resilience*, La Défense.be, 2022, pp. 35-41.
[112] Ludivine Dedonder, *Belgian military's Cyber Command to be operational in 2024*, The Brussels Times, 12 October 2024, https://www.brusselstimes.com/310607/belgian-militarys-cyber-command-to-be-operational-in-2024?utm_source. accessed: 17.03.2025.

cyber component over the years is illustrated by the establishment of a first-of-its-kind integrated Cyber Defence Centre in Mons alongside the development of a new strategy for securing NATO networks.[113]

5.2.3 Current structure and resources

The new unit, allocated 400 million € under the STAR Plan, is recruiting both military personnel and civilian specialists. Until the end of 2024, Cyber Command remained under the authority of the Military Intelligence Service (ADIV/SGRS) and relied on the capabilities already available there. Now, Cyber Command forms the fifth pillar of Brussels' security, functioning as a fully independent entity with its own legal framework. Like other components, it reports directly to the Ministry of Defence. The Cyber Command collaborates closely with the Military Intelligence Service and maintains privileged relationships with industry and the academic world to enhance national resilience.

BECYBERCOM cooperates and exchanges information with various services and companies within Belgium's cyberspace. It also collaborates with researchers from the Royal Military Academy and the Royal Higher Institute for Defence. For example, ongoing cryptography research focuses on stronger encryption techniques and devices capable of generating cryptographic keys.

Belgium's understanding of cyberspace emphasises that there is no clear distinction between times of peace and times of war. Cyber threats and operations occur persistently below the threshold of open conflict, with no definitive crossing of NATO's Article V trigger for collective defence. This continuous engagement environment heavily influences Cyber Command's operational planning and legal framework.

Nearly half (46%) of the personnel at Belgian Cyber Command are civilian specialists. Each year, the unit recruits up to 100 individuals, prioritising a broad range of expertise. It seeks professionals in areas such as cyber threat analysis, cyber operations, and IT system security. New recruits receive rigorous training to address the fast-changing cybersecurity landscape.[114]

Cyber Command is tasked with protecting the networks and weapon systems of the Belgian Armed Forces, including F-35 fighter jets, MQ-9B drones, and mine countermeasure vessels. This involves implementing cryptographic keys and securing system software against cyber threats. Additionally, the unit conducts cyber operations to infiltrate enemy networks, gather intelligence, and execute offensive actions[115] in cyberspace. It holds exclusive legal authority within Belgium to conduct such operations, setting it apart from other national institutions.

---

[113] M, Matishak, NATO *members commit to creating new cyber centre in Belgium*, The Record, 11 July 2024, https://therecord.media/nato-cyberdefense-center-belgium-announcement accessed: 17.03.2025.

[114] Cyber Commande la Défense, *La Défense.be*, 2024, https://www.mil.be/fr/a-propos-de-la-defense/cyber-command/, accessed: 17.03.2025.

[115] Belgian cyber operations follow distinct legal frameworks: The 1998 Intelligence and Security Services Act allows offensive cyber actions, while military cyber operations are governed by laws on armed forces readiness, granting BECYBERCOM exclusive authority.
A. Mattelaer, *Belgian Cyber Command and Legal Framework*, Egmont Policy Brief 295, Egmont Institute, November 2022, https://www.egmontinstitute.be/app/uploads/2022/11/PB-295-Alexander-Mattelaer_Cyber-Command.pdf, accessed: 17.03.2025.

FIGURE 6. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN BELGIUM

5.3 Bulgaria

5.3.1 Overview of the state's cybersecurity situation

In 2020, in response to the increase in cyber threats, the Bulgarian government, with the financial support of the European Commission (EC), announced programmes and initiatives to spend 9 million USD to combat botnets and allocate a further 1 million USD for cyber threats regulations.[116] In October 2022, pro-Russian hackers were behind a 'large-scale' cyber attack on Bulgarian government websites that briefly disabled the websites of the presidential administration, the Ministry of Defence, the Ministry of Interior, the Ministry of Justice and the Constitutional Court. The attack, according to the perpetrators, was caused by Bulgaria's 'betrayal of Russia and support for Ukraine'.[117]

The Bulgarian government has since adopted a National Cyber Security Strategy called 'Cyber Resilient Bulgaria 2020', which aims to provide better protection for citizens, businesses, governments and critical infrastructure.

In September 2023, the US funded a state-of-the-art Cyber Defence Centre in Sofia, Bulgaria, with an investment of 12 million USD. This facility serves as a hub for advanced cyber defence training and operations, providing Bulgarian military personnel with education in deterring, detecting, and defending against cyber threats.[118]

[116] *Bulgaria - Country Commercial Guide. Safety and Security*, International Trade Administration, 1 February 2024, https://www.trade.gov/country-commercial-guides/bulgaria-safety-and-security accessed: 17.03.2025.
[117] D. Antoniuk, *Cyberattack disrupts Bulgarian government websites over 'betrayal to Russia'*, The Record, 18 October 2022, https://therecord.media/cyberattack-disrupts-bulgarian-government-websites-over-betrayal-to-russia accessed: 17.03.2025.
[118] U.S. Embassy in Bulgaria, U.S. *Donates Cyber Defense Center to Bulgaria*, https://bg.usembassy.gov/u-s-donates-cyber-defence-center-to-bulgaria-09-14-2023/ accessed: 17.03.2025.

5.3.2 History and evolution of cyber units

The Communications, Information and Cyber Defence Support Command (bul. Командване за комуникационно-информационна поддръжка и киберотбрана - ККИПКО) was established on 1st of September 2021 as the legal successor of the Stationary Communications and Information System, which had been directly subordinate to the Minister of Defence since 2011. The Stationary CIS was established in place of the then Communication and Information Brigade Command, which was in turn subordinate to the Chief of General Staff of the Bulgarian Army.[119] The Cyber Defence Centre was inaugurated in Sofia in September 2023, owing to 12 million USD in funding from the US. This facility serves as a training hub for Bulgarian military personnel, offering advanced educational programmes in identifying, countering and defending against cyberattacks.[120]

5.3.3 Current structure and resources

The Communication, Information and Cyber Defence Support Command (CICDSC) provides communications and information and cyber defence support to the C2 System during the full spectrum of missions and tasks of the Armed Forces of the Republic of Bulgaria, while ensuring the necessary level of reliability and availability. The CICDSC and the C2 System of the Bulgarian Forces Armed Forces (C2) provide support through the bodies and structures responsible for the planning, construction, development, operation and maintenance of communications, information, navigation and cyber defence systems at headquarters, as well as troops and forces at the strategic, operational and tactical levels of command – both stationary and mobile. The CIS provides the C2 functionality of the armed forces and ensures the effective exchange of information essential for the Ministry of Defence to interact with other ministries and agencies, as well as with NATO and the EU.

The establishment of the CISCDC and its achievement of full operational capability have been designated a priority. Cyber warfare is being developed within the aforementioned CISCDS, which is part of the Bulgarian Armed Forces.[121] Units under the CISCDC will develop capabilities across three main mission parameters:

- "Defence" – communications and cyber defence support for state management bodies during wartime and the C2 System at the strategic level, as well as the secure exchange of classified information at the strategic level;
- "Support for international peace and security" – providing communications and cyber defence for national surveillance of formations participating in crisis response operations abroad;
- Mission "Contribution to peacetime national security" – capabilities built and developed will contribute to the cyber defence of critical infrastructure.

---

[119] *Communications and Information Support and Cyber Defence Command*, Ministry of Defence of the Republic of Bulgaria, https://www.mod.bg/en/ba.html accessed: 17.03.2025.

[120] "U.S. Donates Cyber Defence Center to Bulgaria", *U.S. Embassy in Bulgaria*, 14 September 2023, https://bg.usembassy.gov/u-s-donates-cyber-defence-center-to-bulgaria-09-14-2023/. accessed: 17.03.2025.

[121] *Programme for the development of the defence capabilities of the Bulgarian armed forces 2032*, Ministry of Defence of the Republic of Bulgaria, pp. 22-24.

There are no specific details available on the budget or the current staffing levels of the cyber component. On the other hand, spending on the military sector was 1.92 billion USD in 2023.[122] This was 0.58 billion USD less than assumed in the national document 'National plan for increasing the defence spending to 2% of the gross domestic product until 2024'. It can be assumed, on this basis, that the projected defence spending of 2.8 billion USD for 2024 was not fully met.[123]

On the other hand, a report published in 2024 indicates that the Bulgarian Armed Forces (bul. Българска армия) are facing a serious manpower deficit. The shortage of officers exceeds 26%, while vacancies among soldiers approach 28%. This could significantly affect operational effectiveness, including cyber defence capabilities.[124]

FIGURE 7. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN BULGARIA.

5.4 Canada

5.4.1 Overview of the state's cybersecurity situation

The National Cyber Threat Assessment 2023-2024 report assessed that cybercrime remains a threat that is highly likely to affect Canadians. This means that Canadian businesses and institutions will face DDoS attacks, alterations of website content, ransomware and money laundering technologies.[125] Statistics 2023 on the impact of cybercrime on Canadian businesses reveal that the three most common types of attacks are fraud and phishing (50%), identity theft (31%), and ransomware attacks (13%).[126] Canadian critical infrastructure has been targeted by hostile states, most notably Russia.[127]

[122] *Bulgaria Military Expenditure*, Trading Economics, https://tradingeconomics.com/bulgaria/military-expenditure accessed: 17.03.2025.
[123] *National plan for increasing the defence spending to 2% of the gross domestic product until 2024*, The Republic of Bulgaria Council of Ministers, p. 4.
[124] "Angel Naydenov Recalled that the Bulgarian Soldier is Poor and Homeless", *Fakti.bg*, 12 April 2024, https://fakti.bg/en/bulgaria/872598-angel-naydenov-recalled-that-the-bulgarian-soldier-is-poor-and-homeless#:~:text=The%20shortage%20of%20officers%20exceeds,be%20no%20less%20than%2043%2C000 accessed: 17.03.2025.
[125] National Cyber Threat Assessment 2023-2024, Canadian Center for Cyber Security, p. 3.
[126] Impact of cybercrime on Canadian businesses, 2023, Statistics Canada, https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm, accessed: 17.03.2025.
[127] *Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure*, Canadian Centre for Cyber Security, https://www.cyber.gc.ca/en/news-events/russian-military-cyber-actors-target-us-global-critical-infrastructure, accessed:

According to the Canadian Centre for Cyber Security, spending on recovery from cybersecurity incidents has doubled, reaching 1.2 billion USD in 2023, compared to 600 million USD in 2021. The Canadian Cyber Centre is aware of more than 100 cyber threat incidents involving Canadian municipalities since early 2020. Most of the cases involved social engineering, unauthorised network access, or the execution of malicious code such as ransomware. This demonstrates the importance of critical infrastructure as a target for cybercriminals.[128] In April 2023, pro-Russian hackers launched DDoS attacks on port websites in Halifax, Montreal and Quebec City. While these attacks did not affect service, they did block access to these portals.[129] In addition, Chinese state-backed hackers breached 20 Canadian government networks.[130]

5.4.2 History and evolution of cyber units

The Harper government's 2010 Cyber Security Strategy recognised state cyber operations as a tertiary threat. The strategy's commitments to strengthen cyber security in the military yielded three outcomes: the creation of a Canadian Cyber Task Force and Director General; the development of information sharing with allies; and the strengthening of network defence capabilities. Despite guidance from the Chief of Defence Staff in 2013, the task force has struggled to achieve any of its objectives due to a significant lack of personnel, institutional and force structures. The Canadian Armed Forces' (CAF) difficulties in developing cyber defence under the 2010 strategy continued up to the administration of Prime Minister Justin Trudeau, leading to a final policy change in the 2017 *Strong, Secure, Engaged* (SSE) strategy.

Under the SSE, the Trudeau government has sought to address these issues and provide the Department of National Defence (DND) and CAF with the resources and mandate to develop cyber defence and offensive cyber capabilities. In 2018, the Government of Canada released the National Cyber Security Strategy, which set out a framework for protecting critical infrastructure and responding to cyber incidents. As part of this strategy, the Canadian Centre for Cyber Security was established and became the focal point for coordinating cyber-related activities at the federal level.[131] The DND/CAF Departmental Plan Outcome Report 2019-2020 indicates that the Communications Security Establishment (CSE) and CAF have since worked together to develop proactive cyber capabilities, with some demonstrable success.[132] On 26 September 2024, Bill Blair, Minister of National Defence, and General Jennie Carignan, Chief of Defence Staff, formally announced the creation of the Canadian Armed Forces Cyber Command (CAF

17.03.2025.
Pro-Russian Hackers Ramp Up Attacks on Canadian Infrastructure, MLT Aikins, https://www.mltaikins.com/insights/pro-russian-hackers-ramp-up-attacks-on-canadian-infrastructure, accessed: 17.03.2025.

[128] *National Cyber Threat Assessment 2023-2024*, Canadian Center for Cyber Security, p.11.

[129] *Cyberattacks Hit Canada: Websites Down for Three Major Ports, Port Technology*, https://www.porttechnology.org/news/cyber-attacks-hit-canada-websites-down-for-three-major-ports/, accessed: 17.03.2025.

[130] J. Reddick, *Chinese state-backed hackers breached 20 Canadian government networks over four years, agency warns*, https://therecord.media/canada-20-government-agencies-hacked-china-last-four-years, accessed: 17.03.2025.

[131] National Cyber Security Strategy https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx, p.5, accessed: 17.03.2025.

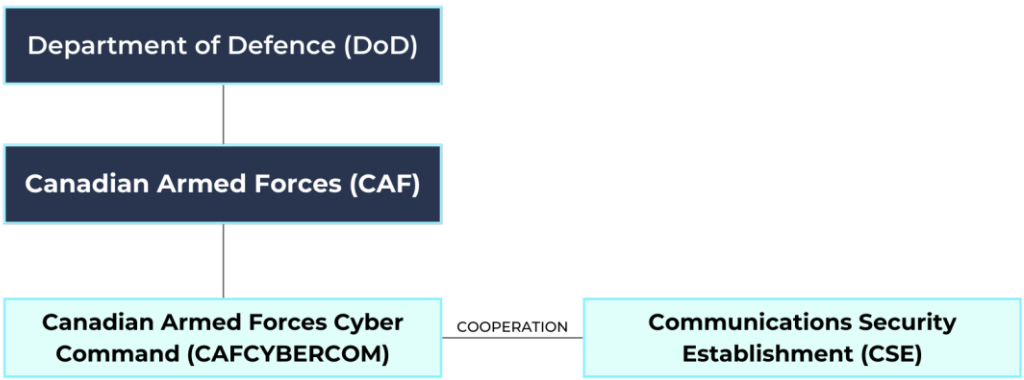
[132] A. Rudolph, *Canada's Active Cyber Defence is Anything But Active*, Canadian Global Affairs Institute, July 2021, https://www.cgai.ca/canadas_active_cyber_defence_is_anything_but_active#Canadian, accessed: 17.03.2025.

Cyber Command; CAFCYBERCOM), as announced in the National Strategy 'Our North, Strong and Free'.[133]

5.4.3 Current structure and resources

Through CAFCYBERCOM, CAF continues to develop and scale its offensive and defensive operations capabilities in close collaboration with CSE Canada. CAF and CSE have a longstanding partnership in developing advanced technical and specialised intelligence delivery capabilities for military operations. In addition, the 2019 Communications Security Establishment Act officially authorised CSE to conduct defensive and offensive cyber operations for national security.[134]

The partnership has evolved over the past decade to include cooperation in cyber areas such as security, defensive and offensive operations. The new CAF Cyber Command also enables Canada to fulfil NATO commitments such as VCISC and SCEPVA. The creation of the new command is in line with similar investments by Canada's key partners and allies in the North American Aerospace Defence Command (NORAD), the Five Eyes Alliance and NATO.[135] The Canadian Special Operations Forces Command (CAFCOM) unit will comprise Signals Intelligence and Joint Electronic Warfare units to facilitate and support various cyber work. CAFCYBERCOM is expected to expand the offensive and defensive capabilities of cyber operations and provide appropriate and specialised cyber solutions.[136]



[133] *Canadian Armed Forces establishes a new Cyber Command*, Government of Canada, 26 September 2024, https://www.canada.ca/en/department-national-defence/news/2024/09/canadian-armed-forces-establishes-a-new-cyber-command.html, accessed: 17.03.2025.
[134] Communications Security Establishment Act, Government of Canada, https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html, accessed: 17.03.2025.
[135] Canadian Global Affairs Institute, *Emerging Technology and Five Eyes: Implications for Canadian Defence*, https://www.cgai.ca/emerging_technology_and_five_eyes_implications_for_canadian_defence, accessed: 17.03.2025.
[136] M. Rojoef, *Canada Debuts New Armed Forces Cyber Command*, The Defense Post, 30 September 2024, https://thedefensepost.com/2024/09/30/canada-debuts-armed-forces-cyber-command/, accessed: 17.03.2025.

FIGURE 8. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN CANADA.

5.5 Croatia

5.5.1 Overview of the state's cybersecurity situation

Croatian institutions and companies are facing an increased wave of cyber attacks following the events of the 24th of February 2022, when Croatia, as a NATO member state, sided with Ukraine. The Minister of Defence emphasised that Croatia "witnesses these attacks almost every day". For example, on June 26 2024, there were DDoS attacks on Croatian institutions. The attacks were claimed by the Russian group NoName057(16).[137] Terms such as cybercrime, cybersecurity, cyber domain threats, cyber infrastructure appear frequently in Croatia's 2017 National Security Strategy. Zagreb identifies cyber threats with the country's increasing technologisation and the digitalisation of public institutions.[138]

In July 2023, the Institute for Information Systems Security (cro. Zavod za sigurnost informacijskih sustava - ZSIS) in Croatia adopted an action plan to implement the National Cybersecurity Strategy. This plan outlines specific measures to bolster the country's cyber defences and improve resilience against potential threats.[139]

5.5.2 History and evolution of cyber units

Cyber Command was established in 2019. It is a unit subordinate to the General Staff of the Croatian Armed Forces (cro. Glavni stožer Oružanih snaga Republike Hrvatske). Cyber Command was established on the organisational and personnel structure of the Centre for Communication and Information Systems (cro. Središnjica za komunikacijsko-informacijske sustave – SKIS, the infrastructure provider for the General Staff). It was established at the request of the Ministry of Defence and the General Staff by order of the President.[140]

In 2020. The US provided 4.2 million USD in special assistance to help Croatia establish a new cybersecurity operations centre in Zagreb. The funds were allocated for equipment, training and technology to prevent cyber attacks and defend the Croatian military, according to the US embassy in Zagreb. US Cyber Command sent a team of 'elite defensive cyber operators' to Croatia for the first time in 2022 to collaborate with the Croatian Cybersecurity Centre of the Croatian Security and Intelligence Agency (cro. Sigurnosno–obavještajna agencija - SOA).[141]

[137] A. Kadyrzhanova, *Croatia struggles with surge in cyberattacks*, Bne Intelli News, 1 July 2024, https://www.intellinews.com/croatia-struggles-with-surge-in-cyber-attacks-331784/ accessed: 17.03.2025.
[138] *National Security Strategy of the Republic of Croatia*, The Republic of Croatia, 2017, pp. 7-12.
[139] Data Guidance, Croatia: ZSIS adopts action plan to implement National Cyber Security Strategy, https://www.dataguidance.com/news/croatia-zsis-adopts-action-plan-implement-national accessed: 17.03.2025.
[140] *Initiatives to improve Cyber Defence capabilities - development of NATO cyber forces – Croatia.*
[141] A. Janofsky, *Cyber Command deployed 'hunt forward' defenders to Croatia to help secure systems*, The Record, 18 August 2022, https://therecord.media/cyber-command-deployed-hunt-forward-defenders-to-croatia-to-help-secure-systems accessed: 17.03.2025.

Collaboration between the public and private sectors is crucial for the development of cyber units. This cooperation brings several important benefits, including expertise and information, protection of critical infrastructure, rapid adaptation to evolving threats, education and training.

5.5.3 Current structure and resources

Croatian Cyber Command (cro. Zapovjedništvo za kibernetički prostor – ZzKP) functions within the General Staff of the Armed Forces (cro. Glavni stožer Oružanih snaga Republike Hrvatske). SOA works to detect and suppress state-sponsored cyber attacks. It cooperates with national authorities and international partners in preventing and suppressing cyber challenges. SOA has actively participated in the National Cybersecurity Council and the Operational and Technical Cybersecurity Coordination Group. These bodies are responsible for monitoring cybersecurity and initiating action in the event of a cyber crisis.[142] Croatian Cyber Command (cro. Zapovjedništvo za kibernetički prostor – ZzKP) took over responsibility for maintaining the military's communication networks in addition to providing cyber defence capabilities. One of the Croatian Cyber Command subunits is Centre for Communication and Information Support (cro. Središte za komunikacijsko-informacijsku potporu).

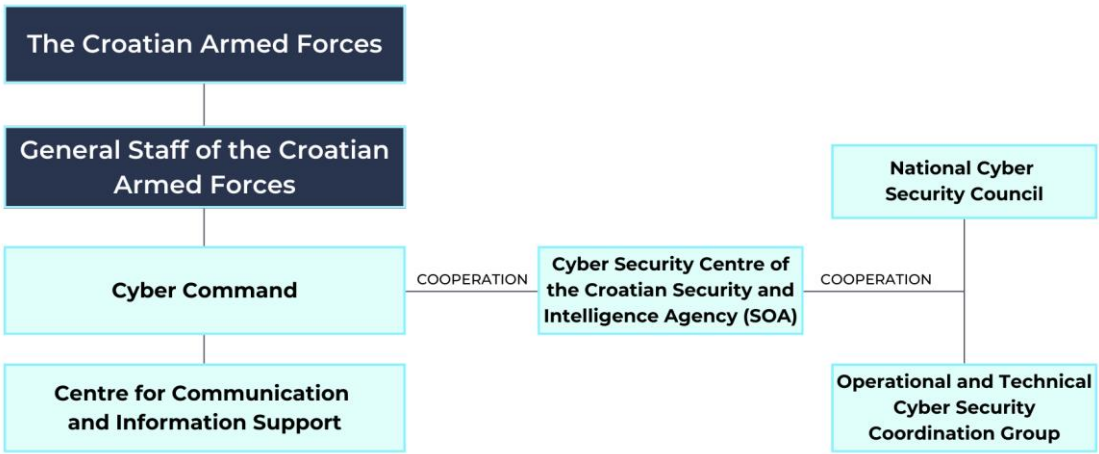


FIGURE 9. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN CROATIA.

5.6 Czech Republic

5.6.1 Overview of the state's cybersecurity situation

The Czech Republic's Cyber Defence Strategy for 2021-2025, like other NATO country documents, links cyber threats to the digitalisation of the country and the technologisation of society. Prague emphasises

[142] *Cyber Security*, Security and Intelligence Agency of the Republic of Croatia, https://www.soa.hr/en/areas-of-activity/cyber-security/ accessed: 17.03.2025.

that the governmental bodies in the Czech Republic have been a target of attacks and cyber espionage for years.[143] In 2023, the National Cyber and Information Security Agency (cz. Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB) registered no fewer than 262 cybersecurity incidents (120 more than in 2022), the highest to date. DDoS attacks accounted for a considerable proportion of all incidents in 2023. The NoName057(16) group was identified as the most frequent perpetrator of these attacks which regularly targeted Czech entities.[144] A total of 268 cybersecurity incidents were recorded, with the threat actor NoName057(16) once again identified among them. However, these incidents pertain solely to that segment of the national infrastructure obligated to report to the National Cyber and Information Security Agency. It is important to note that this dataset does not encompass the entire national landscape, as private sector entities typically do not report cybersecurity incidents unless mandated.[145]

Phishing has remained the most common type of attack for years, followed by network scanning, fake emails, malicious content, and spearphishing.[146] NÚKIB, in cooperation with its partners, identified attempted or successful breaches by at least four separate actors. Analysis suggests that 75-80% of the targets were cyber espionage actors such as Russian APT28 and APT29 (affiliated with SVR and GRU), Chinese Mustang Panda, and North Korean Lazarus. Groups associated with Iran showed lower levels of activity.[147]

5.6.2 History and evolution of cyber units

Information and cyber forces were not established until the 1st of July 2019, with the first unit taking command on the 1st of January 2020. This was the 103rd CIMIC/PsyOps Centre, transformed into the Cyber Force and Information Operations Group. Exactly one year later, a second unit was added, the Computer Incident Response Centre (CIRC), originally part of the Communications and Information Systems Agency (CISA). In this form, these forces still exist today, save for minor changes. However, the decision was taken to reorganise the subordinate units of the Information and Cyber Command into two groups, i.e. regimental-type units, namely the Information Warfare Group and the Cyber Warfare Group.[148] On the 1st of July 2024, the 92nd Cyber Warfare Group was established, focusing on both passive and active operations in cyberspace.[149]

---

[143] *National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025*, National Cyber and Information Security Agency, 18 March 2021, pp. 5-6.

[144] *2023 Report on the State of Cybersecurity in the Czech Republic*, National Cyber and Information Security Agency, 11 September 2024, p. 12.

[145] Národní úřad pro kybernetickou a informační bezpečnost (NUKIB), "NUKIB v roce 2024 zaznamenal více kybernetických incidentů než v předchozích letech," NUKIB, https://nukib.gov.cz/cs/infoservis/aktuality/2215-nukib-v-roce-2024-zaz.namenal-vice-kybernetickych-incidentu-nez-v-predchozich-letech

[146] Ibid. p. 15.

[147] Ibid. p. 23.

[148] I. Zelinka, *Fighting for the enemy's will and the support of its own population: the Cyber Forces and Information Operations Group in Olomouc*, CZ Defence, 29 March 2024, https://www.czdefence.com/article/fighting-for-the-enemys-will-and-the-support-of-its-own-population-the-cyber-forces-and-information-operations-group-in-olomouc accessed: 17.03.2025.

[149] Cyber Forces Command, Ministry of Defence & Armed Forces, 25 October 2024, https://www.mo.gov.cz/en/armed-forces/organisational-structure/cyb/cyber-forces-command-218593/ accessed: 17.03.2025.

5.6.3 Current structure and resources

The Cyber and Information Warfare Command (cz. Velitelství kybernetických sił a informačních operací) is a strategic component contributing to the security and defence of the Czech Republic. Within the command structure, it operates at the tactical level alongside the Land Forces (cz. Pozemní síly), Air Forces (cz. Vzdušné síly), and Territorial Command (cz. Teritoriální velitelství). The superior operational level is formed by the Operations Command (cz. Operační velitelství), which plans, commands, and controls operations of forces and assets both within and outside the territory of the Czech Republic.

The Cyber and Information Warfare Command operates independently, jointly, or in cooperation with other force components and Military Intelligence (cz. Vojenské zpravodajství). It collaborates with entities such as the National Cyber and Information Security Agency (cz. Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB), the central administrative authority for cybersecurity. The Command is capable of conducting information and psychological operations, as well as participating in CIMIC. It can monitor, plan, and manage operations in support of the Armed Forces of the Czech Republic (cz. Armáda České republiky) and allied missions. Additionally, the commander supports the highest levels of army leadership in the field of strategic communications.

The Czech Cyber Command commands the 91st Information Warfare Group (cz. 91. skupina informačního boje) and the aforementioned 92nd Cyber Warfare Group (cz. 92. skupina kybernetického boje).[150] In 2024, the Czech Republic allocated approximately CZK 101 billion to defence, representing 1.37% of its GDP, roughly CZK 10 billion below initial projections. The budget encompassed various domains, including cybersecurity. However, detailed defence expenditure reports have not been publicly released by the Ministry of Defence since 2021.[151]

[150] Ibid.

[151] *Czech Republic Spent 1.37% of GDP on Defence in 2023, Says Defence Minister Cernochova*, Brno Daily, 13 May 2024, https://brnodaily.com/2024/05/13/news/politics/czech-republic-spent-1-37-of-gdp-on-defence-in-2023-says-defence-minister-cernochova/ accessed: 17.03.2025.
Czechia Reaches 2% GDP Defence Spending Target For First Time In 20 Years, *Euractiv*, 19 March 2024, https://www.euractiv.com/section/politics/news/czechia-reaches-2-gdp-defence-spending-target-for-first-time-in-20-years/, accessed: 17.03.2025.

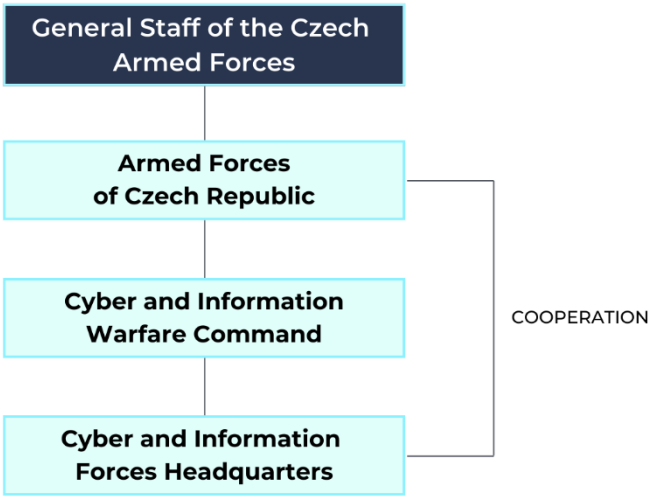


FIGURE 10. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN THE CZECH REPUBLIC

5.7 Denmark

5.7.1 Overview of the state's cybersecurity situation

In early June 2024, the Danish Centre for Cyber Security (den. Centre for Cybersikkerhed - CFCS) raised the threat level of destructive cyberattacks from low to medium. The decision to raise the threat level was based on Russia's increased readiness to use hybrid tactics, including destructive cyberattacks, against European NATO member states.[152] It emphasised that the two most dangerous types of threats facing Denmark are cyber espionage (from Russia and the PRC) and cybercrime. Copenhagen also faces bot farm activity and hostile propaganda. There is an elevated risk of cyber attacks targeting Denmark's critical infrastructure and public institutions. Russia is the main provocateur of such actions. According to analysts, there is no established threat from cyber terrorists.[153]

In June 2024, the Danish CFCS raised the threat level for destructive cyber attacks from "low" to "medium". This adjustment reflects increased concerns over potential cyber threats from state actors, particularly Russia.[154]

[152] *Denmark raises threat level for destructive cyberattacks to 3 on 5-level scale*, Reuters, 4 June 2024, https://www.reuters.com/technology/cybersecurity/denmark-raises-threat-level-destructive-cyber-attacks-3-5-level-scale-2024-06-04/ accessed: 17.03.2025.

[153] *The Cyber Threat Against Denmark* 2024, Centre for Cyber Security, 20 September 2024, p. 5.

[154] Centre for Cyber Security, *The Cyber Threat Against Denmark 2024*, https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs---the-cyber-threat-against-denmark-2024.pdf accessed: 17.03.2025.

5.7.2 History and evolution of cyber units

The defence agreement for 2018-2023 included a provision to strengthen Danish cyber defence with 500 million DKK, but this amount was mainly allocated to activities not strictly related to military security.[155] On 28th of June 2023, the Danish government agreed on a general framework for Danish defence and security from 2024 to 2033. The agreement deals perfunctorily with the issue of cybersecurity, although the parties agreed to "prioritise the strengthening of Danish cyber defence and cybersecurity in relevant bodies across government" and to "enhance cyber and information security".[156]

In 2012, the CFCS was established as part of the Danish Defence Intelligence Service (den. Forsvarets Efterretningstjeneste - DDIS). In 2018. CFCS launched the Danish Cyber Situation Centre. The Cyber Situation Centre is part of the Network Security Service, whose main objective is to prevent cyber attacks.[157] In Denmark, offensive and defensive operations in cyberspace are conducted by the CFCS.[158]

5.7.3 Current structure and resources

The CFCS coordinates actions with the Danish Armed Forces at the tactical level. The effective integration of the CFCS with other types of operations (*e.g.,* land or air) depends on tactical level commanders, who are required to be familiar with the doctrine of cyber operations.[159] To support cyber operations with other types of operations, the cybersecurity liaison officer may be assigned to the tactical commands and headquarters within the Armed Forces.[160] Thus, the CFCS operates at a tactical level within the Danish Armed Forces and the cybersecurity liaison officers are assigned to the military commands to ensure integration of operations.

In 2022, Denmark launched its new National Strategy on cyber and information strategy for 2022-2024. Under the agreement, the government and the contracting parties established a cyber reserve within the defence agreement, allocating 500 million DKK to strengthen Denmark's cyber defence. The strategy additionally states that 270 million DKK has been included for 'key initiatives' in the field of Danish cybersecurity.[161]

---

[155] *Cyber Security*, Danish Ministry of Defence, 3 November 2022, https://www.fmn.dk/en/topics/cyber-security/cyber-security/ accessed: 17.03.2025.

[156] Will and Ability to take responsibility. Danish Defence and Security 2024-2033. Danish Ministry of Defence, 28 June 2023, pp. 9-10.

[157] *Centre for Cyber Security*, Danish Ministry of Defence, 3 November 2022, , https://www.fmn.dk/en/topics/cyber-security/centre-for-cyber-security/ accessed: 17.03.2025.

[158] *Joint Doctrine for Military Cyberspace Operations*, Royal Danish Defence College, September 2019, pp. 4-5.

[159] Ibid.

[160] Ibid, pp. 18-23.

[161] *The Danish National Strategy for Cyber and Information Security*, Danish Ministry of Defence, 3 November 2022, https://www.fmn.dk/en/topics/cyber-security/danish-national-strategy/ accessed: 17.03.2025.

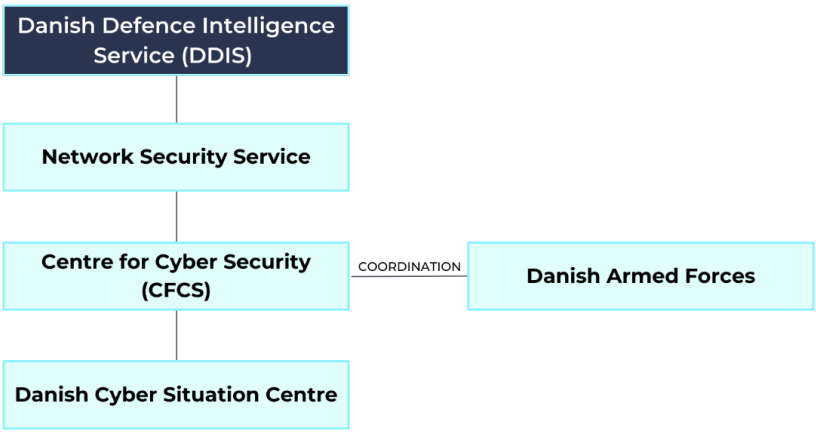


FIGURE 11. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN DENMARK.

5.8 Estonia

5.8.1 Overview of the state's cybersecurity situation

In 2023, the Estonian State Information Office documented 3,314 cyber incidents (mainly phishing, fraud, service disruption, account takeovers, and data theft). There was an increase in DDoS attacks during this period (139 in 2023). Ransomware attacks have also become a major concern, targeting sectors ranging from healthcare to industry. Estonia's cyber threats have been exacerbated by Russia's full-scale invasion of Ukraine and the renewed Israel-Hamas conflict. Analyses indicate that cyberattacks in 2023 showed a prominent level of sophistication, and many were politically motivated. Estonian entities were alleged to have lost a total of around 8.3 million € as a result of the fraud.[162]

5.8.2 History and evolution of cyber units

The Cyber Command of the Estonian Defence Forces was established on 1st of August 2018, combining the cyber competences of the defence domain. Cyber Command (est. Küberväejuhatus) was established on the basis of the Headquarters Support and Signals Battalion and the Information and Communication Systems Section of the Joint Headquarters. In nearly a year and a half of operation, Cyber Command has made significant progress in improving national cooperation and contributing to the development of a comprehensive national defence. In 2019, Cyber Command entered into a cooperation agreement with the Estonian Information System Authority (est. Riigi Infosüsteemi Amet - RIA) to strengthen cross-sector cooperation and cooperation with civilian structures.

In 2016, the US and Estonian Ministries of Defence signed an agreement to launch a collaborative project to develop an automated cyber threat intelligence sharing system between the US Air Force and the

[162] *A year of advanced threats and global tensions: Estonia's cyber security scene in 2023*, E-Estonia, 9 April 2024, https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats/ accessed: 17.03.2025.

Estonian Armed Forces. Estonia's Cyber Command has also participated in international exercises such as Cyber Coalition and Spring Storm. The most well-known training exercise supported by Cyber Command is Locked Shields, organised by NATO CCDCOE, which is based in Tallinn.[163]

Another important project was the establishment of the Estonian Cyber Defence Unit (est. Küberkaitseliit - KKL) and the Estonian Defence League (est. Kaitseliit - EDL) based on a volunteer initiative in the field of cybersecurity and technology. The first units of the Estonian Defence League were established in 2009 within the existing territorial units of the Estonian Defence League in Tartu and Tallinn. On 28th of January 2011, KKL was formally established as an extraterritorial branch within the EDL. Informally, the KKL is still also known as the (Estonian) Cyber Defence League or 'Küberkaitseliit'. A major milestone in the development of the unit was in December 2018, when the KKL headquarters in Tallinn were opened.[164]

5.8.3 Current structure and resources

The main task of Cyber Command is to conduct operations in cyberspace in order to provide command support in the area of operations of the Ministry of Defence. Within Cyber Command, we can distinguish the ICT Centre, whose task is to prepare reserve units, develop the communication rules of the Armed Forces, and handle information and communication incidents. Within the Centre are embedded Planning, Group Services Group, Chief Cryptographic Registry of the Defence Forces, Network Monitoring and Helpdesk Group, and a Frequency Management Section.[165]

Another part of the Estonian Cyber Command is the Cyber and INFOOPS Centre tasks (est. Küber- ja infooperatsiooni-de keskus), which deals with the planning and organisation of cyber and information operations. The Centre has a planning team, a CIRC, a Cyber Operations Group and a Cyber Range.[166] Another entity is the Strategic Communications Centre (est. Strateegilise kommuni-katsiooni keskus - STRATCOM), which deals with issues related to media communications and information. STRATCOM's subdivisions include the Audio, Video and Photo, Publications and Digital Media Groups.[167] The final component is the Headquarters and Support Company (est. Staabi- ja tagalakompanii), which oversees logistics and medical services. The subdivisions of the headquarters comprise the storage group, transport group, repair and maintenance group, superintendent service, and medical centre.[168] The Estonian Cyber Command employs approximately 300 people. It is located at the General Staff of the Defence Forces and the command became fully operational in 2023.[169]

---

[163] *Cyber Security in Estonia 2020*, RIA Estonia, 10 May *2020*, https://ria.ee/en/news/cyber-security-estonia-2020#The-Estonian-Defence-Forces-Cyber-Command accessed: 17.03.2025.
[164] Ibid.
[165] *Information and Communication Technology Centre*, Cyber Command: Republic of Estonia Defence Forces, https://mil.ee/en/landforces/cyber-command/information-and-communication-technology-centre/ accessed: 17.03.2025.
[166] Ibidem, *Cyber and Information Operations Centre*, https://mil.ee/en/landforces/cyber-command/information-and-communication-technology-centre/ accessed: 17.03.2025.
[167] Ibid, *Strategic Communications Centre*, https://mil.ee/en/landforces/cyber-command/information-and-communication-technology-centre/ accessed: 17.03.2025.
[168] Ibid. *Headquarters and Support Company*, https://mil.ee/en/landforces/cyber-command/information-and-communication-technology-centre/ accessed: 17.03.2025.
[169] *Gallery: Eesti küberväejuhatus asus tööle*, ERR, 1 August 2018, https://www.err.ee/850643/galerii-eesti-kubervaejuhatus-asus-toole accessed: 17.03.2025.

FIGURE 12. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN ESTONIA.

5.9 Finland

5.9.1 Overview of the state's cybersecurity situation

Finland's cybersecurity underwent a fundamental transformation after the start of the NATO accession process, which was finalised in 2023. The Finnish authorities are preparing the public for cyber attacks on the premise that even the technically simplest DDoS attacks can effectively disrupt the functioning of the state. Since the beginning of 2019, there has been an increase in the number of attempted cyber attacks on Finland, although they have not been successful. Finland's application for membership of the NATO has increased the threat level of cyber attacks from Russia. As early as the beginning of March 2022, Finnish services reported on possible attempts by the Kremlin to influence Finnish public opinion. The warnings included the possibility of using both traditional and novel methods, such as deepfake recordings.[170]

The most common cyber threats in Finland include ransomware, denial-of-service attacks and data leaks. Attacks on IT service providers have also become more prevalent.[171] The number of malware sightings in Finland has fluctuated greatly between 2019 and 2023. The number of detected malware and malicious traffic peaked at around 81,000 incidents in the third quarter of 2021. The lowest number – 16,752 incidents – was reported in the third quarter of 2019.[172]

Finland focuses on countering cyber threats at the institutional level. This involves spreading awareness and suggesting strategies for organisations. The government noted that raising security from within companies allows for an overall increase in the country's cybersecurity. Guides such as what to do in the event of a ransomware attack on organisations are publicly available on the official website of the National

[170] K. Kaczmarek, *Finland in the light of cyber threats in the context of Russia's aggression against Ukraine*, "Cybersecurity and Law", vol. 9, no.1, War Studies University, p. 205.
[171] K. Kaczmarek, *Finland in the light of cyber threats in the context of Russia's aggression against Ukraine*, "Cybersecurity and Law", vol. 9, no.1, War Studies University, pp. 206-212.
[172] J. Clausnitzer, *Number of malware incidents in Finland Q3 2019-Q3 2023*, Statista, 30 November 2023, https://www.statista.com/statistics/733010/number-of-malware-incidents-per-quarter-in-finland/, accessed: 17.03.2025.

Cybersecurity Centre (Suomi Traficomin Kyberturvallisuuskeskus – TRAFICOM).[173] The centre itself also allows ordinary users to report a cybersecurity incident and offers initial solutions to a case.[174]

The Kybermittari (Cybermeter) tool, developed by the National Cybersecurity Centre, helps business managers and organisations to better control cyber threats and protect the continuity of business operations. Kybermittari shows the level of identification, protection, detection, response and recovery in the context of cyber threats in organisations. The tool also provides managers with valuable information on their preparedness for cyber threats compared to the average level in their sector.[175]

5.9.2 History and evolution of cyber units

In 2019, Finland revised its previous cyber strategy from 2013 to support the development of its cybersecurity and protect key components necessary for digital services. In line with this strategy, Finland has delegated cybersecurity matters to several government entities, including the Security Committee, which is responsible for making recommendations on cybersecurity issues as requested by the Ministry.[176]

The Finnish Defence Forces C5 Agency (suomi. Puolustusvoimien johtamisjärjestelmäkeskus - PVJJK30/FDFC5A) was established in 2007 after the merger of the FDF IT Centre and the National Defence Management Departments and IT centres. In 2013, a Security Committee was established within the Ministry of Defence, which also deals with cybersecurity issues. In 2014, the National Cybersecurity Centre (NCSC-FI) was established.[177] Finland has been conducting a 'cyber recruitment' campaign since 2015. The annual intake of cyber recruits ranges from two to twenty candidates.[178] Currently, Finland's cooperation with the EU and NATO primarily involves incident information exchange, capacity development, training and exercises.

5.9.3 Current structure and resources

Finnish Defence Forces C5 Agency provides IT services to the Defence Forces. One of its remits is cyber defence. The Agency is a subordinate institution of the Finnish Defence Command and operates from 17 locations across Finland. C5 currently employs approximately 500 employees, mostly civilians. The Agency comprises the following departments: the Headquarters (HQ), an IT Services Department, 4 CIS Support Departments, the Cyber Department, and the C5I School. HQ deals with the monitoring and control of the Finnish forces' technical systems. In addition, it is the executive office and provides expert support to other departments. The IT Services Department provides services for operational information

[173] What to do in case of ransomware incident - instructions for management, 15/2022, TRAFICOM, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/What%20to%20do%20in%20case%20of%20a%20ransomware%20incident%20-%20instructions%20for%20management.pdf, accessed: 17.03.2025.
[174] E-services, TRAFICOM, https://www.kyberturvallisuuskeskus.fi/en/contact-us/e-services, accessed: 17.03.2025.
[175] Kybermitarii, TRAFICOM, https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter, accessed: 17.03.2025.
[176] S. Himka, *Analyzing Finland's and NATO's Cybersecurity Strategies*, The Henry M. Jackson School of International Studies, 20 October 2023, https://jsis.washington.edu/news/analyzing-finlands-and-natos-cybersecurity-strategies/, accessed: 17.03.2025.
[177] R. S. Dewar, *National Cybersecurity and Cyberdefence Policy Snapshots*, Center for Security Studies, September 2018, pp. 32-33.
[178] M. Hurt, T. Sõmer, *Cyber Conscription Experience and Best Practice from Selected Countries*, International Centre for Defence and Security, February 2021, p. 5.

systems and integrates acquired ICT services into the Defence Force. The CIS support departments produce operational IT support for management units, support training activities and maintain security technology. The Cyber Department protects data networks and services and develops cyber defence, maintaining the cyber situational awareness of the Defence Force. As Finland does not have a separate Cyber Command, the commander of the C5 Agency, General Janne Jaakkola, is also the Commander of the Finnish Defence Forces.[179]

Finland's cyber defence has become an integral part of its cooperation with NATO, emphasising the exchange of incident information, joint exercises and the development of defence capabilities. Finland has been successively developing its cybersecurity structures and resources via the activities of the C5 Defence Forces Agency and the National Cyber Security Centre. This has made the country more resilient to cyber attacks and able to respond quickly to hybrid threats.[180] It must be added that Finland does not officially confirm whether it has offensive cyber capabilities.

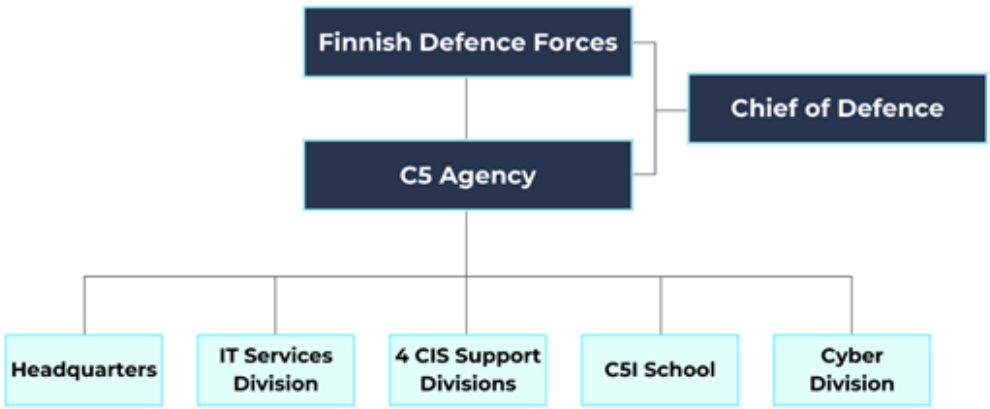


FIGURE 13. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN FINLAND.

5.10 France

5.10.1 Overview of the state's cybersecurity situation

The French National Cybersecurity Agency (fr. Agence nationale de la Sécurité des systèmes d'information - ANSII) confirmed that levels of cyber espionage remained high in 2023, with a significant increase in the frequency of attacks on those individuals and non-governmental structures that create, host or transmit sensitive data. An emerging trend involved the exploitation of corporate and personal mobile phones, which were targeted for espionage. There has also been an increase in the number of attacks believed to be conducted by the Russian Federation. Cyber attacks also remained elevated in 2023, as evidenced by the total number of ransomware attacks reported to ANSSI, which were 30% higher than for the same period in 2022. The Agency noted new destabilisation operations aimed primarily at promoting political discourse, obstructing access to online content, or damaging an organisation's image.

[179] *Finnish Defence Forces C5 Agency*, The Finnish Defence Forces, https://puolustusvoimat.fi/en/about-us/c5-agency, accessed: 17.03.2025.

[180] More information on Finland's cybersecurity can be found in the latest report from the Finnish Cybersecurity Strategy 2024-2035: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf accessed: 17.03.2025.

The most common incidents were DDoS attacks conducted by Russian hackers.[181] Approximately 83% of cyber incidents in France do not have a specific country of origin, although if a state actor responsible for the cyber attacks can readily be identified, it is the Russian Federation in 6 of every 11 cases. Other nations identified as the countries of origin of such incidents include China, Iran, North Korea, Türkiye, Bangladesh and France itself. Institutions of the French State were amongst those affected in 35 of the 64 incidents reported. The most common type of incident was 'hijacking' (*e.g.,* by phishing).[182]

5.10.2 History and evolution of cyber units

In 2009, France established the National Cyber Security Agency (ANSSI) to better allocate roles between institutions. The 2011 National Cyber Security Strategy reaffirmed the objective of creating a centralised cyber model, with the government seeking to protect critical private actors. The 2013 Defence White Paper outlined France's cyber ambitions and its intention to treat major cyber attacks as 'acts of war'. At the end of 2016, M. Le Drian, the French Defence Minister, brought together the disparate elements of cyber doctrine in a speech in which he announced the creation of a French Cyber Command.[183]

In 2017, the French Cyber Defence Command (fr. Le commandement de la cyberdéfense - COMCYBER) was created. The 2019 Public Elements for the Military Cyber Warfare Doctrine document formalised cyber operations as part of the French Armed Forces' activities, stating that the Ministry of the Armed Forces has the capacity and doctrine to conduct offensive cyber operations pertaining to the duties of the armed forces.[184] COMCYBER has since consolidated its operations into two structures.[185] The first is the Cyber Defence Command (*fr. état-major de la cyberdéfense* – EM-CYBER), which conducts operations through the Cyber Operations Centre (CO-CYBER) and the second, established in 2020, is the Armed Forces Cyber Defence Group (*fr. groupement de la cyberdéfense des armées* – GCA), which brings together and coordinates several specialised cyber defence centres.[186]

5.10.3 Current structure and resources

COMCYBER brings together all the Cyber Defence Forces of the Ministry of the Armed Forces. It is directly subordinate to the Chief of Defence Staff (fr. Le chef d'état-major des armées - CEMA). COMCYBER assists and advises the Minister of the Armed Forces in his area of specialisation. COMCYBER consists of the already mentioned EM-CYBER and the GCA which groups together centres specialising in cyber defence like the Centre for Defensive Computer Warfare Analysis (fr. Le Centre

[181] *ANSSI publishes the 2023 Cyber Threat Overview*, French Cybersecurity Agency, 14 May 2024, https://cyber.gouv.fr/en/actualites/anssi-publishes-2023-cyber-threat-overview accessed: 17.03.2025.
[182] *Most cyber incidents in France have unidentified origins*, Surfshark, 3 September 2024, https://surfshark.com/research/chart/cyber-attacks-france accessed: 17.03.2025.
[183] B. Toucas, *With Its New 'White Book,' France Looks to Become a World-Class Player in Cyber Space'*, War on the Rocks, 29 March 2018, https://warontherocks.com/2018/03/with-its-new-white-book-france-looks-to-become-a-world-class-player-in-cyber-space/ accessed: 17.03.2025.
[184] K. Bojarski, *France and its doctrine of cyber operations - offensive actions*, Counterintelligence.co.uk, 8 July 2022, https://counterintelligence.pl/en/2022/08/francja-i-jej-doktryna-operacji-cyber-dzialania-ofensywne/ accessed: 17.03.2025.
[185] A. Olech, *Zagraniczna aktywność militarna Republiki Francuskiej*, Poznań 2022, Wydawnictwo Kontekst.
[186] *#NotreDéfense : Le COMCYBER, une unité opérationnelle en charge de la manœuvre cyber globale*, État-major des armées, 17 March 2021, https://www.defense.gouv.fr/ema/actualites/notredefense-comcyber-unite-operationnelle-charge-manoeuvre-cyber-globale accessed: 17.03.2025.

d'analyse en lutte informatique défensive - CALID); the Information Systems Security Audit Centre (fr. Le Centre d'audits de la Sécurité des systèmes d'information - CASSI); the Operational Preparation Cyber Centre (fr. Le centre cyber de préparation opérationnelle - C2PO); and the Main Certification Authority for the Armed Forces (fr. Le centre des homologations principales interarmées – CHPI).[187]

Of equal importance, the Digital and Cyber Support Brigade (fr. Brigade d'Appui Numérique et du Cyber - BANC) is a specialised unit of the French Army. This was created in 2024 as part of the transformation of the Information and Communications Systems Command (fr. Commandement des systèmes d'information et de communication - COMSIC) into the Land Digital and Cyber Support Command (fr. Le Commandement de l'Appui Terrestre Numérique et Cyber - CATNC). This brigade specialises in mastering the digital and cyber domains and is an essential component of the arsenal of the French Armed Forces.[188]

The 2024-2030 Military Spending Planning (fr. La loi de programmation militaire - LPM) Act makes provision of 4 billion € for 'planned cyber needs'. In 2023, the number of military cyber operators was confirmed as 3,502, with nearly 1,100 positions left vacant. The current LPM has increased the maximum number of cyber operators by 953, which, by 2030, will bring the maximum number of military positions within this domain to 5,553.[189] ANSSI and COMCYBER work directly with French technology companies (including Thales, Airbus, and Atos) to develop cybersecurity innovations for military and civilian applications.

Based on an analysis of French documents, it is clear that the doctrine is quite transparent and that Paris does not marginalise defence in cyberspace.[190] Such a course of action, at a time of increasing activity in this area, seems more sensible than innovative. Moreover, the demarcation of cyberspace troops as a separate pillar of the armed forces appears imminent.

[187] Ibid.

[188] Ministere des Armees, *Brigade d'Appui Numérique et du Cyber (BANC)*, https://www.defense.gouv.fr/terre/unites-larmee-terre/nos-brigades/brigade-dappui-numerique-du-cyber-banc , https://www.defense.gouv.fr/terre/unites-larmee-terre/nos-brigades, accessed: 17.03.2025.

[189] *Pour une coordination de la Cyberdefense plus offensive dans la loi de programmation militaire 2024-2030*, Commisions des affaires etrangeres et de la defense, 24 May 2023, pp. 1-3.

[190] L. Olejnik, *French doctrine of information operations - engaging over information space*, https://blog.lukaszolejnik.com/french-doctrine-of-information-operations-engaging-over-information-space/?fbclid=IwAR3QJwPjd8MJCDLij3CFlBlaYBGRwa-PREuv3E00fBeWYc9Zvh_PDJxRH7I, accessed: 17.03.2025.

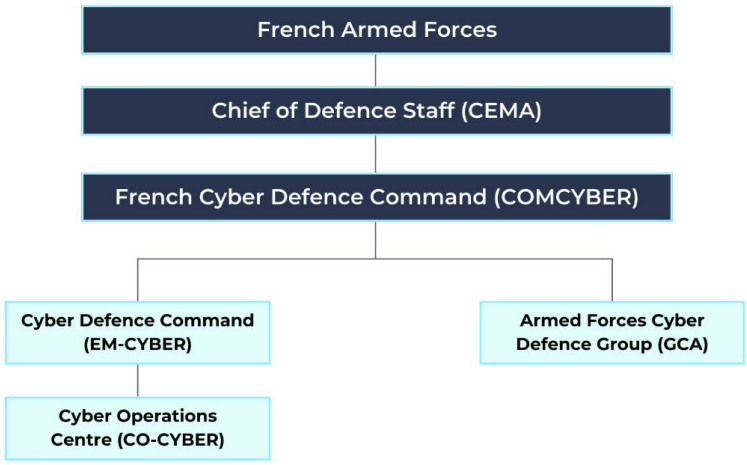


FIGURE 14. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN FRANCE.

5.11 Germany

5.11.1 Overview of the state's cybersecurity situation

A report published by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik; BSI) in November 2023 provided an update on the cybersecurity situation in Germany. The authors suggested that cyber criminals were expected to make changes in the selection of their 'victims', as ransomware attacks had primarily been targeting small and medium-sized organisations as well as state institutions and municipalities. Previously, the majority of attacks had been directed toward large enterprises, with industry being one of the three primary targets for these attacks. In addition, abuse of German residents was widespread, with such methods as phishing and sextortion dominating.[191]

The increasing professionalisation of cybercriminals and the spate of vulnerabilities being discovered in software, which are often exploited during attacks, were identified as a real threat. Opportunities for cybercriminals are also opening up with the development of AI, which can authenticate phishing messages, contribute to disinformation campaigns on social networks, and even autonomously generate malicious code. In contrast, the DDoS attacks by Russian activists recorded by the BSI caused, at worst, only 'minor' permanent damage. The Federal Office classifies these attacks as propaganda aimed at creating uncertainty and undermining trust in the state.[192]

5.11.2 History and evolution of cyber units

A key year for the German approach towards cyber forces was 2016, which saw the publication of the second version of the National Security Strategy (NCSS), the White Paper on German Security Policy

[191] *The State of IT Security in Germany*, Federal Office for Information Security, 2 November 2023, https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html accessed: 17.03.2025.
[192] Ibid.

and the German Security Policy Concept. The aforementioned White Paper placed a strong emphasis on cyber threats to the German Armed Forces. However, it was unclear regarding the types of cyber capabilities and operations that the Bundeswehr wanted to develop. Nevertheless, in 2017, the 'Cyber and Information Domain Service' (CIR) was established, and a year later, a conceptual paper (the 'Concept for the German Armed Forces') was released, explaining that the Bundeswehr intended to develop the full spectrum of offensive and defensive operations in cyberspace. The ensuing version of Germany's National Cyber Security Strategy 2021 also played a significant role.

Russian aggression against Ukraine in 2022 triggered a strong reaction in Germany. In June, Germany announced an increase in defence spending of 100 billion €, of which 21 billion € was allocated for communication systems and cyber capabilities. In November 2022, Germany's cyberspace personnel stood at around 14,500. A Joint Intelligence Centre was also established in 2020. There are also plans to establish a Cyber Warfare and Information Centre[193]. On the 4th of April 2024, Germany's Defence Minister, Boris Pistorius, presented a restructuring plan for the Bundeswehr, under which the Cyber and Information Warfare arena was transformed into a distinct fourth branch of the armed forces.[194]

5.11.3 Current structure and resources

The Bundeswehr Communication and Information Systems Command (CISC) is responsible for providing training at the Bundeswehr Communication and Information Systems School, and is responsible for operating the Bundeswehr IT system at the Bundeswehr Communication and Information Systems Service Centre and exercising C2 over the soldiers of six Communication and Information Systems Support Battalions as well as the NATO interface – the 1st NATO Communication Battalion.

Strategic Reconnaissance Command (SRC) operates within the CIR. It comprises four battalions and provides information for early threat intelligence and support for the Federal Armed Forces (Bundeswehr) operations abroad. The Bundeswehr's Technical Analysis Centre for Signal Intelligence and the Intelligence Centre are also part of the cyber forces structures. The last element is the Bundeswehr Geoinformation Centre, and provides the armed forces and the Federal Ministry of Defence with information on all geospatial factors.[195] Within the Cyber and Information Domain Service, some 16,000 military and civilian personnel currently work across 25 departments, with the HQ located in Bonn.[196]

[193] *Cyber Capabilities And National Power Volume 2*, The International Center for Strategic Studies, vol. 2, 7 September 2023, pp. 47-49.
[194] L. Gibadło, J. Gotkowska, *Nowy plan restrukturyzacji Bundeswehry*, Ośrodek Studiów Wschodnich, 11 April 2024, https://www.osw.waw.pl/pl/publikacje/analizy/2024-04-11/nowy-plan-restrukturyzacji-bundeswehry, accessed: 17.03.2025.
[195] *Cyber and Information Domain Service*, Bundeswehr, https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service, accessed: 17.03.2025.
[196] Ibid.

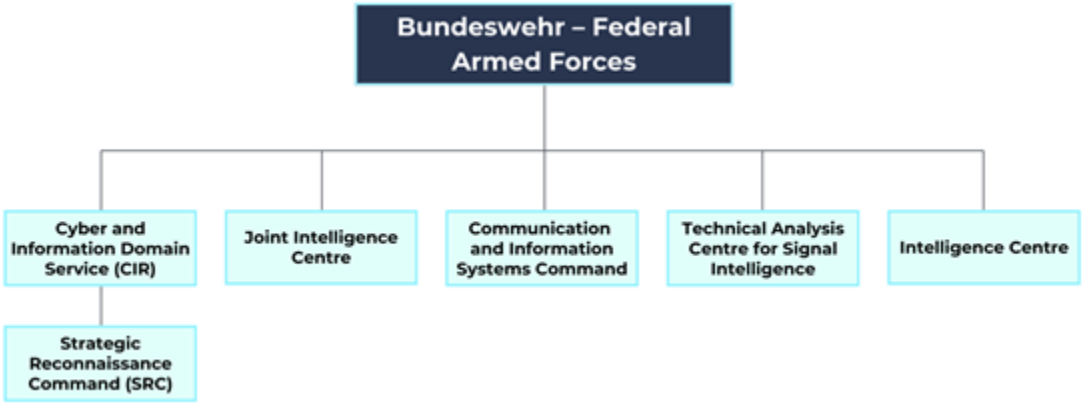


FIGURE 15. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN GERMANY

5.12 Greece

5.12.1 Overview of the state's cybersecurity situation

Like other countries, Greece has experienced an increase in cyberattacks, prompting the country's cybersecurity programme to become a top national security priority. Recent cyber incidents have affected critical infrastructure, namely the National Natural Gas System Operator (gr. Ο Διαχειριστής Εθνικού Συστήματος Φυσικού Αερίου - DESFA). This has negatively affected the availability of natural gas. Critical infrastructure itself remains vulnerable to advanced cyberattacks, with criminals being able to take remote control of essential infrastructure components. The reason for this is that energy systems, such as power plants, are often based on outdated technologies that were not designed with modern cyber threats in mind.[197]

Another significant cyber attack caused the Hellenic Post's (gr. Ελληνικά Ταχυδρομεία - ELTA) computer systems to crash, leading to the temporary suspension of commercial services at all post offices. In turn, the launch of a DDoS attack on Greece's national online exam platform for secondary schools caused delays and disruption for students across the country. The Greek Ministry of Digital Governance is spearheading a digital transformation initiative, as can be seen from the provisions of the Digital Transformation Bible 2020-2025.

Another important document is the National Cyber Security Strategy 2020-2025. In view of the increasing number of attacks on critical infrastructure, in 2024, the Ministry of Governance established the National Cyber Security Authority (NSCA) as a new body that is an extension of the General Directorate of Cyber Security. It is to be headed by a cybersecurity expert, appointed for a five-year term. The Authority is to facilitate the implementation of EU legislation (with NIS Directive 2 being a priority) and strengthen Greece's cyber defences.[198] Such a vulnerability to cyberattacks carried out by online criminals indicates

[197] Alexios Lekidis, 'Cyber-attack TTP analysis for EPES systems', arXiv, 17 February 2023, https://doi.org/10.48550/arXiv.2302.09164. accessed: 17.03.2025.
[198] *Greece Information Technology National Cybersecurity Strategy*, U.S International Trade Administration, 7 October 2024, https://www.trade.gov/market-intelligence/greece-information-technology-national-cybersecurity-strategy accessed: 17.03.2025.

the weakness of the security measures of Greek entities, some of which remain completely unaware that they have become the targets of cybercriminals.[199]

5.12.2 History and evolution of cyber units

In 2004, the Cyber Defence Directorate (CDD) was created within the Hellenic National Defence General Staff (gr. ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ - Hellenic National Defence General Staff (HNDGS)).[200] It is responsible for the coordination and implementation of cyber defence operations at strategic, operational and tactical levels in times of peace, crisis, or war. Its primary objective is to protect the information infrastructure of the Greek Armed Forces and the Ministry of Defence. The CDD is also responsible for organising the annual national cyber defence exercise (PANOPTES) and conducting cyber defence training for military and public sector personnel at two schools on cybersecurity and cyber defence concepts and practices. The Directorate's personnel are also trained by NATO CCDCOE and participate in Alliance exercises, including Crossed Swords, Locked Shields, and Cyber Coalition.[201]

Published in 2020, the National Cyber Security Strategy 2020-2025 indicates the level of functioning of the General Directorate for Cyber Security within the HNDGS. It is considered the National CSIRT, and its purpose is to mitigate incidents in the military sector, as well as to conduct cyber defence. The Directorate's overarching mission is cybersecurity and a risk reduction in communications.[202] The HNDGS participated in the annual NATO cybersecurity exercise 'Cyber Coalition 2023' in Tallinn, Estonia.[203]

5.12.3 Current structure and resources

In 2024, the decision to create a cyber unit was taken and 'Unit 1864' was established, a dedicated cyber defence unit with a remit to prevent threats and improve cybersecurity. The cyber defence unit can carry out defensive operations such as the detection of cyber attacks or provide incident response support, both inside and outside the organisation, with a view to defending critical infrastructure. Greek authorities, however, emphasise that they conduct mainly defensive operations in cyberspace.

There are plans to improve the organisational structure and recruit talented personnel in line with the provisions of the new law. Cooperation between the public and private sectors is described as crucial. For this reason, with the creation of Unit 1864, an entity called the 'Hellenic Centre of Defence Innovation' has been established to align the public and private sectors.

Despite the emerging cyber threat, Greece's annual defence budgets mainly take into account conventional systems, including the air force and navy. There is currently no data on the funding of the Greek cyber military. However, it can be assumed that these amounts are marginal relative to the expenditure allocated to the purchase of F-35 and Rafale aircraft.[204]

---

[199] E. Stamatouku, *Greece Moves to Enhance Cyber Security Amid Frequent Attacks*, Balkan Insight, 11 December 2023, https://balkaninsight.com/2023/12/11/greece-moves-to-enhance-cyber-security-amid-frequent-attacks/ accessed: 17.03.2025.
[200] *Initiatives to improve Cyber Defence capabilities - development of NATO cyber forces* -
[201] *The Cyber Defence Directorate...*, CERTCOOP, https://www.certcoop.gr/index.php/hcdd/ accessed: 17.03.2025.
[202] National Cybersecurity Strategy 2020-2025, National Cybersecurity Authority, p. 29.
[203] *Greek Armed Forces Take Part in NATO 2023 Cyber Exercise*, Tovima.com, 5 December 2023, https://www.tovima.com/politics/greek-armed-forces-take-part-in-nato-2023-cyber-exercise/ accessed: 17.03.2025.

[204] *Greece - Country Commercial Guide - Defense*, U.S International Trade Administration, 28 December 2023, https://www.trade.gov/country-commercial-guides/greece-defense accessed: 17.03.2025.

FIGURE 16. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN GREECE.

5.13 Hungary

5.13.1 Overview of the state's cybersecurity situation

Since April 2023, at least 40 different media sites in Hungary have been the target of DDoS attacks. These included leading independent media which have been critical of Prime Minister Viktor Orbán's government, including Telex, HVG, 444.hu, Magyar Hang and Népszava. In contrast, these cyber attacks bypassed all media supporting the ruling Fidesz Party, suggestive of a political or ideological motive. Despite this, no group has claimed responsibility, and the attacks have been attributed to hacker organisations.

However, such attacks have happened before. In 2022, the website of the United Opposition Movement fell victim to a major DDoS attack. The timing was significant, as the site was hosting primaries for its prime ministerial candidate. Simultaneously, DDoS attacks targeting independent media portals were organised. In March, hackers claiming to be members of the Anonymous group attacked right-wing and conservative-affiliated media, citing their support for the Russian invasion of Ukraine. Further, in July 2023, the Budapest Pride website was suspended for several hours on the day of LGBTQ+ related events in the capital.[205]

5.13.2 History and evolution of cyber units

Hungary joined the NATO CCDCOE in June 2010 as a sponsor state. Two years later, Budapest adopted Hungary's National Military Strategy, in which cyberspace was recognised as the fifth domain of warfare. In 2013, the Ministry of Defence issued the Hungarian Defence Forces' Cyber Defence Concept. The establishment and development of a Military Computer Incident Response Capability (Mil-CIRC) by the Military Security Service was commissioned by the Minister of Defence in late 2014; subsequently, the Military Computer Emergency Response Team (Mil-CERT) was established.[206]

The National Security Strategy was adopted by the Hungarian government in 2021. It required the Hungarian Defence Forces (hun. Magyar Honvédség - HDF) to establish effective capabilities against

[205] *Hungary: DDoS cyberattacks pose major new threat to media freedom*, International Press Institute, 29 August 2023, https://ipi.media/hungary-ddos-cyber-attacks-pose-major-new-threat-to-media-freedom/ accessed: 17.03.2025.
[206] L. Kovacs, G. Szentgali, National Cyber Security Organisation: Hungary, NATO CCDCOE, Tallinn 2015, pp. 10-11.

cyber attacks and hybrid warfare. Based on this doctrine, an independent cyber defence unit was created within the Defence Forces, which performs the core tasks of defending the HDF and securing it against attacks.[207]

5.13.3 Current structure and resources

The current structure of Hungary's military cyber forces focuses on cyber defence and the development of cyber defence capabilities within the Hungarian Defence Forces. The Hungarian Defence Forces Cyber Operations Command (hun. Magyar Honvédség Kiberhadműveleti Parancsnoksága) is subordinated to the General Staff (hun. Honvéd Vezérkar). In 2023, Hungary opened the CyOC under the Military National Security Service, to which the Centre is subordinated.[208] The personnel and budget allocations for the military cyber component are as yet unknown. Hungary's cyber forces and cybersecurity operate based on the governance of the 2021 document 'National Military Strategy of Hungary'. Hungary is a member of the NATO CCD COE,[209] in which it actively participates in cyber defence capability development activities. The country also places a strong emphasis on education, research, development and consultation in this field.

FIGURE 17. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN HUNGARY.

[207] A. Bencsik, M. Karpiuk, *The legal status of the cyberarmy in Hungary and Poland. An overview*, 'Cybersecurity and law', no. 2, vol. 10, pp. 22-25.
[208] *New Military Cyberspace Command Inaugurated*, Hungary Today, 3 October 2023, https://hungarytoday.hu/new-military-cyberspace-command-inaugurated/ accessed: 17.03.2025.
[209] *Hungary joins the Centre*, CCDCOE, https://ccdcoe.org/news/2010/hungary-joins-the-centre/ accessed: 17.03.2025.

5.14 Iceland

5.14.1 Overview of the state's cybersecurity situation

Iceland currently ranks 10th among European countries in terms of cybersecurity. In 2020, it ranked 31st.[210] In 2022, there were 700 cases of cyberattacks in Iceland. The year before, companies and individuals were attacked 600 times, and in 2020, only 266 times.[211] In April 2015, the Minister of the Interior published the National Cybersecurity Strategy, which covers the period 2015-2026.[212] It is worth noting that Iceland does not have a regular army, and its security is guaranteed by countries such as the US, Norway and Denmark.

In June 2024, Árvakur, the parent company of Iceland's major news services (including Morgunblaðið and the K100 radio station), fell victim to a sophisticated cyber attack attributed to a Russian group known as Akira. Four months earlier, the University of Reykjavík reported a massive breach in which hackers obtained approximately 185 gigabytes of sensitive data. Cyber operations also targeted the Icelandic energy sector, with repeated attacks attributed to Russian-based threat actors based on IP addresses. In response to the adversaries, Iceland strengthened its cybersecurity measures through national exercises and closer cooperation between key stakeholders in the energy sector.[213]

5.14.2 History and evolution of cyber units

Iceland's national security and defence strategy is based on the country's cooperation with NATO, active cooperation with other Nordic countries, and a defence agreement with the US. The country's cyber capabilities have been developed through international cooperation and civilian actors. In 2013, the Icelandic Government established the Computer Emergency Response Team (CERT-IS).

Investments have also been made in modernising the public sector's digital infrastructure through initiatives such as Digital Iceland, which was launched in 2018. Three years later, the Icelandic Government published a comprehensive National Cybersecurity Strategy 2022-2037. This document emphasises the importance of international cooperation, particularly with bodies such as NATO and the EU, which is expected to strengthen Iceland's cyber defences. In addition, the document presents plans for comprehensive training, the integration of curriculum, as well as the establishment of a dedicated cybersecurity institution. In March 2023, Iceland became a formal member of NATO CCDCOE.[214] In 2023, a joint team from Iceland and Sweden won NATO's largest cyber defence exercise, Locked Shields. This participation underscores Iceland's commitment to strengthening its cyber defence capabilities and enhancing its cooperation with international partners.

---

[210] *Iceland among the best countries in the field of cyber security*, Iceland Monitor, 15 September 2024, https://icelandmonitor.mbl.is/news/news/2024/09/15/iceland_among_the_best_countries_in_the_field_of_cy/ accessed: 17.03.2025.

[211] A. Petrosyan, *Total number of cyberattacks in Iceland from 2020 to 2023*, Statista, 18 June 2024, https://www.statista.com/statistics/1473652/denmark-cyberattacks-number/ accessed: 17.03.2025.

[212] *Iceland*, Cyberwiser.eu, https://cyberwiser.eu/iceland accessed: 17.03.2025.

[213] C. Ayliffe, *Safeguarding Iceland's Digital Horizon: The Urgent Call for Proactive Cybersecurity*, Nanitor, 25 June 2024, https://nanitor.com/resources/blog/cyber-exposure-alerts/safeguarding-icelands-digital-horizon-the-urgent-call-for-proactive-cybersecurity/ accessed: 17.03.2025.

[214] J. Sigholm, *The Case for an Icelandic Cyber Exploitation and Defense (ICED) Force for NATO Coalition Operations*.

5.14.3 Current structure and resources

There is currently no separate cyber unit in Iceland due to the absence of any formal armed forces. Moreover, Iceland has not appointed a Minister of National Defence within its government, and national security issues are handled within the Ministry of Foreign Affairs. The Icelandic Ministry of Foreign Affairs has a functional department in the form of the Directorate of Defence, and issues related to the military dimension of cybersecurity may be dealt with by this unit. While Iceland does not have a formal military, the country works closely with other NATO allies on cybersecurity, and cyber units are being developed within the NATO CCDCOE. The need to strengthen security capabilities in the cyber domain is emphasised in Iceland's National Cyber Security Strategy 2022-2037, which was published in February 2022.[215]

The key objectives of the strategy focus on two main pillars: the development of exceptional competence in cybersecurity and the establishment of a secure Internet environment. To enhance cybersecurity knowledge and skills, the strategy emphasises the importance of public education, research, and international cooperation. It aims to strengthen national capabilities to prevent, respond to, and mitigate cyber attacks through the adoption of advanced technologies and best practices. At the same time, it seeks to create a safer digital space by aligning legal frameworks with international standards, thereby improving the effectiveness of law enforcement in cyberspace. Special attention is given to the protection of vulnerable groups, particularly children, and to bolstering the resilience of critical infrastructure through improved security measures and comprehensive risk assessments.

Recently, Reykjavík established the National Coordination Centre (Eyvör NCC-IS). Eyvör NCC-IS serves as Iceland's pivotal point for cybersecurity coordination. It facilitates collaboration among national and European cybersecurity entities, disseminating relevant outcomes, and supporting capacity-building initiatives across various sectors.

FIGURE 18. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN ICELAND.

5.15 Italy

5.15.1 Overview of the state's cybersecurity situation

The Italian Cyber Security Department, officially known as the National Cybersecurity Agency (ACN), was established with Decree-Law No. 82 on June 14, 2021. The Agency's goal is to protect national interests in cyberspace, coordinating public actors involved in cybersecurity and promoting Italy's digital strategic

[215] *Icelandic National Cybersecurity Strategy 2022-2037*, Government of Iceland, February 2022.

autonomy. Among the main functions of the ACN are the prevention and mitigation of cybersecurity incidents, supporting public administrations and businesses in managing cyber threats, promoting cybersecurity culture through training and awareness programmes, and supervising and certifying IT products and services.

The Director General of ACN also coordinates the work of the Inter-Ministerial Committee on Cyber Security (it. Comitato Interministeriale per la Cybersicurezza - CIC), which is made up of ministers responsible for key areas of national security. The Committee develops a cybersecurity strategy, oversees its implementation and coordinates the prevention and response to cyber threats by public institutions.[216] In 2023, the ACN managed 1,411 cyberattacks, representing a 29% increase from the previous year. The most severely affected sectors were telecommunications and central/local public administration, with a significant rise in DDoS, phishing, and ransomware attacks.

The Agency is also the national reference point for the National Coordination Centre (NCC-IT), which supports the mission of the European Cybersecurity Competence Centre (ECCC) in strengthening the EU's strategic autonomy and developing technological and industrial capabilities within the cybersecurity field.

In January 2025, a pro-Russian hacking group claimed responsibility for cyber attacks targeting Italian government websites, including ministries and public services. This was reportedly in response to Italy's support for Ukraine.[217]

5.15.2 History and evolution of cyber units

As early as 2013, the Italian Ministry of Defence recognised cyber attacks as a threat to national defence and demarcated cyberspace as a fifth domain of war. In 2015, Rome issued a White Paper on International Security and Defence, recognising the need to create operational defence capabilities within the cyber domain. Cyber defence was also formally addressed in the Ministry of Defence's official multi-year planning document for 2019-2021.

In 2017, Italy established a military command which is solely responsible for conducting cyber operations – the Joint Cyber Command (it. Comando Interforze Operazioni Cibernetiche - CIOC). The command reached full operational capability in 2019. The Cyber Command was physically located within the CERT of the Italian Armed Forces (CERT Difesa – CERT-D).[218]

In 2020, this entity was integrated into the Network Operations Command (it. Comando per le Operazioni in Rete – COR), which was also established in 2020. The basis of this mission is to strengthen Italy's defence capabilities in cyberspace and to support NATO in cyber operations. As an integral part of the

---

[216] *Il Dominio cyber: il quadro normativo nazionale ed internazionale per la conduzione di operazioni cibernetiche, tra limiti di sviluppo e impiego dell'arma cibernetica*, Istituto Superiore di Stato Maggiore Interforze, 25° Corso - 3a Sezione - 9° Gruppo di Lavoro, Centro Alti Studi per la Difesa, 2024, https://www.difesa.it/assets/allegati/46666/9_gdl_25_issmi_-as_smd_05-_as_sdm_16.pdf. accessed: 17.03.2025.

[217] TVP World, *Pro-Russian hackers target Italian government and public service websites*, https://tvpworld.com/84466557/-pro-russian-hackers-target-italian-government-and-public-service-websites, accessed: 17.03.2025.

[218] S. De. T. Colatin, *National Cybersecurity Organisation: ITALY*, NATO CCDCOE, Tallinn 2020, pp. 17-18.

Italian defence system, COR participates in exercises such as Joint Stars 25, which aim to improve operational capabilities in new operational domains such as space.[219]

5.15.3 Current structure and resources

The COR operates under the supervision of the Chief of Defence Staff and collaborates with the cyber defence and cybersecurity units of the Land Forces, Navy and Air Force[220] whose representatives serve as part of the Operations Command.

The Cyber Operations Command (COR) comprises three key departments. Department C4 is responsible for the technical and operational management of defence ICT systems, including the Defence Transport Network (DIFENET), configuration control of systems, and service quality assurance. The Department of Security and Cyber Defence ensures an appropriate security posture by monitoring cyber threats, conducting vulnerability analyses, and managing the digital certification system for the Armed Forces. Finally, the Department of Cyber Operations is tasked with planning and conducting military operations in cyberspace to neutralise threats. It also supports training, doctrinal development, and innovation within the field of cyber defence. The Network Operations Command (COR) conducts defensive and offensive cyber operations, plans military activities and supports NATO in cyber operations.

At the tactical level, an example of a unit operating in cyberspace is the 9th Cybernetic Security Regiment "Rombo" of the Italian Army. On the 9th October 2023, the existing Cybernetic Security Unit of the ITA Army was assigned the name, flag and traditions of the 9th Electronic Warfare Battalion, or "Rombo", before being renamed the 9th Cybernetic Security Regiment "Rombo".

The Regiment is part of the Signal Arm and assigned to the Tactical Intelligence Brigade, which is tasked with performing cyber operations related to the defence of the Italian Army's IT networks and command-and-control systems to protect critical infrastructure, platforms and weapon systems.

The 9th Cyber Security Regiment "Rombo" comprises a Command and Support Company and a Cybersecurity Battalion. The Battalion is formed from the 1st Cybersecurity Company, the 2nd Cybersecurity Company and the Training and Innovation Section.

[219] *Report Difesa*, "Difesa: la Joint Stars 25 si terrà in Sardegna nel mese di aprile, sotto la guida del Comando Operativo di Vertice Interforze. Schierati numerosi assetti delle Forze Armate, Corpi Armati dello Stato e altri Dicasteri e Agenzie", 23 January 2025, accessed: 17.03.2025., https://www.reportdifesa.it/difesa-la-joint-stars-25-si-terra-in-sardegna-nel-mese-di-aprile-sotto-la-guida-del-comando-operativo-di-vertice-interforze-schierati-numerosi-assetti-delle-forze-armate-corpi-armati-dello-stato-e/. accessed: 17.03.2025.

[220] Alessandro Marrone, Ester Sabatino *and* Ottavia Credi, *Italy and Cyber Defence*, Istituto Affari Internazionali (IAI), September 2021, https://www.iai.it/sites/default/files/iai2112_en.pdf, accessed: 17.03.2025.

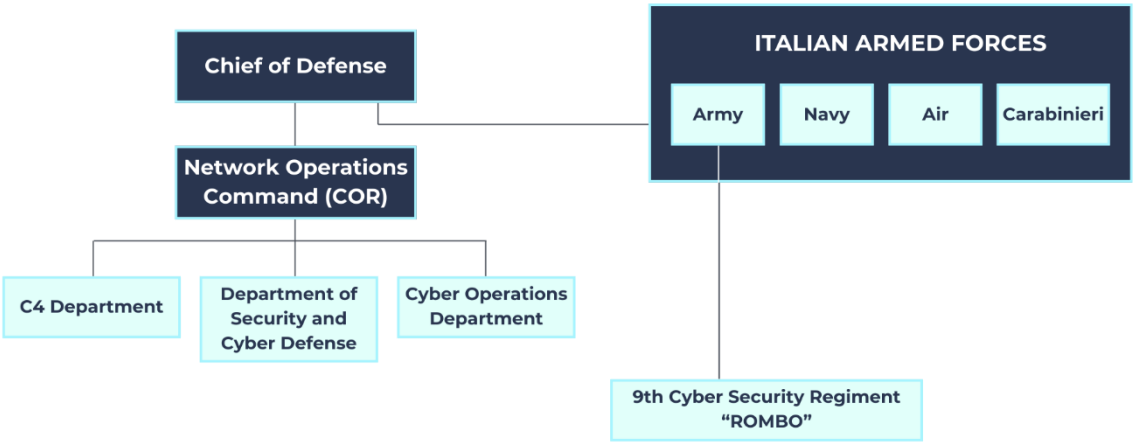


FIGURE 19. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN ITALY.

5.16 Latvia

5.16.1 Overview of the state's cybersecurity situation

Geographical proximity and Riga's alignment with Ukraine have led to an intensification of DDoS attacks on its public and private sectors.[221] Since the Russian military invasion of Ukraine, the number of cyber incidents in Latvia has increased by 40%, while attacks on state institutions and critical infrastructure have quadrupled. In the second quarter of this year, the number of hacking attempts reached its highest level in two years and has increased by 56% since the beginning of the year.[222] Latvia is now second in the EU, after Poland, in terms of the number of cyber attacks. For example, in 2022, 16% of all Russian cyberattacks were directed against Latvia.[223]

On 20th June 2024, the Latvian Parliament adopted the National Cyber Security Act. The document established a new institution, the National Cyber Security Centre, which, from 1st September 2024, acts as a focal point on issues related to this field. In turn, a new National Security Strategy was approved in March 2023, which will be in effect until 2026.[224]

[221] *The Cybersecurity Strategy of Latvia 2023-2026*, pp. 8-10.
[222] *CERT: Latvia sees highest level of cyberattacks in two years*, LSM, 15 October 2024, https://eng.lsm.lv/article/society/crime/15.10.2024-cert-latvia-sees-highest-level-of-cyberattacks-in-two-years.a572581/ accessed: 17.03.2025.
[223] *New law significantly strengthens cybersecurity in Latvia*, Latvijas Republikas Saeima, 20 June 2024, https://www.saeima.lv/en/news/saeima-news/33693-new-law-significantly-strengthens-cybersecurity-in-latvia accessed: 17.03.2025.
[224] *Cybersecurity*, Ministry of Defence Republic of Latvia, 2024, https://www.mod.gov.lv/en/cybersecurity accessed: 17.03.2025.

5.16.2 History and evolution of cyber units

There is no separate Cyber Force/Cyber Command within the Latvian National Armed Forces (lt. Nacionālie bruņotie spēki - NAF). However, there is a NAF National Guard Cyber Defence Unit (CDU), which was established in 2013 with the aim of involving information technology specialists in the National Guard and supporting the armed forces. Initially, three professional soldiers were active in the unit, while the rest of the staff consisted of volunteers from the cyber field. In early 2015, the unit reached initial operational capability and reached full operational capability three years later. In 2020, a selection system was developed to ensure an efficient and tailored recruitment of new personnel. The unit takes part in periodic exercises, including Locked Shields and, in 2024, the Latvian team achieved the highest score.[225]

In 2014, the Military Computer Emergency Readiness Team (Mil-CERT) was created and became operational in 2018.[226] Six years later, the commander of the Latvian Armed Forces issued an order to create a new battalion-level structure for the CDU, which will be integrated with electromagnetic warfare capabilities.[227]

5.16.3 Current structure and resources

Mil-CERT operates under the operational supervision of the State Secretary of the Ministry of Defence and works closely with the Latvian CERT, the institution responsible for preventing and responding to cybersecurity incidents. It also provides consultations for personnel responsible for cybersecurity in the defence sector, as well as cooperation with Latvian institutions and other foreign partners in the field of cybersecurity.[228]

The main task of the CDU is to provide support to the National Armed Forces in times of peace, crisis and war in terms of IT security incident prevention and cybersecurity expertise, as well as regularly testing the IT systems of Latvia's critical infrastructure. In addition, the CDU may be asked to support CERT.LV and Mil-CERT. This shows strong CIMIC, which strengthens the overall cyber resilience and level of cybersecurity in Latvia. In addition, the country participates in NATO's VCISC mechanism and the PESCO Cyber Rapid Response Team project. The CDU's main focus is on defensive cyber operations and providing support to NAF, CERT.LV and Mil-CERT.

The unit provides IT monitoring to the structures of the Ministry of Defence and its subordinate institutions, including the National Armed Forces. The National Guard Cyber Defence Unit is part of the Latvian National Guard and comprises several hundred specialists, although the exact number remains classified for security reasons. Nevertheless, the commander's statements indicate that interest in joining the Latvian Cyber Force is growing.[229] For the period 2023-2026 (and beyond), the Latvian Ministry of Defence

[225] A. Asere, *National Guard Cyber Defense Unit - the best of the best*, Labs of Latvia, 18 July 2024, https://labsoflatvia.com/en/news/national-guard-cyber-defense-unit-the-best-of-the-best accessed: 17.03.2025.
[226] *Ministry of Defence launches Military Computer Emergency Readiness Team*, Ministry of Defence Republic of Latvia, 28 November 2018, https://www.mod.gov.lv/en/news/ministry-defence-launches-military-computer-emergency-readiness-team accessed: 17.03.2025.
[227] *Initiatives to improve Cyber Defence capabilities - development of NATO cyber forces - Latvia*
[228] Ibid.
[229] A. Asere, *National Guard Cyber Defense Unit - the best of the best*, Labs of Latvia, 18 July 2024, https://labsoflatvia.com/en/news/national-guard-cyber-defense-unit-the-best-of-the-best accessed: 17.03.2025.

has allocated more than 20.5 million € to strengthen cybersecurity management.[230] The Latvian unit was established in 2013, and in February 2024, an order to create a new battalion-level structure for the CDU was issued, which will be integrated with electromagnetic warfare capabilities.

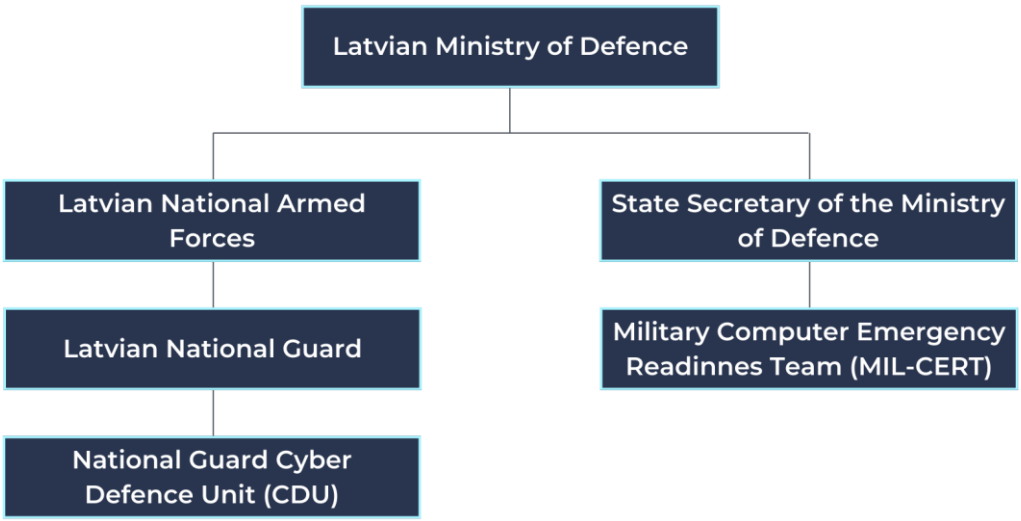


FIGURE 20. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN LATVIA.

5.17 Lithuania

5.17.1 Overview of the state's cybersecurity situation

Lithuania remains a target of Kremlin-linked groups. On the one hand, in 2023 National Cyber Security Centre (NCSC) recorded 2,378 cybersecurity incidents, a 30% decrease from 2022. Concurrently, the number of attacks classified as being 'more dangerous' increased (by 12%).[231] The most damaging cyber attacks in the country stemmed from DDoS, ransomware or social engineering-based intrusions.

Lithuania is strengthening cooperation with Indo-Pacific countries in the cyber field, notably Japan, Australia, South Korea, Singapore, and Taiwan, *inter alia*. Along with other allies, Lithuania has also joined the IT Coalition within the Ukrainian Defence Contact Group (Ramstein format). Vilnius also continues to strengthen the cyber sector by providing training to the general public, private companies and organisations.

5.17.2 History and evolution of cyber units

In 2023, the Lithuanian Ministry of National Defence decided to establish a new unit of the Lithuanian Armed Forces, the Cyber Defence Command (CDC) (lit. Kibernetinės gynybos valdyba - CDC). The

[230] *The Cybersecurity Strategy of Latvia 2023-2026*, p. 31.
[231] *Overview of the cybersecurity status in Lithuania: key information 2023*, Ministry of National Defence: Republic of Lithuania, 2023, pp. 6-10.

project was approved by the State Defence Council in early 2024 and has since been submitted to the government for review. It envisages the addition of the CDC to the current structure of the Lithuanian Armed Forces, while the first step is to restructure the Information Technology Service at the Ministry of National Defence. The structure of the CDC will include the Main Command, the Grand Hetman Kristupas Radvil Perkūnas Battalion.[232]

Prior to the decision to establish a separate Cyber Command, cyber responsibilities in Lithuania were divided between several entities:

- Information Technology Service at the MoD.
- NCSC (lit. Nacionalinis kibernetinio saugumo centras - NCSC).
- Cybersecurity Policy and Information Technology Group.
- Core Centre of State Telecommunications (lit. Kertinis valstybės telekomunikacijų centras - KVTC).[233]

In 2024, the Seimas of Lithuania allocated over €2 billion to the Ministry of Defence, part of which is allocated for cybersecurity. In addition, an additional 58 million € was provided to the Ministry, of which 7.9 million € was earmarked for the implementation of the National Cybersecurity Development Programme.[234]

5.17.3 Current structure and resources

The Lithuanian Cyber Command (LTCYBERCOM) was officially established on 1st of January 2025, as a new column within the Lithuanian Armed Forces. This initiative aims to consolidate the country's cyber defence assets under a single umbrella, allowing for more effective responses to emerging cyber threats and protecting critical national infrastructure. It currently has initial operational capability.[235]

Meanwhile, the NCSC will continue to serve as the National Cyber Agency, providing cyber incident response to and resilience within government institutions and key sectors. Its activities will complement the efforts of LTCYBERCOM in building a comprehensive Cyber Defence Strategy across the country.

[232] *The Ministry of National Defence is establishing Lithuanian Armed Forces Cyber Defence Command*, Ministry of National Defence: Republic of Lithuania, 9 April 2024, https://kam.lt/en/the-ministry-of-national-defence-is-establishing-lithuanian-armed-forces-cyber-defence-command/ accessed: 17.03.2025.
[233] Ibid.
[234] *Budget Statement*, Ministry of National Defence: Republic of Lithuania, 5 July 2024, https://kam.lt/en/facts-and-trends/budget-statement/ accessed: 17.03.2025.
[235] *Lithuanian Cyber Defence Command opened*, Ministry of National Defence Republic of Lithuania, 3 January 2025, https://kam.lt/en/lithuanian-cyber-defence-command-opened/ accessed: 17.03.2025.

FIGURE 21. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN LITHUANIA.

5.18 Luxembourg

5.18.1 Overview of the state's cybersecurity situation

The global increase in cyber threats worldwide has not spared Luxembourg. Organisations operating in the country recorded an average of 1,446 cyberattacks per week in Q3 2024, equivalent to an 82% quarter-over-quarter increase. The financial and banking sectors were the most vulnerable, with an average of 723 attacks per week per organisation.[236]

In 2021, Luxembourg adopted a formal Cyber Defence Strategy for 2021-2031, which was prepared in collaboration between the Directorate of Defence and the Luxembourg Armed Forces. In April 2022, the Directorate of Defence and the University of Luxembourg (UL) signed a partnership agreement, which established a Cybersecurity Policy Chair at the university for five years, starting in September 2022. In turn, in November 2023, the Directorate of Defence of Luxembourg, in cooperation with UL, launched the Cybersecurity and Cyber Defence Research Competence Centre (CyberHub).[237]

5.18.2 History and evolution of cyber units

Luxembourg's military cyber structures originated in 2011, when the Council of Government approved the creation of two new entities: the Luxembourg Cybersecurity Council and the Government Computer

[236] A. Stevensson, *Luxembourg businesses facing ever more cyberattacks*, Luxembourg Times, 21 October 2024, https://www.luxtimes.lu/businessandfinance/luxembourg-businesses-facing-ever-more-cyberattacks/23606264.html accessed: 17.03.2025.

[237] *Cyber Defence*, The Luxembourg Government, https://defense.gouvernement.lu/en/la-defense/cyber.html accessed: 17.03.2025.

Emergency Response Team (GOVCERT.LU).[238] The Cyber/SecuSIC Office (fr. Le bureau Cyber/SecuSIC) was developed within the Department of Information Systems and Communication (fr. Département Systèmes Information et Communication; DSIC). Since 2021, this bureau has participated in the international NATO's Locked Shields exercises. In the edition organised in 2023, Luxembourg partnered with Latvia as part of the exercise and was ranked fourth.[239]

5.18.3 Current structure and resources

The role of military CERT has been assigned to GovCERT. The Chief of Defence (fr. Chef d'État-Major) is part of the Crisis Management Team within the Cyberattack Response Plan (PIU Cyber). In turn, there is a Luxembourg House of Cybersecurity (LHC) within the Department of CIS of the Armed Forces.[240]

In order to implement the Cyber Defence Strategy, the Luxembourg Cyber Defence Cloud (LCDC) and the Luxembourg Cyber Range projects have been initiated, under the auspices of the Cyber Management Team of the Directorate of Defence. The LCDC is a private cloud based on secure data centres in Luxembourg which provides storage and processing space for unclassified and classified information requiring heightened security standards. The Cyber Range, on the other hand, which was officially launched in October 2021, is used for exercises, training and security testing; it also supports skill development of cybersecurity.[241]

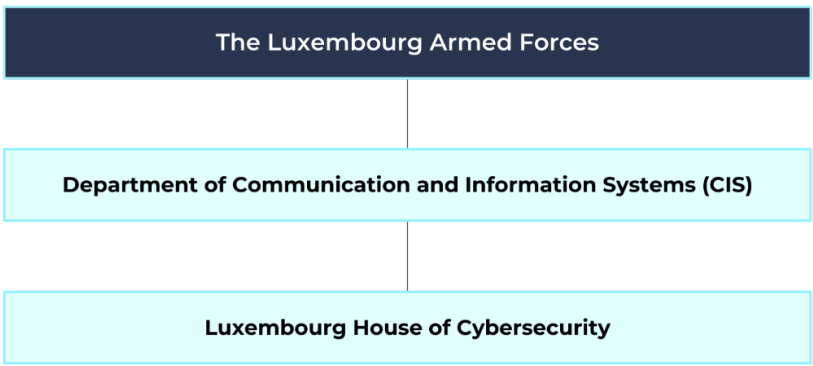


FIGURE 22. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN LUXEMBOURG.

[238] P. M. Zotz, National Cybersecurity Organisation: Luxembourg, NATO CCDCOE, Tallinn 2021, https://ccdcoe.org/uploads/2021/05/NCS_organisation_LUX-2021-FINAL.pdf accessed: 17.03.2025.
[239] *Service de cyberdéfense*, L'Armée luxembourgeoise, 21 February 2024, https://armee.public.lu/fr/missions/service-cyberdefense.html accessed: 17.03.2025.
[240] P. M. Zotz, ibid. p. 19.
[241] *Cyber Defence*, The Luxembourg Government, https://defense.gouvernement.lu/en/la-defense/cyber.html accessed: 17.03.2025.

5.19 Montenegro

5.19.1 Overview of the state's cybersecurity situation

In August 2022, Montenegro became the target of a major cyber attack that caused a widespread failure of the digital infrastructure of a large part of the country's public administration. The attack has since been attributed to the Russian Federation.[242] It also led to an increased debate on the amendment of cyber solutions, the creation of a new Cybersecurity Agency, as well as mobilisation on issues of compliance with the EU's 2023-2024 declarations and restrictive measures.[243]

5.19.2 History and evolution of cyber units

Montenegro has been developing its cybersecurity capabilities since the adoption of the first Information Security Act in 2010. Another crucial document in this regard is the National Cybersecurity Strategy for 2022-2026.[244] Despite limited resources in terms of military and state structures in this field, Montenegro is actively engaged in international initiatives to strengthen its cybersecurity capacities. One key project is the cooperation with France and Slovenia, which has led to the establishment of the Western Balkans Cyber Capacity Centre (WB3C), based in Podgorica. This centre focuses on training specialists in the areas of cybercrime, cybersecurity and cyber diplomacy, contributing to the development of defence and strategic capabilities in the Western Balkans region.[245]

In addition, as part of its strategic partnership with the United Nations Office on Drugs and Crime (UNODC) for 2024-2029, Montenegro has committed to strengthening capacities of law enforcement and the judiciary to counter cybercrime. This included cooperation with regional and international actors, as well as a partnership with the newly established Cybersecurity Capacity-Building Centre in Podgorica.[246]

Another key initiative is the Computer Incident Response Team (CIRT) founded in 2012 as a joint project between the Government of Montenegro and the International Telecommunications Union (ITU). *Nota bene*, it is not a strictly a military structure, as Montenegro has not yet developed such capabilities. On the other hand, the Montenegrin Armed Forces have actively participated in NATO exercises such as Cyber Coalition 2023 and Steadfast Defender 24,[247] and joining NATO in 2017 was a significant milestone for the country's cyber capabilities.

Although the Montenegrin government does not currently plan to create a military structure concerning the cyber sphere, the creation of a Cybersecurity Agency was proposed in October 2024. This Agency would focus on protecting IT systems outside the state administration, while CIRT would remain responsible for government infrastructure. However, no further steps were taken, due to experts' warnings

[242] P. Król, *Czarnogóra oskarża Rosję o cyberatak*, Kresy.pl, 4 September 2022, https://kresy.pl/wydarzenia/czarnogora-oskarza-rosje-o-cyberatak, accessed: 17.03.2025.
[243] *Montenegro Report 2024*, European External Action Service (EEAS), 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/Montenegro%20Report%202024.pdf, accessed: 17.03.2025.
[244] B. Dzakula, A. Mihailovic, N. Zaric, Current Cybersecurity Capacities and Digital Rights in Montenegro, 2021, p. 25.
[245] "CyberCenter", *French Embassy in Montenegro*, https://me.ambafrance.org/-CyberCenter. accessed: 17.03.2025.
[246] United Nations Office on Drugs and Crime, 'Report on South Eastern Europe: Regional Assessment of the Impact of Cybercrime on Crime Prevention and Criminal Justice Systems', https://www.unodc.org/documents/southeasterneurope//202404_UNODC_Report_SPF_ENG_FINAL.pdf. accessed: 17.03.2025.
[247] *Montenegro*, NCSI, 2024, https://ncsi.ega.ee/country/me/ accessed: 17.03.2025.

of overlaps between the two institutions and the risk of politicisation of the Agency, whose leadership was to be appointed by governmental bodies.[248]

5.19.3 Current structure and resources

Montenegro currently lacks military cyber resources as well as a military cyber doctrine. However, the 2022-2026 strategy outlines the development of cyber capabilities within the Ministry of Defence (MoD). The report shows that the current structure of the Ministry separates the Head of the Cybersecurity Office, eight independent advisers, the Head of the Cyber Operations Office, five cyber analysts and the Montenegrin defence adviser to NATO CCDCOE.

This brings the total number of cybersecurity personnel to 17, indicating a significant commitment to cybersecurity, especially in the context of defence and international cooperation. By 2026, the number of staff is expected to increase to 20. In addition, the national CIRT, under the MoD, has 16 officers, with a plan to increase this number to 24 by 2026.[249]

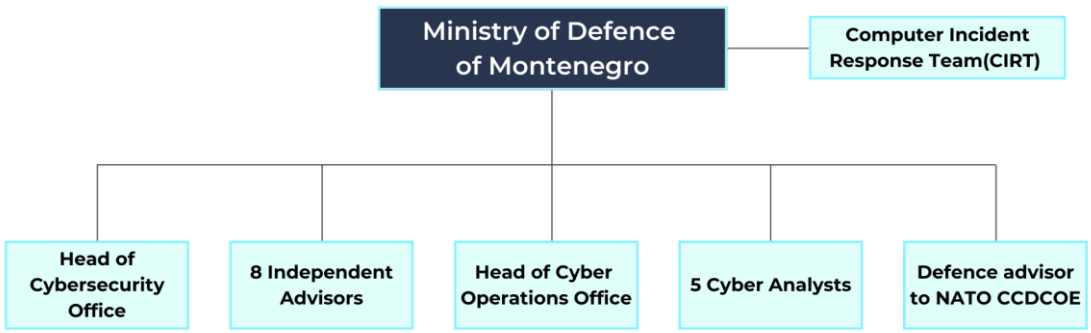


FIGURE 23. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN MONTENEGRO.

5.20 Netherlands

5.20.1 Overview of the state's cybersecurity situation

In 2021, a total of 6,300 ransomware attacks targeting companies were reported. In a survey conducted a year later, 15% of the Dutch population (*circa* 2.2 million people) indicated that they had been victims of at least one form of online crime. Ransomware attacks primarily affected enterprises rather than small

[248] I. Ivanovic, 'Montenegro's Proposed New Cybersecurity Structure Raises Concerns', *Balkan Insight*, 2 October 2024, https://balkaninsight.com/2024/10/02/montenegros-proposed-new-cybersecurity-structure-raises-concerns/. accessed: 17.03.2025.
[249] B. Dzakula, A. Mihailovic, N. Zaric, *Current Cybersecurity Capacities and Digital Rights in Montenegro*, 2021, pp. 7-8.

businesses (4% compared to 0.3%). There was also an increase in the number of attacks on the financial sector, with 3.4% of companies affected in 2024, compared to 2.2% in 2023.[250]

The Netherlands has a well-developed cyber ecosystem at both civilian and military levels. Key institutions include the Dutch Research Council's Cybersecurity Programme, the NCSC (nl. Nationaal Cyber Security Centrum – NCSC), which holds a central national role, and the Cybersecurity Council (nl. Cybersecurity Raad – CSR), an advisory body comprising representatives drawn from both public and private sectors. On the military side, the Defence Cyber Command (nl. Defensie Cyber Commando – DCC) acts as the coordinating authority for cyber operations and capabilities within the Ministry of Defence (MoD).

While DCC is an important institution, it is part of a much broader cyber architecture, which includes other cyber units across the armed forces (the army, navy, air force, and military police), and strategic-level intelligence responsibilities under the Military Intelligence and Security Service (nl. Militaire Inlichtingen- en Veiligheidsdienst – MIVD). Cyber governance in the Netherlands also involves several coordination platforms, such as the Cyber Governance Board (with high-level representatives from various ministries), a director-level cyber governance forum, and a working-level cyber coordination board. These efforts are guided by the Netherlands Cybersecurity Strategy 2022–2028, which frames the country's approach to cybersecurity in a comprehensive and integrated manner.[251]

5.20.2 History and evolution of cyber units

In order to strengthen the digital capabilities of the MoD, the 'Taskforce Cyber' was established in 2012. The result of this decision was the establishment in June 2015 of Defence Cyber Command (DCC), which was placed under the direct authority of the Chief of Defence of the Armed Forces three years later. Initially part of the Royal Netherlands Army (which is responsible for land operations), the DCC was moved in 2018 to operate directly under the Chief of Defence (CHOD). This structural elevation brought the DCC to a status not dissimilar to the Special Operations Command (SOCOM) and the Directorate of Operations (DOPS). The change reflects the growing strategic importance of cyber operations across all military domains. The DCC is responsible for conducting military cyber operations and acts as the coordinating authority for cyber activities across the entire MoD.

In 2013, the participation of teams from the Netherlands in the NATO CCDCOE cyber exercise was initiated. In 2016, on the other hand, the DCC introduced the conscription of reservists for service in the DCC in case of heightened cyber threats, operational demand, or national emergencies involving cyber incidents. The original conscription target was 150, but as of 2018, there were only 30 recruits.[252]

In 2014, as part of a cooperative initiative known as 'Project Symbolon', the Military Intelligence and Security Service (nl. Militaire Inlichtingen- en Veiligheidsdienst - MIVD), together with the General Intelligence and Security Service (nl. Algemene Inlichtingen- en Veiligheidsdienst - AIVD), established the Joint SIGINT Cyber Unit (JSCU).[253]

---

[250] *Statistics Netherlands releases Cyber Security Monitor 2022*, Hadrian, 2023, https://hadrian.io/blog/statistics-netherlands-releases-cyber-security-monitor-2022, accessed: 17.03.2025.
[251] *Netherlands*, NCSI, 30 April 2024, https://ncsi.ega.ee/country/nl/ accessed: 17.03.2025.
[252] M. Smeets, *The challenges of military adaptation to the cyberdomain: a case study of the Netherlands*, Small Wars & Insurgencies, 2023, vol. 34, no. 7, 1343-1362, pp. 1345-1351.
[253] Ibid.

5.20.3 Current structure and resources

The DCC, now operating under the CHOD, plays a central role in the Netherlands' military cyber operations. Originally established within the Royal Army, it has since evolved into a joint command, serving all branches of the armed forces and acting as the principal coordinating authority for cyber operations within the MoD. Like other operational commands, the DCC does not hold a standing mandate to conduct Operational Preparation of the Environment (OPE) unless a specific mission is defined and authorised. Activities related to intelligence gathering, including those that may involve aspects resembling OPE, fall under the responsibility of the Military Intelligence and Security Service (nl. Militaire Inlichtingen- en Veiligheidsdienst – MIVD).

The MIVD operates independently from the DCC and has a standing legal mandate to collect intelligence under the Intelligence and Security Services Act (nl. Wet op de inlichtingen- en veiligheidsdiensten – Wiv). It is supervised by the Secretary General of the MoD and performs its tasks within the legal framework defined by this act, focusing on intelligence rather than operational command functions.[254]

The Cyber Capabilities and National Power Report[255] mentions the Netherlands' military cyber capabilities. It lists the following facets:

- The country has military cyber capabilities; however, these are less developed than in countries such as the US, UK or Israel.
- Cyber offensive capabilities are under the control of the MoD. However, it is not known whether they have ever been used operationally.
- The Dutch strategy focuses mainly on cyber defence, international cooperation and the integration of cyber operations with conventional armed forces.
- The Netherlands is actively cooperating with NATO on cybersecurity, while adapting its military to new threats in the digital domain.

[254] Ibid.
[255] *Cyber Capabilities and National Power: Volume 2 - The Netherlands*. International Institute for Strategic Studies (IISS), 2023, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_07-the-netherlands.pdf accessed: 17.03.2025.

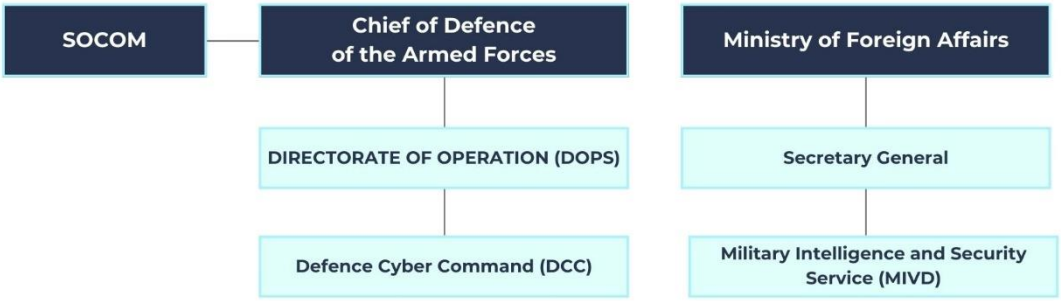


FIGURE 24. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN THE NETHERLANDS.

5.21 North Macedonia

5.21.1 Overview of the state's cybersecurity situation

The North Macedonian authorities did not publish a revised version of the National Cybersecurity Strategy, continuing to rely on the draft envisaged for 2018-2022. At the time, the authors highlighted that the digitalisation of businesses and e-services was progressing while noting the extant threat from cyber criminals and the low cybersecurity standards of small and medium-sized enterprises (SMEs). The need to implement cyber solutions in internal forces and the armed forces was noted, given that this was a precondition for NATO and EU membership.

In 2019, the Minister of Information Society and Administration of North Macedonia stated that the country, standing on the threshold of EU membership (not yet a member of NATO), is becoming an increasingly attractive target for cyber criminals.[256] Consequently, strengthening national cybersecurity capabilities was a core objective of the strategy, a policy which sought to reduce the risk of cyberattacks.[257]

The most significant cyberattack against Skopje was a DDoS attack on the day of the parliamentary elections, which took place in July 2020. According to available data from 2021, a total of 122 public websites were hacked. On 21st February 2023, there was a wave of false bomb alarms and cyber attacks. It resulted in the evacuation of more than 30 locations in Skopje and Prilep, including schools, offices, TV

[256] D. Mazepa, Narodowa Strategia Bezpieczeństwa Cybernetycznego Republiki Macedonii Północnej i Plan Działania 2018-2022, Wschodnioznawstwo 13 (2019): 77-90, https://ejournals.eu/czasopismo/wschodnioznawstwo/artykul/narodowa-strategia-bezpieczenstwa-cybernetycznego-republiki-macedonii-polnocnej-i-plan-dzialania-2018-2022, accessed: 17.03.2025.
[257] *Republic of Macedonia National Cyber Strategy 2018-2022*, Republic of Macedonia, July 2018, https://eucyberdirect.eu/atlas/sources/republic-of-macedonia-national-cyber-strategy-2018-2022 accessed: 17.03.2025.

stations, courts, shopping centres, hotels and residential buildings, as well as the presidential palace, for the first time in history. The perpetrators managed to seriously disrupt the functioning of the state.

As a result of this incident, the government of North Macedonia pledged to strengthen cybersecurity.[258] NATO also reacted in March 2024, sending a high-level delegation led by James Appathurai, Deputy Assistant Secretary General for Security Challenges. The delegation worked with the authorities in assessing the situation and discussing further support. Following the visit, Appathurai stressed that the country was grappling with a "deliberate, sustained and cynical hybrid attack".[259]

5.21.2 History and evolution of cyber units

In 2017, the communication and cyber defence team was established. The Army of the Republic of North Macedonia participated in the exercise "Cyber Coalition 22".[260] National cyber capabilities were developed, even before its accession to NATO, but they were limited to taking part in exercises with the US side and the organisation itself. In 2021, North Macedonia signed an MoU with NATO regarding future cooperation in cyber defence.[261]

The military branch of cyber capabilities is currently being developed within the Military CSIRT, a division of the MoD and the Armed Forces.[262] It is also worth noting that, despite active cooperation with NATO in the field of cyber defence, North Macedonia remains the only non-member country of the NATO CCDCOE.

5.21.3 Current structure and resources

The North Macedonian Armed Forces have not designated a specific unit responsible for the cybersecurity of military operations and cyber operations. However, key elements of the National Cybersecurity Strategy 2018-2022 remain unfulfilled – cyber troops have not been established, and the military tasks in this area are partly carried out by the Military Computer Security Incident Response Team (MIL-CERT), and the Armed Forces of North Macedonia.

[258] "North Macedonia Steps Up Security After Cyberattacks and Bomb Hoaxes Linked to Ukraine War", *IntelliNews*, 22 February 2023, https://www.intellinews.com/north-macedonia-steps-up-security-after-cyber-attacks-and-bomb-hoaxes-linked-to-ukraine-war-270736/. accessed: 17.03.2025.
[259] "NATO and EU Meet to Enhance Cooperation on Cyber Defence", *NATO*, 8 March 2023, https://www.nato.int/cps/en/natohq/news_212621.htm. accessed: 17.03.2025.
[260] *History of the Army*, Army of the Republic of North Macedonia, https://mil.mk/history/?lang=en#1495112660340-dd2e5790-d213 accessed: 17.03.2025.
[261] *NATO and North Macedonia strengthen responses to cyber threats*, NATO, 19 February 2021, https://www.nato.int/cps/en/natohq/news_181656.htm accessed: 17.03.2025.
[262] *Participation of Army members in the exercise "Cyber Unity 2023"*, Army of the Republic of North Macedonia, 20 September 2023, https://mil.mk/general-staff-activities/uchestvo-na-pripadnici-na-armijata-na-vezhbata-cyber-unity-2023/?lang=en accessed: 17.03.2025.

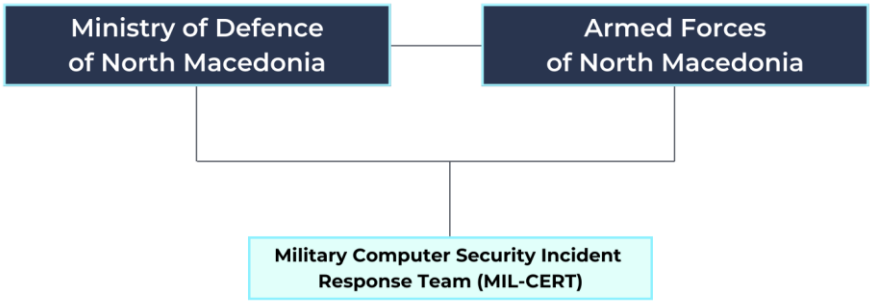


FIGURE 25. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN NORTH MACEDONIA.

5.22 Norway

5.22.1 Overview of the state's cybersecurity situation

Norway is experiencing targeted attacks on critical infrastructure, and cyber attacks are one of the most serious threats to the country's security. They are mostly invisible and difficult to detect, aiming to take control of systems. Government institutions and NATO infrastructure in the country are also targets of these attacks. On 12th of July 2023, it was revealed that hackers, exploiting software vulnerabilities, breached the computer system used by 12 Norwegian ministries and had access to it for at least two and a half months.

In addition to the activities undertaken within NATO and the EU, Norway, together with the Nordic countries, collaborates within the cyber field through the Nordic Defence Cooperation (NORDEFCO).[263] Notably, the largest and most consequential attacks were carried out by hackers and entities of hostile states, even before the full-scale invasion of Ukraine in February 2022.[264] According to Norway's Cybersecurity Agency, the number of cyber attacks tripled between 2019 and 2021.[265]

[263] K. Kaczmarek, *Nordic Countries in the Face of Digital Threats*, Cybersecurity and Law, 2024, pp. 151-161.

[264] *Top 10 Cybersecurity Breaches in Norway*, Cyberlands.IO, https://www.cyberlands.io/topsecuritybreachesnorway accessed: 17.03.2025.

[265] *Norway government ministries hit by cyberattack*, Reuters, 24 July 2023, https://www.reuters.com/technology/norway-government-ministries-hit-by-cyber-attack-2023-07-24/ accessed: 17.03.2025.

5.22.2 History and evolution of cyber units

In September 2012, the Norwegian Defence Information Infrastructure was renamed the Cyber Defence Force (nor. Cyberforsvaret). The remit of Norway's extant cyber forces was to support the Norwegian Armed Forces in establishing, operating, developing and protecting their communications. In 2017, it was estimated that Cyberforsvaret's headcount was approximately 1,200 civilian and military personnel.[266]

5.22.3 Current structure and resources

Cyberforsvaret is currently located at Camp Jørstadmoen in Lillehammer. It is responsible for establishing and maintaining the Armed Forces' freedom of action within the digital domain. It also protects the Armed Forces' ICT systems against all digital threats posed by military and civilian actors. The Department also operates and maintains the Armed Forces' jointly integrated management system (FIF).

Cyberforsvaret consists of conscripts, trainees, military and civilian cyber engineers, as well as liaison personnel and operational military staff. The cyber unit is composed of several departments, including the Cyber Defence CIS Regiment, Cybersecurity Centre, Cyber Defence Weapons School, Cyber Defence ICT Services, Cyber Defence Base and Alarm Services. Since 2022, the Commander of the Norwegian Cyber Force has been General Halvor Johansen. It is estimated that Cyberforsvaret currently has around 1,500 military and civilian members.[267]

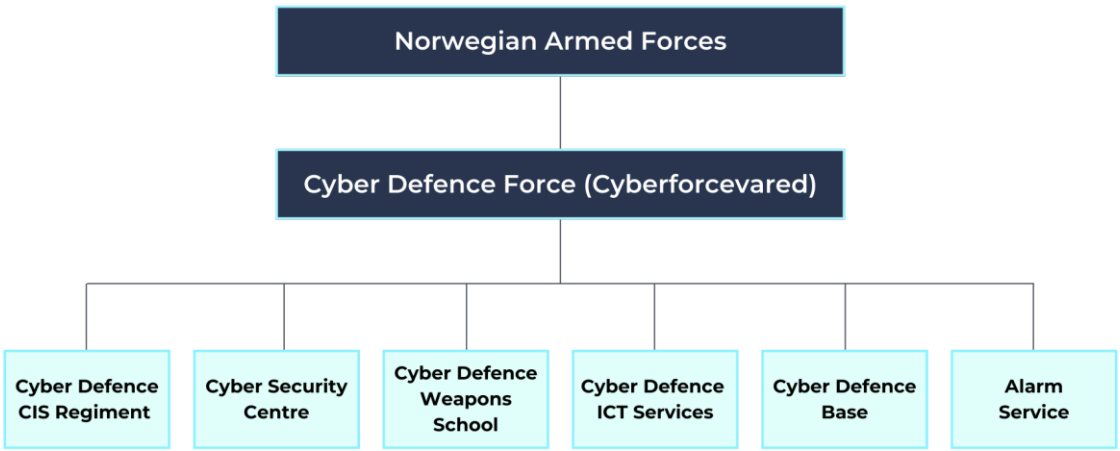


FIGURE 26. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN NORWAY.

[266] *Norwegian Defence 2013: Facts and Figures*, Norwegian Ministry of Defence, 2013, p. 13.
[267] *The Norwegian Cyber Defence*, Norwegian Armed Forces, https://www.forsvaret.no/en/organisation/norwegian-cyber-defence accessed: 17.03.2025.

5.23 Poland

5.23.1 Overview of the state's cybersecurity situation

The number of cyberattacks in Poland has increased from 50 incidents in 1996 to more than 80,200 in 2023. Since 2011, the number of cybersecurity incidents has been steadily rising, and a milestone was reached in 2021 when Russia and Belarus launched hybrid operations against Poland and NATO to destabilise the situation before a full-scale Russian invasion of Ukraine.[268] Poland was ranked 6th on the Cyber Defence Index 2022/23 published by the "MIT Technology Review".[269] In February 2024, Poland became the most frequently targeted country globally in terms of cyberattacks, according to the Cyber Defence Forces, with more than 1,000 attacks recorded each week. Most Polish companies are considered inadequately prepared to defend against such digital threats.

According to an AON study, fewer than 43% of enterprises in Poland have implemented a post-incident plan or a formal review of the risks related to cyberattacks.[270] Polish Deputy Prime Minister and Minister of Digitalisation Krzysztof Gawkowski stated that Poland is Russia's most frequent target within EU cyberspace.

Between 1st January and July 11th 2024, 368,078 cybersecurity incidents were reported to the CERT NASK team, with 62,014 labelled as 'new incidents'.[271] In June 2024, Poland announced that it is increasing its spending on cybersecurity to almost 760 million USD to improve digital security.[272]

5.23.2 History and evolution of cyber units

The first concept for a Polish 'cyber army' was conceived in 2018, when the then Minister of Defence announced a plan to create a unit of 1,000 soldiers. The idea was not finalised, but the process of creating a cyber unit resumed. On May 2nd of May 2019, Minister of Defence, Mariusz Blaszczak, appointed General Karol Molenda as the plenipotentiary for the establishment of cyber defence troops. His first step was consolidating the various military entities responsible for cybersecurity. As a result, the National Cryptology Centre and the IT Inspectorate were merged into the NCSC.

In September 2019, the Minister of Defence signed the concept for the organisation and functioning of the Cyber Defence Forces. Two months later, the decision of the Minister of Defence on the organisation and functioning of the Cyber Defence System in the Ministry of National Defence came into force. In February 2020, a group for the formation of the Cyber Defence Forces command was established, while in March, a transitional implementation team for the creation of the Cyber Defence Forces was

[268] A. Sas, *Number of cyber security incidents handled by CERT in Poland from 1996 to 2023*, Statista, 22 May 2024, https://www.statista.com/statistics/1028557/poland-cybersecurity-incidents/ accessed: 17.03.2025.
[269] *Poland ranks 6th in the global cybersecurity ranking*, Instytut Kościuszko, 2 February 2024, https://ik.org.pl/en/2024/02/02/cyber-coalition-key-role-of-poland-in-nato-cyber-warfare-exercises/ accessed: 17.03.2025.
[270] *Poland ICT the most cyberattacked country in the world*, International Trade Administration U.S, 28 February 2024, https://www.trade.gov/market-intelligence/poland-ict-most-cyber-attacked-country-world accessed: 17.03.2025.
[271] P. Makowiec, *Tysiące zagrożeń, gigantyczne wzrosty? Tezy kontra statystyki CERT Polska*, Cyberdefence24, https://cyberdefence24.pl/cyberbezpieczenstwo/tysiace-zagrozen-gigantyczne-wzrosty-tezy-kontra-statystyki-cert-polska, accessed: 17.03.2025.
[272] J. Gregory, *Poland spending $760 million on cybersecurity after attack*, Security Intelligence, https://www.ibm.com/think/news/poland-cybersecurity-spending-increases, accessed: 17.03.2025.

established, and the implementation of cyberspace as a domain of operational activities in the Polish Armed Forces was created. The project to establish a cyber army gained further support in April 2020, with the appointment of the Plenipotentiary of the Minister of National Defence for Cybersecurity.[273]

On 8th of February 2022, another milestone in the development of the cyber forces of the Polish Armed Forces was achieved with the official establishment of the Cyber Forces Command (pl. Dowództwo Wojsk Cyberobrony) and the Polish Cyber Defence Forces (pl. Wojska Obrony Cyberprzestrzeni). In 2023, approximately 5,000 people (military and civilian; although the precise number of 'cyber soldiers' is not disclosed) were engaged by the Cyber Defence Forces.[274]

5.23.3 Current structure and resources

The Cyber Defence Forces are a specialised component of the Armed Forces. They are responsible, within the Ministry of National Defence, for areas related to cryptology, cybersecurity, and the construction and operation of teleinformatics systems. The Cyber Defence Forces have 12 subordinate military units in their structure, including two units specialised for operations in cyberspace: "A" in Białobrzegi and "B" in Gdynia. Their main objective is to conduct operations in cyberspace across three dimensions: defensive, reconnaissance and offensive. In 2024, the formation of a third cyber operations unit, Unit 'C' in Wrocław, commenced.

Also, an Operations Support Unit in Legionowo is in the process of being formed. The Cyber Defence Forces structure also includes the Military Frequency Management Office (pl. Wojskowe Biuro Zarządzania Częstotliwościami - WBZC), the Command Systems Support Centre (pl. Centrum Wsparcia Systemów Dowodzenia Sił Zbrojnych - CWSD), the Cyber Resource Centre (pl. Centrum Zasobów Cyberprzestrzeni Sił Zbrojnych – CZC) and six Regional IT Centres (pl. Regionalne Centrum Informatyki - RCI). The commander of the Cyberspace Defence Forces Component is Major General Karol Molenda.[275] In the 2024 budget, 1,806,684 thousand PLN was allocated for cybersecurity and cryptologic support.[276]

[273] *Cyber Defence Forces*, Cyber.Mil.PL, https://www.cyber.mil.pl/wojska-obrony-cyberprzestrzeni/ accessed: 17.03.2025.
[274] A. Kozłowski, *Polish 'cyberclaws'. Building of the cyberarmy of the rising military power in Europe*, Casimir Pulaski Foundation, 26 June 2023, https://pulaski.pl/en/polish-cyberclaws-building-of-the-cyberarmy-of-the-rising-military-power-in-europe/ accessed: 17.03.2025.
[275] *Wojska Obrony Cyberprzestrzeni*, Ministry of Defence, https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni, accessed: 17.03.2025.
[276] *Podstawowe informacje o budżecie resortu obrony narodowej na 2024 r*, Ministry of Defence, March 2024, p.8.

FIGURE 27. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN POLAND.

5.24 Portugal

5.24.1 Overview of the state's cybersecurity situation

In 2022, Portugal was the target of 9% of cyber attacks targeting EU. According to Portuguese data protection Authority (por. Comissão Nacional de Proteção de Dados - CNPD), the main vectors of attacks were vulnerabilities in infrastructure security, lack of training in identifying phishing campaigns, and malware distribution, with a particular focus on ransomware. A lack of awareness among decision-makers regarding the risks associated with insufficient investment in security mechanisms was noted.[277]

The number of incidents, as registered by CERT.PT, increased by 14%, from 1,781 in 2021 to 2,023 in 2022. Among these incidents were those cyber attacks with a significant impact on infrastructure and services in Portugal. Cybersecurity incidents in Portugal in 2022 mostly affected the banking (phishing attacks targeting customers), education, science, technology, transport and health sectors.

Portugal has had a National Cybersecurity Strategy since 2015, although it was updated in 2019. This resulted in the National Cybersecurity Strategy 2019-2023 policy document.[278] It was based on three main strategic objectives, specifically maximising resilience, promoting innovation and ensuring adequate resources.[279] In October 2024, the Portuguese Council of Ministers approved two draft laws on cybersecurity and digital services, aiming to strengthen the national mechanisms for protection against

[277] J. L. Arnaut, J. L Figueiredo, *Data protection and cybersecurity in Portugal: challenges ahead through 2023*, The Legal 500, https://www.inhouselawyer.co.uk/legal-briefing/data-protection-and-cybersecurity-in-portugal-challenges-ahead-through-2023/ accessed: 17.03.2025.
[278] E. Magrani, *Cybersecurity in Portugal: Trends and Compliance*, CCA, 30 October 2023, https://www.cca.law/en/insights-and-media/newsletters/Cybersecurity-in-Portugal-Trends-and-Compliance/9147/ accessed: 17.03.2025.
[279] Centro Nacional de Cibersegurança, "National Strategy for Cyberspace Security 2019-2023", June 2019, https://cncs.gov.pt/docs/portugal-ncss-2019-2023-en-2.pdf. accessed: 17.03.2025.

cyber threats. In addition, a National Coordination Centre (por. Centro Nacional de Cibersegurança - CNCS) was established, which plays a key role in the country and on the European continent.[280]

It is also worth noting that the Portuguese cybersecurity market is growing rapidly. It is forecast to grow at an average annual rate of 7.75% between 2025 and 2029, which is expected to translate into a market value of 239 million USD by 2029. This growth is driven by a growing number of SMEs that are increasingly investing in cloud solutions and cybersecurity.[281]

5.24.2 History and evolution of cyber units

The Cyber Defence Centre, which had been operational since 2014, was replaced by the Joint Cyber Defence Operations Command (por. Comando de Operações de Ciberdefesa - COCiber). This is a result of the enactment of Decree-Law No. 19/2022 of 24th January 2022, which implemented the Organic Law of the General Staff of the Armed Forces. The Command is tasked with planning, directing, coordinating, controlling and executing operations in and through cyberspace in support of military objectives and to ensure the freedom of action of the Armed Forces in this domain.[282]

In line with the implementation plan for the National Cyber Defence Strategy, which forms an integral part of the Portuguese Armed Forces General Staff (por. Estado-Maior-General das Forças Armadas – EMGFA) Strategic Directive 2021-2023, and in response to the strategic objectives set out therein, the training and retention of human resources, doctrinal consolidation and technology, as well as enhanced interoperability, are priorities toward the ultimate goal of strengthening cyber defence response capabilities.[283]

5.24.3 Current structure and resources

COCiber, comprising military personnel drawn from the naval, land and air forces, functions within the structure of the Portuguese Armed Forces and reports to the EMGFA. Its mission is to conduct operations in cyberspace and develop national capabilities for the prevention, monitoring, detection, response, analysis and remediation of cybersecurity incidents and cyber attacks within the theatre of national defence.

COCiber includes the:

- Cyber Defence Operations Force (por. Força de Operações de Ciberdefesa - FOCiber), which performs military cyber operations, manages the National Defence Cyber Incident Response Centre (PRTCERTDEF) and deploys rapid response teams.

[280] Centro Nacional de Cibersegurança, "NCC-PT - Centro Nacional de Coordenação, https://www.cncs.gov.pt/en/ncc-pt-centro-nacional-de-coordenacao/. accessed: 17.03.2025.
[281] Statista, 'Cybersecurity - Portugal', https://www.statista.com/outlook/tmo/cybersecurity/portugal. accessed: 17.03.2025.

[282] Ministry of National Defence of Portugal, 'Estado-Maior-General das Forças Armadas', https://www.defesa.gov.pt/pt/defesa/organizacao/forcasarmadas/emgfa. accessed: 17.03.2025.
[283] *Comando de Operações de Ciberdefesa - COCiber*, Republica Portuguesa Defesa Nacional, 2024, https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro/Paginas/default.aspx accessed: 17.03.2025.

- Department of Cyber Defence Systems (por. Departamento de sistemos de defesa - DSCiber), which develops and maintains the cyber defence infrastructure, conducts vulnerability audits and ensures interoperability with allied countries.[284]

Additionally, COCiber coordinates and shares information with the NCSC, the National CIRC, other international Computer Emergency Response Teams (CERTs), the NATO Cyber Security Centre and cybersecurity stakeholders. This structured and collaborative approach strengthens Portugal's national cyber threat response strategy.[285]

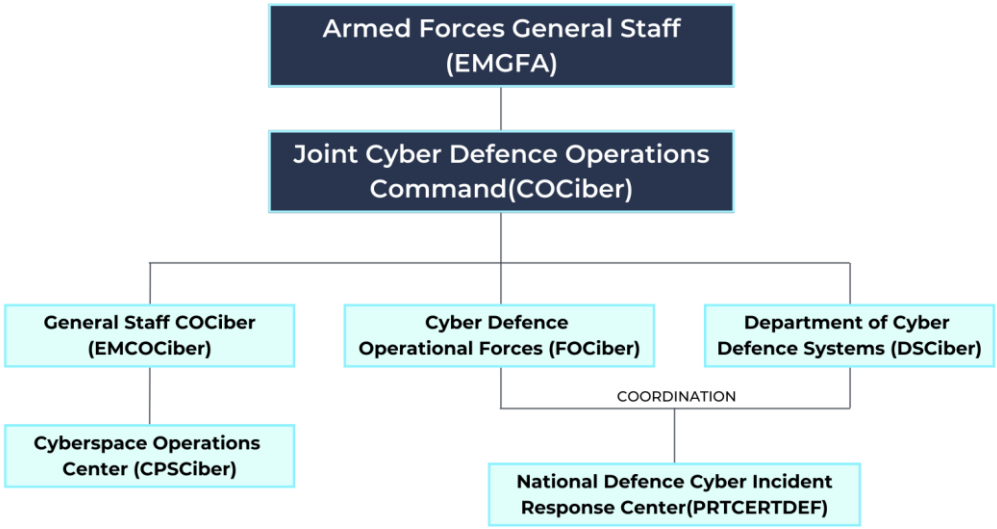


FIGURE 28. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN PORTUGAL.

5.25 Romania

5.25.1 Overview of the state's cybersecurity situation

The rapid digitalisation and technologisation of all aspects of life in Romania have led to cybersecurity becoming a challenge for Bucharest. The year 2021 was marked by hackers' preference for ransomware and infostealer attacks. According to an audit of the Romanian National Cyber Security Directorate (rom. Directoratul Național de Securitate Cibernetică - DNSC), ransomware attacks accounted for 35% of incidents, infostealers were used in 29% of cases, trojans were reported in 20% of incidents, downloaders were responsible for 6% of attacks, the use of backdoors accounted for 4%, exploits—attacks that take advantage of vulnerabilities in software or systems to gain unauthorized access or execute malicious code—accounted for 4%, and worms for less than 1%. In order to distribute these applications, cyber

[284] Diário da República, "Decreto Regulamentar n.º 214/2023", 17 July 2023, https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-regulamentar/2023-214064876 accessed: 17.03.2025.
[285] Ibid.

actors mainly conducted phishing campaigns, sending an average of 3,813 emails of this type in the first half of 2021 alone.

In order to update its security policy, the Romanian government approved the New Cybersecurity Strategy of Romania 2.0 for 2022-2027.[286] Romania also ranked sixth in the infamous "Top Cybercrime Havens" ranking, which examined levels of cybercrime activity in individual countries.[287]

5.25.2 History and evolution of cyber units

The Romanian Ministry of National Defence (rom. Ministerul Apărării Naționale - MApN) has been assigned responsibility for the cyber defence domain. On 1st of December 2018, the CDC (rom. Comandamentul Apărării Cibernetice - CApC) was established. It operates under the command of the Romanian CHOD as a specialised body of the MApN in the field of cybersecurity, cyber defence and IT. The CApC reached initial operational capability in 2021, with full capability achieved in 2024. Since the establishment of the CDC, the unit has provided daily cyber defence operations.

Since June 2019, Romania has been one of the sponsoring countries of the NATO-accredited CCDCOE and, since 2018, MApN has participated in the development of Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity under the EU's Permanent Structured Cooperation Programme (PESCO). Romania sent a technical officer to CCDCOE in 2018 and, as a member state, participated in cyber defence exercises, including Locked Shields and Crossed Swords.[288] The intensified enhancement of cyber capabilities by the Romanian MoD has been ongoing for 4 years with a view to meeting the requirements of the national defence strategy, NATO and the EU.[289]

5.25.3 Current structure and resources

The CDC is part of the forces that actively contribute to the mission of the Romanian Armed Forces. In this context, its role is to plan, organise, control and conduct operations in cyberspace in order to support functional resilience and impact the joint forces across both national and allied environments. At the same time, the command provides network management, development and IT services.

Within the Romanian CDC, we can distinguish the Information Technology Agency, the Cyber Defence Agency and the Logistics Support Section. The cyber level commander of the CApC is General Gheorghe Iordache, and the Chief of Staff is Colonel Costel Maftei. Personnel numbers have not been disclosed by the Romanian side due to the sensitivity of this information.[290]

[286] I. Petcu, *The New Challenges of Romania's Cyber Security Policy*, Romanian Cyber Security Journal, May 2022, pp. 57-67.
[287] R. Lemos, *Nigeria & Romania Ranked Among Top Cybercrime Havens*, Dark Reading, 18 April 2024, https://www.darkreading.com/cybersecurity-analytics/nigeria-romania-ranked-among-top-cybercrime-havens accessed: 17.03.2025.
[288] K. Kaska, *National Cybersecurity Organisation: Romania*, NATO CCDCOE, Tallinn 2020, pp. 10-12.
[289] A. Olech, Interview with expert Iulian Popa of the New Strategy Center.
[290] *Cyber Command*, Ministerul Apărării Naționale, https://cybercommand.ro/webroot/en/pages/structure accessed: 17.03.2025.

FIGURE 29. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN ROMANIA.

5.26 Slovakia

5.26.1 Overview of the state's cybersecurity situation

As in other EU countries, the digital space in Slovakia has been and remains affected by the ongoing war in Ukraine. As a result, Bratislava and the NCSC (SK-CERT), founded in September 2019, have recorded attempted DDoS attacks on news portals and state institutions. In 2022, a total of 48,887,103 potential incidents in cyberspace were identified. Most incidents were detected and reported in May 2022. The targets of the attacks were primarily the public, banking and healthcare sectors.

The most common activities of cybercriminals, on the other hand, were information gathering, DDoS and DoS attacks, the use of botnets and malicious code. The problem for Slovakia at present is the lack of a sufficient number of cybersecurity professionals. Slovakia currently has only 86 certified cybersecurity auditors, while the audits themselves can be carried out by 52 authorised companies.[291] Slovakia's cyberspace has also been attacked by hackers linked to the Russian Federation. In 2022, Anonymous.ru attacked several sites in Slovakia, including airport and taxi services.[292]

5.26.2 History and evolution of cyber units

CSIRT.MIL.SK is the Military CSIRT of the MoD of the Slovak Republic. It was established on September 18 2013, as a special department within the Slovak Armed Forces. Based on a ministerial decision, it was integrated into Military Intelligence (a special service of the MoD of the Slovak Republic) on the 1st of November 2016 as CSIRT.MIL and subsequently renamed CSIRT.MIL.SK. On the 12th of February 2018, CSIRT.MIL.SK successfully obtained accreditation from the certifying body 'Trusted Introducer'. As a

[291] O. Evsyukova, M. Karpiuk, M. Kelemen, *Cyberthreats in Ukraine, Poland and Slovakia*, Cybersecurity and Law, no. 1, vol. 11, 2024, pp. 71-75.
[292] L. Kobzová, *Russian hackers have attacked several EU countries. Slovakia was also a victim*, Adapt Institute, 1 July 2024, https://www.adaptinstitute.org/russian-hackers-have-attacked-several-eu-countries-slovakia-was-also-a-victim/01/07/2024/ accessed: 17.03.2025.

result, it has become a full member of the international community of CSIRT/CERT teams – TF-CSIRT (Task Force of Computer Security Incident Response Teams).[293]

5.26.3 Current structure and resources

The Cyber Defence Centre of the Slovak Republic is a department within Military Intelligence that performs tasks of the Cyber Defence of the Slovak Republic, as well as providing cybersecurity for the information and communication infrastructures of the MoD and the Armed Forces of the Slovak Republic, in addition to other organisations which are subordinate to the Ministry. The Centre collects, aggregates, analyses and evaluates information important for Cyber Defence, informs affected parties of current threats and suggests appropriate measures. The Military Computer Security Response Team, CSIRT.MIL.SK, is also an integral part of the Cyber Defence Centre of the Slovak Republic.[294]

FIGURE 30. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN SLOVAKIA.

5.27 Slovenia

5.27.1 Overview of the state's cybersecurity situation

In 2018, the Slovenian Ministry of Public Administration published a cyber threat assessment. At that time, it was assessed that the main actors of cyber threats were cyber criminals, insiders, states or hacktivists.[295] Slovenia experienced more cyber attacks in 2022 than in 2021. At that time, 4,123 cybersecurity incidents were recorded, an increase of almost a third since 2021, according to the report of the SI-CERT National Cybersecurity Response Centre (NSCRC). Such cyber attacks were led by

[293] *CSIRT.MIL.SK*, Cyber Defence Center of the Slovak Republic, https://ckosr.sk/75688/?mne=3149 accessed: 17.03.2025.
[294] *Cyber Defence*, Cyber Defence Center of the Slovak Republic, https://ckosr.sk/75689/?mne=3146 accessed: 17.03.2025.

[295] D. Štrucl, *National Cybersecurity Organisation: Slovenia*, NATO CCDCOE, Tallinn 2021, pp. 10-11.

phishing attacks, accounting for 1,432 incidents, notwithstanding attacks on desktop computers and mobile devices.[296]

Slovenia faced a wave of DDoS attacks in 2024. In response, Prime Minister Robert Golob announced increased funding and the hiring of additional staff to strengthen cybersecurity. Russia was blamed for the spate of attacks in 2024, and the reason cited for the increase in cyber aggression was Slovenia's support for Ukraine. Active attacks of similar intensity are expected to continue for at least another two years.[297]

5.27.2 History and evolution of cyber units

The development of cybersecurity in the Slovenian Army (SAF) began in 2003 with the adoption of NATO Directive ACO 70-198 by the MoD and the SAF. In July 2011, the General Staff of the Slovenian Armed Forces (slv. Generalštab Slovenske vojske -GŠSV) issued an order to implement the strategic transformation imperatives, and in July 2013, the MoD prepared a cyber defence concept. Subsequently, in May 2014, the GŠSV issued an order to establish a new cyber defence capability. In October of the same year, a series of regulations were issued, resulting in the formation of a new cybersecurity section and MIL-CERT.

The 2020 Security White Paper and the Law on the Provision of Funds for Investment in the Slovenian Armed Forces from 2021 to 2026 provide a high level of cyber defence and increased cooperation with allies.[298] Slovenia has an official cybersecurity strategy document, although it is obsolete, given that it dates back to 2016.[299] Since then, no new initiatives have been forthcoming in the creation of a unified cybersecurity strategy for the country. In 2024, Slovenia signed an agreement with Poland on cooperation in the digital sector. The agreement envisages a further increase in the digital skills of citizens and an increase in digitalisation, including helping businesses with cybersecurity.[300]

According to the EC, in 2023, Slovenia made significant progress in the development of e-administration. Nevertheless, raising basic digital competency in Slovenian society remains a challenge.[301] Cybersecurity in Slovenia is regulated by the Information Security Act and the Decree on Information Security in State Administration.[302]

---

[296] *Europe in brief: Slovenia sees rise in cyberattacks*, ENR, 30 June 2023, https://europeannewsroom.com/europe-in-brief-slovenia-sees-rise-in-cyber-attacks/, accessed: 17.03.2025.
[297] *Slovenia hit by another cyberattack*, The Slovenia Times, 11 April 2024, https://sloveniatimes.com/40402/slovenia-hit-by-another-cyberattack, accessed: 17.03.2025.
[298] Ibid. p. 21-22.
[299] *Cyber Security Strategy of the Republic of Slovenia*, Government of the Republic of Slovenia, 2016, https://www.gov.si/assets/ministrstva/MDP/DID/Cyber_Security_Strategy_Slovenia.pdf, accessed: 17.03.2025.
[300] *Polska i Słowenia będą współpracować w zakresie cyberbezpieczeństwa i AI*, CyberDefence24, 2024 https://cyberdefence24.pl/technologie/polska-i-slowenia-beda-wspolpracowac-w-zakresie-cyberbezpieczenstwa-i-ai , accessed: 17.03.2025.
[301] *Slovenia - 2024 Digital Decade Country Report*. European Commission,
[302]Official Gazette of the Republic of Slovenia [Uradni list RS], Nos. 30/18 and 95/21, Official Gazette of the Republic of Slovenia [Uradni list RS], Nos. 29/18 and 131/20 https://pisrs.si/pregledPredpisa?id=ZAKO7707, accessed: 17.03.2025.

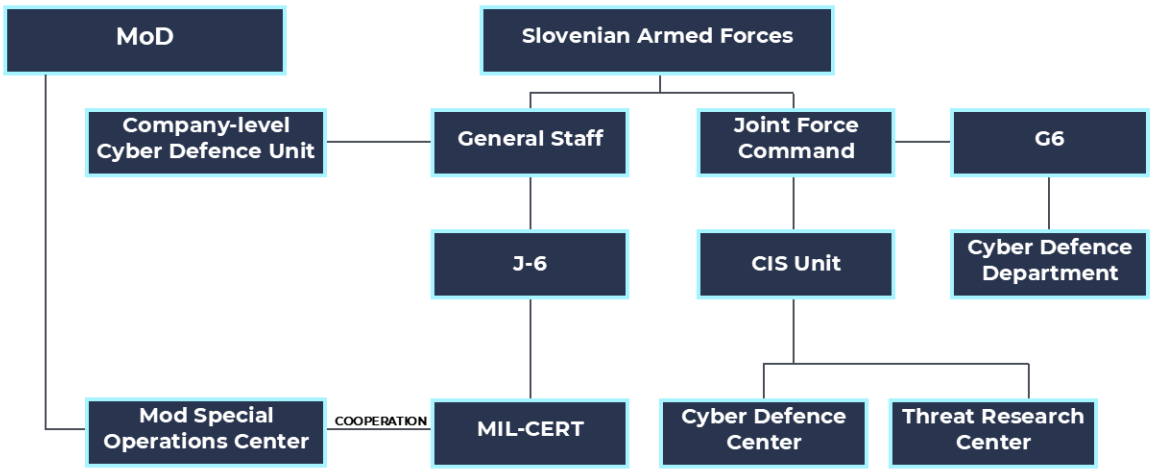
5.27.3 Current structure and resources

In October 2014, the Order on the Establishment of Cybersecurity Capabilities was issued, setting the foundation for SAF's Cyber Defence Strategy. This was followed by the Order for Work in the Slovenian Armed Forces for 2015 and 2016, which led to the formation of a cybersecurity section within the J-6 Department. At the same time, MIL-CERT was established as a working group, focusing on enhancing cyber resilience and response mechanisms.[303]

By 2018, SAF expanded its cybersecurity capabilities by creating two detachment-sized centres, one of which was dedicated to cyber defence and another to cyber threat research. These centres were placed at the tactical level and integrated into the main battalion-level CIS unit (*Enota za komunikacijske in informacijske sisteme – EKIS*). Their primary function was to conduct cyber defence operations and research evolving cyber threats.[304]

Slovenia officially recognised cyberspace as the fifth operational domain of warfare, reinforcing its commitment to cybersecurity and integrating cyber defence tasks within the existing armed forces structure. This strategic decision positioned cyber operations as a core component of its national defence policy.[305]

Looking ahead, SAF plans to establish a CDU at the company level by 2025. This unit will be integrated with all major CIS units and will operate under the auspices of the newly established joint CIS and Cyber Defence Headquarters (CISCDHQ), which will serve as the central command for cyber operations.



[303] *Initiatives to improve Cyber Defence capabilities - development of NATO cyber forces – Slovenia*, accessed: 17.03.2025.
[304] Enota za komunikacijske in informacijske sisteme (EKIS) | GOV.SI
[305] *Obrambna strategija Republike Slovenije*, Vlada Republike Slovenije, datum: 24. 04. 2024. Dostopno na: http://www.vlada.si/.

FIGURE 31. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN SLOVENIA.

5.28 Spain

5.28.1 Overview of the state's cybersecurity situation

According to expert assessments, in the case of Spain, the prevailing target of cyber criminals and hostile countries is its critical infrastructure.[306] The primary adversary responsible for carrying out attacks is the Russian Federation, particularly since 2022. According to Javier Candau, Head of Cybersecurity at Spain's National Intelligence Centre, in 2023, 45% of all major attacks against Spain were carried out within Russian territory.[307] The selection of targets in the form of defence industry entities and related ministries was linked to Spanish support for the Ukrainian cause.[308]

In its report on cyber threats and trends in 2024, the National Cryptologic Centre indicates that around 35% of the cyber espionage campaigns registered in 2023 were directed against government institutions. It also highlighted that Russia, China, North Korea and Iran all pose a significant cyber threat to Spain.[309]

During these attacks, hostile actors used ransomware and phishing against Spanish entities.[310] Expert data shows that 68% of Spanish companies lack adequate protection against cyber attacks, particularly SMEs.[311]

Catalonia is the region most frequently targeted by cyber criminals. This is linked to a longstanding disinformation campaign by the Russian Federation, which instrumentalises the dispute between the government in Madrid and the Catalan authorities. This is aimed at destabilising the political situation in Spain and inciting the public.[312]

5.28.2 History and evolution of cyber units

In 2006, the National Institute of Communication Technologies (spa. Instituto Nacional de Tecnologías de la Comunicación – INTECO) was created. In 2014, INTECO was rebranded as the Spanish National Institute of Cybersecurity (spa. Instituto Nacional de Ciberseguridad – INCIBE) and is dedicated exclusively to operations within this sphere. It is a public entity under the Ministry of Digital Transformation and Civil Service through the Secretariat of State for Digitalisation and AI. INCIBE is responsible for

[306] *Initiatives to improve Cyber Defence capabilities - development of NATO cyber forces - Spain*
[307] Brais Cedeira, El jefe de ciberseguridad del CNI: "El 45% de ataques graves a España este año viene de Rusia", El Español, 20 May 2023, https://www.elespanol.com/espana/20230520/ciberseguridad-cni-ataques-graves-espana-viene-rusia/764423880_0.html. accessed: 17.03.2025.
[308] *Spain Detains 3 Over Cyberattacks On Pro-Ukrainian Nations*, Radio Free Europe, 20 July 2024, https://www.rferl.org/a/cybercrime-nato-russia-spain-ukraine/33044049.html accessed: 17.03.2025.
[309] Centro Criptológico Nacional, "CCN-CERT IA-04/24: Ciberamenazas y Tendencias. Edición 2024", October 2024, https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html. accessed: 17.03.2025.
[310] T. Bianchi, *Distribution of cyber-attacks in Spain in 2023, by type*, Statista, 21 March 2024, https://www.statista.com/statistics/1458071/spain-share-cyber-attacks-by-type/ accessed: 17.03.2025.
[311] *68% of Spanish companies have no defence against cyber-attacks*, IFEMA Madrid, 2024, https://www.ifema.es/en/sicur/news/defense-against-cyberattacks accessed: 17.03.2025.
[312] C. Popov, *Catalonia is the most cyber-attacked region in Spain*, Bitdefender, 12 October 2023, https://www.bitdefender.com/en-us/blog/hotforsecurity/catalonia-is-the-most-cyber-attacked-region-in-spain/ accessed: 17.03.2025.

strengthening digital trust, enhancing cybersecurity and resilience, and supporting the market via promoting the safe use of cyberspace in Spain.[313]

In 2008, the National Cryptologic Centre (spa. Centro Criptológico Nacional) was established.[314] It is responsible for protecting classified information, ensuring the security of public administration ICT systems, developing and implementing national cryptographic technologies, and cooperating with international organisations and agencies.[315]

In January 2011, the Chief of Defence Staff (spa. Jefe del Estado Mayor de la Defensa -JEMAD) approved the 'Vision for Cyber Defence', while the 'Military Cyber Defence Concept' was subsequently approved in July of that year. A year later, JEMAD approved the 'Action Plan for Achieving Military Cyber Defence Capabilities'. All these decisions laid the groundwork for the Joint CDC, which was established by decree of the Minister of Defence in February 2013.

As part of the 2015 restructuring of the Spanish Armed Forces, the Armed Forces Information Systems and Telecommunications Command (spa. Jefatura de Sistemas de Información y Telecomunicaciones de las Fuerzas Armadas) was created. In 2020, it was integrated into the Joint Cyber Command (spa. Mando Conjunto del Ciberespacio - MCCE).[316] Its responsibilities are to plan and coordinate operations in cyberspace while integrating resources and personnel from diverse types of armed forces to ensure effective defence against cyber threats.[317]

5.28.3 Current structure and resources

The Joint Cyber Command comprises the MCCE Command, the Secretariat, and the Joint Staff of the Cyber Command. The PSDC is further divided into six sections, as follows:

- Coordination Section (C-0): Coordination of internal activities;
- Cyber Intelligence and Security Section (C-2): Threat analysis and cyber intelligence;
- Operations Section (C-3): Planning and conducting cyber operations;
- Plans Section (C-5): Development of strategies and long-term plans;
- Preparation Section (C-7): Training and preparation of staff and units;
- Cooperation and Representation Section (C-9): Maintaining contacts with other international institutions and organisations.[318]

The Joint Cyber Command also includes an operational command which is responsible for the implementation of cyber defence operations, as well as an Administrative and Service Command, which

[313] Instituto Nacional de Ciberseguridad (INCIBE), *'What is INCIBE'*, https://www.incibe.es/en/incibe/corporate-information/what-is-incibe. accessed: 17.03.2025.
[314] A. Marrone, E. Sabatino, op. cit. pp. 23-24.
[315] Centro Criptológico Nacional, 'CCN functions', https://www.ccn.cni.es/en/menu-ccn-en/functions-of-the-ccn. accessed: 17.03.2025.
[316] *Initiatives to improve Cyber Defence capabilities - development of NATO cyber forces - Spain*
[317] Ministerio de Defensa de España, 'Mando Conjunto del Ciberespacio (MCCE)', https://emad.defensa.gob.es/unidades/mcce/. accessed: 17.03.2025
[318] Ministerio de Defensa de España, 'Mando Conjunto del Ciberespacio (MCCE)', https://emad.defensa.gob.es/unidades/mcce/. accessed: 17.03.2025.

manages administrative and technical support. The current Commander of the MCCE is Major General Rafael García Hernández. The MCCE's current operational strength is approximately 300 soldiers and 100 civilians, with plans to expand to 1,200 personnel by 2030. The Combined Cyber Command is also working on acquiring and developing the NATO Classified Cyber Range (NCCR) training facility.[319]

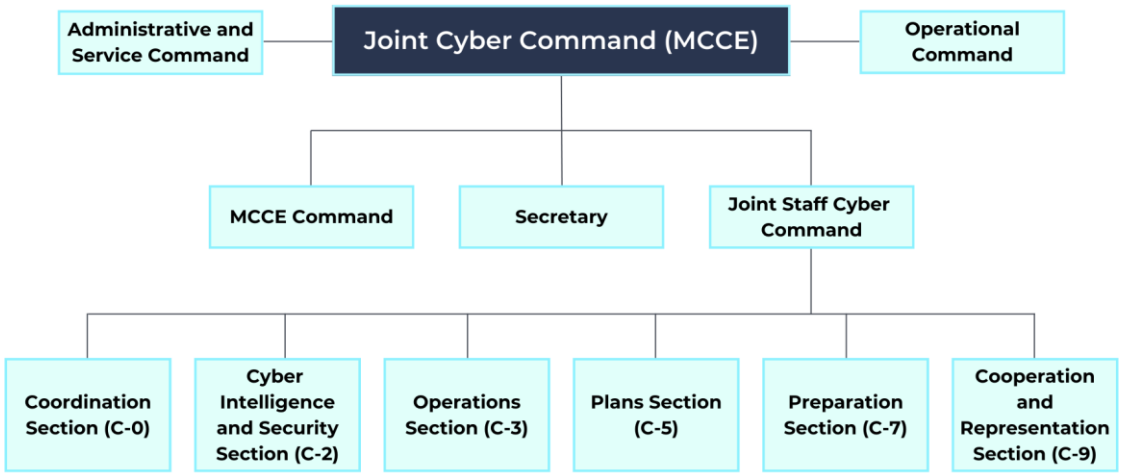


FIGURE 32. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN SPAIN.

5.29 Sweden

5.29.1 Overview of the state's cybersecurity situation

Since 2019, cyber attacks targeting Swedish companies and institutions have intensified. This resulted in the establishment of the NCSC in 2020, which included the Swedish Armed Forces and the Swedish Security Service (swe. Säkerhetspolisen - SÄPO). In its annual report, the SÄPO detailed how cyber attacks and influence operations are constantly being carried out by hostile state actors.

Statistics show that the number of cyber attacks in Sweden has tripled since 2019/2020. Most of these attacks have been attributed to actors linked to the Russian Federation. An interesting exception is the activity of Iran within the Stockholm cybersecurity sphere. The SÄPO accused the intelligence service of Tehran of hacking a text messaging service following religiously motivated incidents.[320]

5.29.2 History and evolution of cyber units

Swedish cyber forces have been developed continuously since 2000, with the first unit of this type established as a result of the Swedish Defence Act of 2000. In 2011, the Swedish Armed Forces decided

[319] Ibid.
[320] P. Kirby, *Sweden blames Iran for cyber-attack after Quran burnings*, BBC, 24 September 2024, https://www.bbc.com/news/articles/c0lw0081e1yo accessed: 17.03.2025.

to merge the three cyber defence units into the Armed Forces Telecommunications and Information Systems Team (swe. Försvarsmaktens telekommunikations – och informationssystemförband - FMTIS). Political decisions, logistical and planning difficulties meant that this process was not finalised until January 1st 2016. However, a separate military force was not established; only a command and intelligence unit.[321]

In the following years, additional units were created and transformed into a comprehensive cyber defence system. The Swedish parliament passed the Total Defence Act in December 2020, which included investments in strengthening the military's cyber capabilities by 2025. A decision was also made regarding the creation of cyber units called ITF and 2ITF.[322]

5.29.3 Current structure and resources

The cyber defence units operate primarily within the Armed Forces and may also support other agencies within the national cyber framework through the NCSC. Cyber activities are carried out by the Swedish Armed Forces and their dedicated cyber units. These units are funded through the Swedish Defence Act, although the exact financial outlay for 2024 has not been disclosed, nor has the number of active personnel.[323]

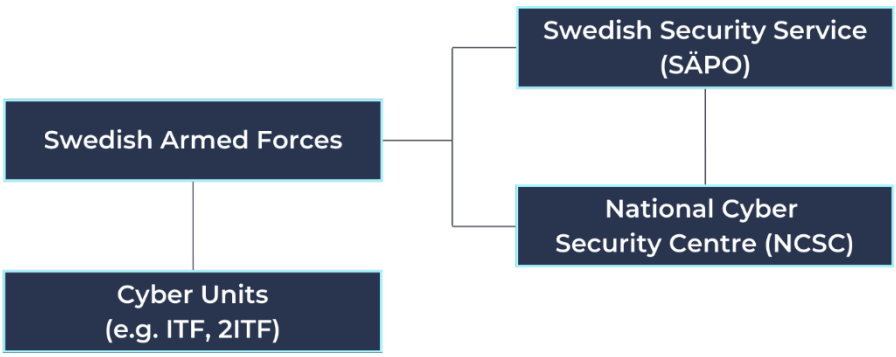


FIGURE 33. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN SWEDEN.

[321] M. Törn, *Försvarsmakten har fått ett nytt förband*, Försvarsmakten, 28 January 2016, https://www.forsvarsmakten.se/sv/aktuellt/2016/01/forsvarsmakten-har-fatt-ett-nytt-forband/ accessed: 17.03.2025.
[322] *Sweden steps up cyber efforts*, Shepard, 19 January 2022, https://www.shephardmedia.com/news/digital-battlespace/sweden-steps-up-cyber-efforts/ accessed: 17.03.2025.
[323] Interview.

5.30 Turkey

5.30.1 Overview of the state's cybersecurity situation

Turkey's strategic location on the Black Sea at the crossroads of Europe and Asia makes it a focal point on the international stage both globally and regionally. This also applies to the cyber sphere, which one might presume should not be driven by geography. The 2019 Global Cybersecurity Index report indicated that Turkey had become one of the 20 safest countries in the world in terms of cybersecurity. This achievement was made possible by preventive measures that led to a reduction in cyberattacks on Turkey from 118,470 in 2020 to 84,113 in 2021.[324]

Nevertheless, the global rise in cyber tensions has not spared Ankara either. In August 2023, Turkey became one of the most cyber-exposed countries. This was influenced by several events in the region in which the Turkish authorities were involved, such as the outbreak of another Israeli-Palestinian war, activities in Lebanon, the Israeli-Iranian conflict, and the war in Ukraine.[325]

Turkey's cybersecurity strategy has since evolved in response to these threats. In 2020, the government published the 'National Cybersecurity Strategy and Action Plan for 2020-2023'.[326] It was updated and extended in 2024 for a period of four years. It now emphasises the need for tackling cyber threats around the clock, threats which are constantly growing in number and complexity, as well as further strengthening Turkey's leading position in the field of cybersecurity at the international level.[327]

5.30.2 History and evolution of cyber units

In October 2010, the Turkish military released a 'Red Book' in which it was suggested that cyberspace was seen as an unconventional threat. A year after its publication, the Turkish National Security Council ratified the National Strategy, which, for the first time, included cyber threats. At that time, government institutions such as the Computer/Cyber Emergency Response Team (TR-CERT) and the Cyber Fusion Centre began to develop. Both organisations operate under the oversight of the Ministry of National Defence of Türkiye.

By 2010-2011, a plan was being prepared to establish a 'Cyber Command' within the General Staff of the Turkish Armed Forces (tür. Türk Silahlı Kuvvetleri Genelkurmay Başkanlığı -TSKGB), and its implementation began in 2013. Concurrently, the Turkish Minister of Communications and Transport approved the implementation of the Turkish Cyber Defence Programme.[328] However, it should be noted that the Turkish Armed Forces CDC was established in 2012, originally in the form of the Cyber Defence Centre.[329]

---

[324] D. Liszkowska, *Türkey's Cybersecurity Policy Framework*, Cybersecurity and Law, no. 11, vol. 1, pp. 80-81.
[325] *Türkiye becomes world's most cyber targeted region in 2023*, Daily Sabah, 7 December 2023, https://www.dailysabah.com/turkiye/turkiye-becomes-worlds-most-cyber-targeted-region-in-2023/news accessed: 17.03.2025.
[326] D. Liszkowska, *Türkey's Cybersecurity Policy...*, p. 85.
[327] *National Cyber Security Strategy and Action Plan (2024-2028)*, Ministry of Transport and Infrastructure of the Republic of Turkey, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2024-2028.pdf accessed: 17.03.2025.
[328] O. Eitan, *Turkey-Challenges to the Struggle against Cyber Threats*, Cyber, Intelligence and Security, vol. 2, no. 1, May 2018, pp. 42-44.
[329] *Turkey-Challenges to the Struggle against Cyber Threats*, INSS, CYBER CAPABILITIES AND NATIONAL POWER, no. 2 May 2018, p. 143.

However, the development of threats has led to increasing cooperation in the cyber field between ministries. In late 2016, the Turkish government launched a recruitment campaign for university graduates to work in cybersecurity.[330] An important element of the development and evolution of Turkey's military cyber structures is the conducting of annual military cyber exercises, which were introduced to train proactive responses to national security threats.[331]

5.30.3 Current structure and resources

The military cyber defence is the responsibility of the MoD, which holds the highest authority in the cyber domain. The Turkish Armed Forces CDC (tür. Silahlı Kuvvetleri Siber Savunma Komutanlığı - TSKSSK) is the primary cybersecurity unit and is responsible for the defence of military networks in Turkey and, simultaneously, is the highest military CERT authority (TAF-CERT). TAF-CERT is a transmission organisation that cooperates with NATO, the national CERT, and units subordinate to the military.

In the command structure, the TSKSSK functions within the Directorate of Communication, Electronics and Information Systems of the Turkish General Staff. The Turkish CDC involves personnel from all services, and the Command itself works closely with the Ministry of Transport and Infrastructure.[332] There is also an extensive Cybercrime Department of the Turkish National Police (TNP), which conducts cybercrime investigations and also provides forensic expertise in support of other police agencies and the prosecution in cases where technology is a significant factor in the crime or is linked to evidence in the case.[333] In addition, Turkey has well-established and active cyber intelligence capabilities on domestic political surveillance, foreign espionage and counter-espionage targets.[334]

[330] *Turkey Establishing a 'Cyber Army' To Counter National Cyber Threats*, Space Watch, 13 June 2017, https://spacewatch.global/2017/06/turkey-establishing-cyber-army-counter-national-cyber-threats/ accessed: 17.03.2025.
[331] E. Halisdemir, *National Cybersecurity Organisation: Turkey*, NATO CCDCOE, Tallinn 2021, p. 14.

[332] Ibid, pp. 14-15.
[333] *Turkey*, Council of Europe, https://www.coe.int/en/web/octopus/-/turkey accessed: 17.03.2025.
[334] *Capabilities and National Power: Volume 2 - Türkiye*, International Institute for Strategic Studies (IISS), 2023 https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_12-turkiye.pdf accessed: 17.03.2025.

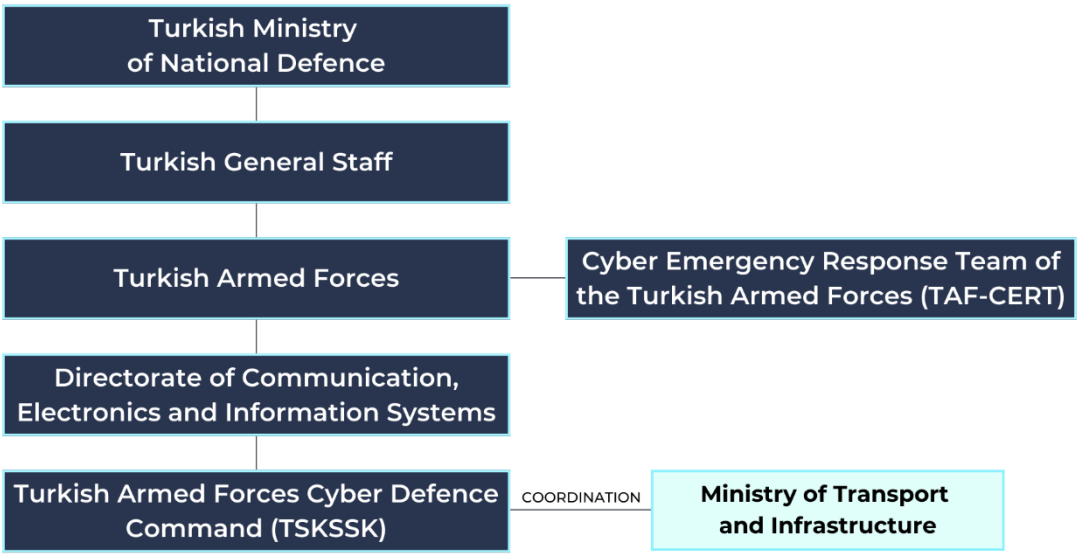


FIGURE 34. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN TURKEY.

5.31 The United Kingdom

5.31.1 Overview of the state's cybersecurity situation

The UK assumes that its cyberspace is under attack from entities identified as organised (cyber)criminal groups, which may be used by unfriendly states as proxies for cyber attacks. Furthermore, adversarial states such as Russia, China, Iran or North Korea are identified as the greatest cyber threats to UK interests. The listed threat actors are also 'hacktivists' and individuals.[335] Phishing, ransomware, spyware and DDoS attacks are identified as the most common forms of cyber attacks.

The problem lies not only in the form of such cyber attacks, but also in how to adequately protect against them. Research shows that British citizens and companies are showing improved 'cyber-hygiene' online. On the other hand, the 2024 Cybersecurity Breach Survey found that 50% of businesses had been the victim of a cyber attack or security breach in the previous 12 months, an increase of more than 10% compared to 2022. The UK's Action Fraud reported that, in 2020, victims of online shopping fraud lost a total of 63.8 million £.[336] The Cybersecurity Strategy 2022-2030 indicates that the UK is the third most frequently attacked country after the US and Ukraine. The adoption of this document during such a crucial period suggests that London is taking the evolution of the cyber environment and the security of this domain very seriously.[337]

[335] *Cybersecurity in the UK*, House of Commons, 19 April 2024, pp. 7-8.
[336] *UK Cybercrime Statistics 2024*, Twenty Four IT, 25 October 2024, https://www.twenty-four.it/services/cyber-security-services/cyber-crime-prevention/cybercrime-statistics-uk/ accessed: 17.03.2025.
[337] *Government Cyber Security Strategy Building a cyber resilient public sector*, HM Government, 2022, p. 17.

5.31.2 History and evolution of cyber units

Initially, agencies such as Government Communications Headquarters (GCHQ) played a leading role. The 2009 Cybersecurity Strategy doctrine suggested the need to develop offensive and defensive capabilities within the digital domain. In 2013, the UK established the Defence Cyber Operations Group (JFCyG), which reported directly to UK Strategic Command.

A crucial step was the creation of the NCSC in 2016, again operating within GCHQ. Plans to form a cyber unit were reported as early as September 2018. Another milestone was the establishment of the National Cyber Force in 2020. This unit took over the objectives of the former National Offensive Cyber Programme (NOCP), which had been operational since 2014.[338]

5.31.3 Current structure and resources

Strategic policy on cybersecurity is determined by the Prime Minister and Cabinet and enacted by the NCF, NCSS and NCSC. Unlike the US, the UK has yet to establish a unified military Cyber Command. However, the UK Armed Forces are responsible for cybersecurity. C2 of this task rests with UK Strategic Command and its subordinate JFCyG.

The NCF integrates relevant cyber elements of GCHQ with segments of the MoD, the Secret Intelligence Service (SIS) and Defence Science and Technology Laboratory under a single organisation and unified command. The NCF Commander reports to both the Head of GCHQ and the Commander of Strategic Command, and NCF operations are politically authorised by the Minister of Foreign Affairs or the Secretary of State for Defence.[339] Since 2023, the NCF Commander has been General Tim Neal-Hopes. In the NCF's first year, 76 million £ was invested in the unit.[340]

[338] *Cyber Capabilities And National Power: A Net Assessment. United Kingdom*, The International Institute For Strategic Studies, 2021, pp. 29-39.
[339] Ibid.
[340] K. Sengputa, *UK is nearly ready to launch force to hit hostile countries with cyberattacks*, Independent, 10 January 2020, https://www.independent.co.uk/news/uk/home-news/cyber-warfare-security-force-iran-crisis-ministry-of-defence-a9278591.html accessed: 17.03.2025.

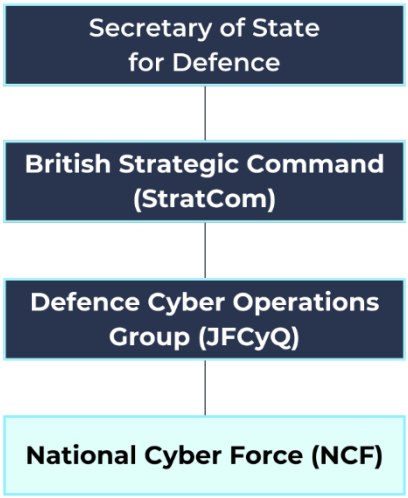


FIGURE 35. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN THE UK.

5.32 The United States

5.32.1 Overview of the state's cybersecurity situation

The greatest threat to US cybersecurity comes from state-sponsored hackers – most notably those originating from Russia, China, North Korea and Iran. In the case of Russia, the US considers the Russian Foreign Intelligence Service (SVR) particularly dangerous and holds it accountable for, *inter alia*, the cyber attack on SolarWinds[341]. Originally, SVR's activity was limited to espionage activities targeting governments, think tanks, healthcare or energy sectors. However, there has been a gradual expansion of areas of interest, including education, aviation, law enforcement and military entities, and its most common tactic is to gain access to the cloud by exploiting vulnerabilities.[342]

Washington, however, regards the People's Republic of China as its greatest cyber adversary. Threat actors supported by Chinese policymakers include the Volt Typhoon group,[343] which primarily targets communications, energy, and transport systems sectors within the continental United States and across its maritime territories, including the US Virgin Islands. US Cyber Command (USCYBERCOM) emphasises that China is using malicious software to threaten American infrastructure, including manipulating systems providing water, power or fuel, in addition to gaining access to IT networks.

[341] Biden Administration Announces Expansion of Sanctions Against Russia and Signals Potential Additional Restrictions Following SolarWinds Cyber Attack, Mayer Brown, 16 April 2021, https://www.mayerbrown.com/en/insights/publications/2021/04/biden-administration-announces-expansion-of-sanctions-against-russia-and-signals-potential-additional-restrictions-following-solarwinds-cyber-attack accessed: 17.03.2025.

[342] Cybersecurity and Infrastructure Security Agency, *SVR Cyber Actors Adapt Tactics for Initial Cloud Access*, February 26, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a accessed: 05.02.2025.

[343] Cybersecurity and Infrastructure Security Agency, *People's Republic of China Cyber Threat*, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china accessed: 05.02.2025.

The USCYBERCOM commander stated that "the cyber challenge posed by China is unparalleled in terms of the challenges the United States and its allies have ever faced".[344] China's espionage activities are also being observed in Cuba. Recent reports indicate the presence of several intelligence bases equipped with SIGINT systems on the island (*e.g.*, the base in Bejucal).

In the US, responsibility for ransomware attacks against healthcare sectors and other critical infrastructure facilities (e.g. the Critical Infrastructure Fund DPRK attack and other malicious cyber activities) is attributed to North Korea (the DPRK) which also uses other techniques to launch cyber attacks, such as stealing cryptocurrencies and/or demanding ransoms in return.[345] As a result of these illicit operations, the DPRK enriches its national budget while pursuing the regime's goals and priorities. Cybercrime groups associated with or sponsored by the DPRK, as identified by the U.S., include APT Kimsuky, Lazarus Group, APT38, and BlueNoroff. Pyongyang has also focused its efforts on obtaining data related to key military and energy technologies. One notorious example of such activity was the DPRK's release of a malware variant known as 'BLINDINGCAN' on August 19 2020.[346]

The US has also expressed concern over cyber activities originating from Iran, particularly in the context of electoral interference. Ahead of the 2024 presidential election, officials were especially wary due to Iranian-linked cyber operations during the 2020 election cycle. These operations included efforts to obtain voter registration data and distribute deceptive emails posing as members of the far-right Proud Boys group, which contained threats and disinformation aimed at intimidating voters and influencing public opinion. The US has implicated the Islamic Revolutionary Guard Corps (IRGC), affiliated with the Iranian government and identified as a terrorist organisation, as being responsible for the attacks.[347]

5.32.2 History and evolution of cyber units

The US Cyber Command (USCYBERCOM) is considered the primary authority responsible for cybersecurity. It was established on the initiative of Robert Gates, who recognised such emergent technologies as a growing threat. However, the defence of cyberspace began earlier and, even as early as 1972, the US military was making efforts to reduce vulnerabilities and protect information systems. In 1998, the Department of Defense created the Joint Task Force-Computer Network Defence (JTF-CND), which operated in cooperation with the Defence Information Systems Agency (DISA). A year later, JTF-CND evolved into the Joint Task Force-Computer Network Operations (JTF-CNO), operating within the US Space Command (USSPACECOM). Following the dissolution of USSPACOM in October 2002, JTF-CNO was transferred to USSTRATCOM.

---

[344] U.S. Department of Defense, *U.S. Can Respond Decisively to Cyber Threat Posed by China*, February 1, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3663799/us-can-respond-decisively-to-cyber-threat-posed-by-china/ accessed: 05.02.2025.

[345] Cybersecurity and Infrastructure Security Agency, *#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities*, February 09, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a accessed: 05.02.2025.

[346] Cybersecurity and Infrastructure Security Agency, *North Korea State-Sponsored Cyber Threat: Advisories*, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/north-korea/publications accessed: 05.02.2025.

[347] Cybersecurity and Infrastructure Security Agency, *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities*, December 18, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a accessed: 05.02.2025.

In 2004, Secretary of Defence Donald Rumsfeld divided the JTF-CNO into defensive and offensive components, specifically the Joint Task Force – Global Network Operations (JTF-GNO), which was responsible for defence, and the Joint Functional Component Command – Network Warfare (JFCC-NW), tasked with planning offensive cyber operations. It was not until 2009 that Gates ordered the Department of Defense to reorganise cyberspace. As a result, JFCC-NW and JTF-GNO merged on May 21 2010, into the US Cyber Command.[348]

Since 2012, USCYBERCOM has established 133 new cyber teams:[349]

- 13 National Mission Teams that were established to defend against large-scale cyber attacks that could affect US national security. Their mission is to detect, neutralise and respond to cyber threats of strategic importance.
- 68 Cyber Protection Teams focusing on the Department of Defence's critical networks and systems against prioritised threats. They are responsible for securing critical infrastructure to ensure its continuity and reliability in the event of attacks.
- 27 Combat Mission Teams delivering coordinated cyber attacks that support operational plans and crisis operations. Their mission is to use cyberspace in warfare to neutralise hostile cyber activities.
- 25 Cyber Support Teams that provide analytical and planning support to national and combat mission teams, assisting in the development of strategies and tactics, as well as threat analysis.

5.32.3 Current structure and resources

Currently, the USCYBERCOM structure comprises six components:

- The US Army Cyber Command (ARCYBER) is responsible for operating and defending the US Army network. The team consists of 16,500 soldiers, civilians and contractors;[350]
- US Fleet Cyber Command (FCC)/Navy Space Command (NAVSPACE), which is equipped with 13,000 posts and quarters for active and reserve sailors and civilians organised into 26 active commands, 40 Cyber Mission Force units, and 29 reserve commands around the world;[351]
- Sixteenth Air Force (Air Forces Cyber);
- US Marine Corps Forces Cyberspace Command;
- Cyber National Mission Force (CNMF);
- Joint Force Headquarters – Department of Defense Information Network.

The budget request for USCYBERCOM for the fiscal year 2025 is $1,705,736 bn, which is $54,432 m higher than the estimate for fiscal year 2024.[352] Since early 2015, USCYBERCOM has been undergoing

[348] U.S. Cyber Command, *Our History*, https://www.cybercom.mil/About/History/ accessed: 05.02.2025.
[349] U.S. Cyber Command, *History*, U.S. Cyber Command Official Website, https://www.cybercom.mil/About/History , accessed: 10.02.2025.
[350] U.S. Army Cyber Command, https://www.arcyber.army.mil/About/About-Army-Cyber/ accessed: 05.02.2025.
[351] U.S. Fleet Cyber Command/Navy Space Command, *Command Description*, https://www.fcc.navy.mil/ accessed: 05.02.2025.
[352] United States Cyber Command, *Fiscal Year 2025 Budget Estimates*, March 2024, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/CYBERCOM_OP-5.pdf accessed: 05.02.2025.

significant changes to enhance its cyber warfare capabilities.[353] The case for a dedicated US Cyber Military Force is being considered.[354]

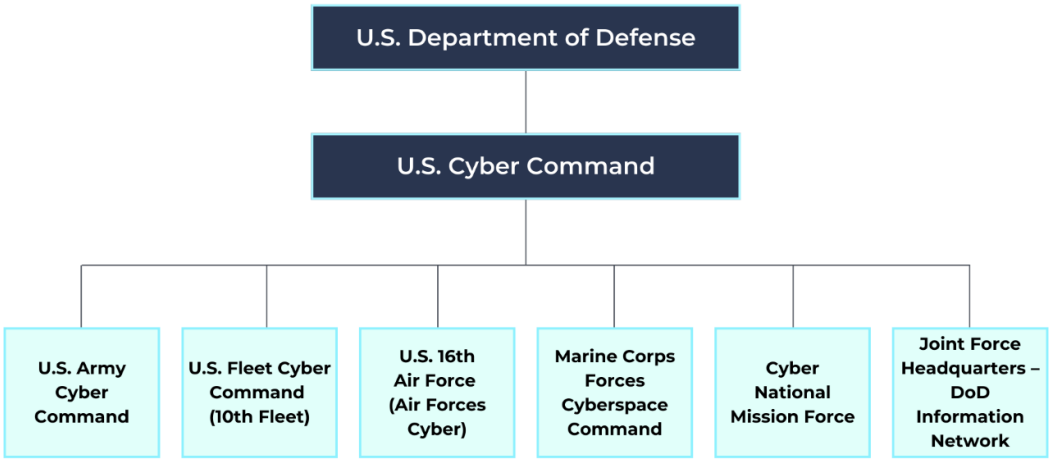


FIGURE 36. CYBER FORCES: CURRENT STATUS AND ORGANISATIONAL FRAMEWORK IN THE US.

[353] M. Pomerleau, *House lawmakers receive first briefing on Cybercom 2.0 model: Members heard from top DOD officials on the plan to mature U.S. Cyber Command*, DefenseScoop, https://defensescoop.com/2025/02/12/cybercom-2-0-model-house-lawmakers-receive-first-briefing, accessed: 23.02.2025.
[354] C. Couillard, *Beyond USCYBERCOM: The Need to Establish a Dedicated U.S. Cyber Military Force*, Cyber Defense Review, Spring 2024, https://cyberdefensereview.army.mil/Portals/6/Documents/2024_Spring/Couillard_CDRV9N1-Spring-2024.pdf, accessed: 16.02.2025.

6. Challenges and progress in NATO Cyber Force development

With thirty-two member states, the greatest extent of NATO membership since its establishment, each state has advanced its cyber capabilities over recent years to safeguard national security and enhance multinational cooperation. Moreover, after many cyber attacks, the significance of the Alliance has escalated due to emerging challenges in the cyber realm, requiring the use of innovative technology, an interactive strategy, and a defensive stance. NATO is a military institution and, in light of the present global conflicts, its military stance in cyberspace will become more crucial.[355]

Analysing the many concerns of cyber issues inside NATO members at both the national and international levels is very challenging.[356] Moreover, the concept of cyber forces is still very new and, for many countries, remains more of a vision or project rather than an established branch of the armed forces.[357] This paper emphasises the advancement of cyber involvement and the development of cyber forces in particular countries, while referencing several institutions in specific nations and within NATO as a whole. This evolution is driven by the growing number of cyber-related and hybrid threats and the shifting approach of the Alliance and its member states.[358] It must be underlined that cyberspace is full of challenges from malicious actors, and the process of cyber development will be contested.

Regarding land, sea, air, and space, the Alliance's acknowledgement of cyberspace as an operational domain underlines NATO's strategic vision of modern conflicts, in which cyber forces could be crucial. Such awareness is the very foundation for conducting effective cyber operations and serves as the pillar for greater cyber resilience. Recent developments of NATO policies, supported by national changes of specific countries, show that the cyber domain requires yet more active operations.[359]

Establishing itself at the Warsaw Summit, the NATO Cyber Defence Pledge highlights the need for member states to improve their own national cyber defences,[360] as any weaknesses in one state could endanger the whole Alliance.[361] Furthermore, as this research pointed out, the Alliance has been carrying out a number of projects to foster collaboration, coordination, support, readiness, and inspiration to improve allied nation-to-nation cooperation and deal with cyber incidents. Exercises like the annual Cyber Coalition model actual cyber attacks and assess the extent of coordination among NATO entities. They

---

[355] NATO JFCBS, *Cyber Coalition 2024 – Strengthening NATO Cyber Defence*, https://jfcbs.nato.int/page5964943/2024/cyber-coalition-2024--strengthening-natocyber-defence, accessed: 16.02.2025.

[356] V. Psychogiou, *Cyberspace: Is NATO Doing Enough?*, https://finabel.org/wp-content/uploads/2023/01/Cyberspace_Is-NATO-doing-enough-_-Vasiliki-Psychogiou_DAN.pdf, accessed: 16.02.2025.

[357] J. Blessing, *The Global Spread of Cyber Forces, 2000–2018*, 13th International Conference on Cyber Conflict Going Viral T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.) 2021, NATO CCDCOE Publications, Tallinn.

[358] NATO, *Statement by the North Atlantic Council on recent Russian hybrid activities*, http://nato.int/cps/en/natohq/official_texts_225230.htm?selectedLocale=en7, accessed: 16.02.2025.

[359] P. Hałys, *Cyberspace as a Domain of Operational Activities and the Resulting Challenge*, Faculty of Mechanical Engineering, Wroclaw University of Science and Technology, 2021, Volume 53, Number 2(200).

[360] A. Kozłowski, *NATO in Cyberspace After Madrid Summit, Pulaski Commentary*, https://pulaski.pl/en/pulaski-commentary-nato-in-cyberspace-after-madrid-summit-andrzej-kozlowski/, accessed: 16.02.2025.

[361] NATO CCD COE, *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit, accessed: 14.02.2025.

underscore the need to share capabilities and best practices as well as to practice with extant or future cyber forces. Notwithstanding these initiatives, NATO still faces major difficulties, especially in keeping up with the fast technological developments and ever more complex cyber threats.[362]

Both state and non-state actors conduct cyberspace operations. Non-state actors include individuals, criminal organisations, terrorist groups, and state-affiliated or state-sanctioned "patriotic hackers". State actors primarily consist of intelligence services and militaries. This diversity of threats makes it extremely difficult for countries and their defence units to effectively address the wide range of cyber threats they face.

State-sponsored cyber operations tend to be more impactful due to superior resources and funding, with NATO identifying Russia and China as primary cyber threats at the 2021 Brussels Summit. Adversaries utilise cyber operations in three key ways: first, to achieve independent effects in cyberspace, ranging from unsophisticated DDoS attacks, such as those targeting Estonia in 2007, to more sophisticated malware deployment, such as the 2014 Russian-sponsored compromise of a German steel mill's ICS. Second, cyber operations serve as a military force multiplier, as exemplified by Russia's 2008 invasion of Georgia, where cyber attacks on communication systems weakened Georgia's ability to coordinate its defences, and in Russia's illegal occupation of Crimea, where cyber tools were deployed alongside kinetic weapons. Finally, cyber operations facilitate broader grey zone activities, including industrial espionage, intellectual property theft, election meddling, and infrastructure compromise, with notable examples such as China's 2009 theft of F-35 fighter jet designs, Russian infiltration of US power grids, and various election interference campaigns targeting the US and Europe.[363]

The disparate degrees of cyber force development among NATO members indicate each nation's dedication to improving its cyber capabilities. While some nations—like the US, the UK, Estonia, Italy, and France—have sophisticated cyber forces with dedicated military cyber commands, others lack the people, resources or technical infrastructure. This disparity creates flaws in NATO's collective defence system, which enables rivals to access the larger NATO network via its weaker members. The rising occurrence of cybercrime, particularly in relation to Russia and China, has driven several NATO nations to hasten the creation of dedicated cyber teams. Other European nations were sparked into action by the invasion of Ukraine, an event which emphasised the importance of investing in cyber capabilities as a basic component of national defence.[364]

There has been a growing number of implementations of cyber strategies in the 21st century. This approach is closely linked to the establishment of a civilian framework for cybersecurity and the creation of cyber forces. Unsurprisingly, those countries which have prioritised the implementation of strategies are significantly enhancing their cyber military capabilities.

---

[362] NATO ACT, *Cyber Coalition: NATO's Flagship Cyber Exercise*, https://www.act.nato.int/activities/cyber-coalition, accessed: 14.02.2025.

[363] J. Blessing, *Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain*, NATO 2030 and Beyond: A Handbook for the Next Generation of Transatlantic Leaders, Johns Hopkins University SAIS, 2021, pp. 264-266.

[364] S. Spaulding, M. Montgomery, *NATO and Cyber: Outrunning the Bear*, CSIS, 24.07.2024, https://www.csis.org/analysis/nato-and-cyber-outrunning-bear, accessed: 14.02.2025.

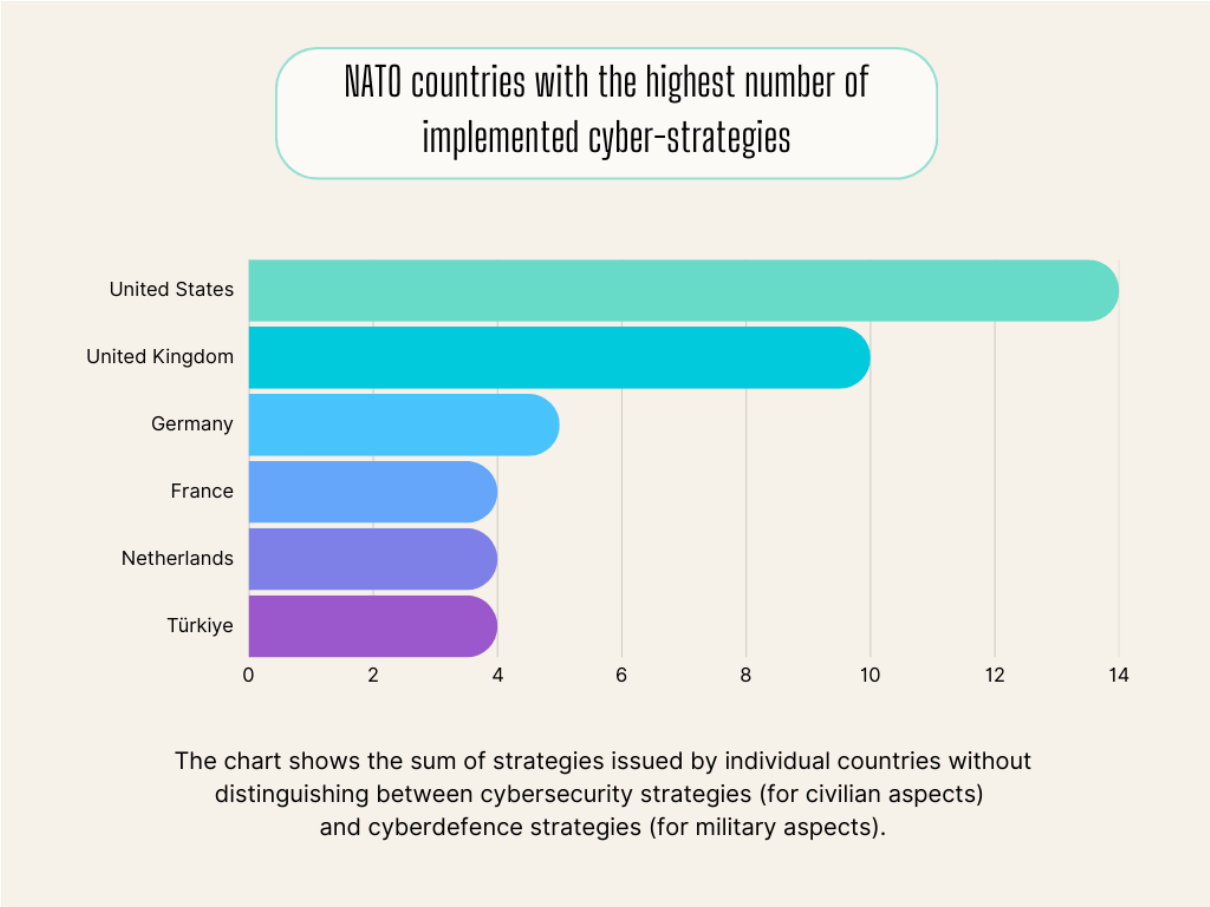


FIGURE 37. NATO COUNTRIES WITH THE HIGHEST NUMBER OF IMPLEMENTED CYBER STRATEGIES.

The development of national cyber commands/cyber units among NATO members has been an evident trend in the recent decade. Originally, mostly dedicated groups worked alongside conventional armed forces, as they are absolutely vital in conducting both defensive and offensive cyber operations.[365] Many countries in the Alliance, it could be said, more than half, as proven in this report, have already made significant strides in developing their cyber forces, even at the preliminary level, focusing on both protecting national infrastructure and carrying out cyber operations. If the adversary is already identifiable (for instance, malicious activity from the Russian Federation), the integration of national cyber forces into NATO's larger structure would definitely strengthen the Alliance's collective security posture and enable a coordinated and efficient response to cyber attacks.

Cyber-related activities are very often state-sponsored, and their growing complexity emphasises the critical need for robust cyber capabilities to protect military networks, government institutions, and critical infrastructure.[366] Countries, international organisations, and civilians are in danger of being exposed to

[365] M. Smeets, *The challenges of military adaptation to the cyberdomain: a case study of the Netherlands*, Small Wars & Insurgencies 2023, vol. 34, no. 7, pp. 1343–136.
[366] CSIS, *Significant Cyber Incidents, Significant Cyber Incidents Since 2006 (2006-2025)*, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents, accessed: 18.02.2025.

cyberattacks. As stated, a well-organised, committed, and well-funded cyber force could be a 'game changer' in the cyber rivalry.

Improving a nation's cyber resilience depends critically on CIMIC since cyber threats are often transnational, multifarious, and demand a whole-of-nation response. Both the military and the civilian sectors offer special strengths and capabilities; good cooperation among these agencies enhances the general capacity of a nation to prevent, react to, and recover from cyber events.[367]

The modern battlefield has transcended traditional domains to include cyberspace, where information warfare, digital espionage, and disruptive cyberattacks are now critical tools of geopolitical competition.[368] The ability to operate effectively in cyberspace is not merely a strategic advantage but a fundamental requirement for modern defence.[369] Given that cyberattacks can cripple national economies, interfere with democratic processes, and disable military assets, NATO countries must ensure their cyber forces are prepared to counter these threats proactively.[370]

NATO members must recognise that cyberspace is not just an operational domain—it is a battlefield where preparedness, resilience, and offensive capabilities are essential for maintaining security and strategic stability.[371] However, questions remain regarding the legal and operational boundaries of NATO's cyber strategy, particularly concerning the extent to which cyber attacks can be considered acts of war and whether NATO's collective defence clause, Article 5, would be triggered in the event of a significant cyber attack.[372]

Currently, cyber defence serves as a support element within NATO's land, air, and sea operational commands, though the potential establishment of a dedicated NATO command for cyber operations remains an open possibility. This would depend on the development of doctrines and capabilities, a process that is still in its early stages. In the meantime, NATO agencies play a critical role by providing continuous monitoring and assistance during cyber attacks, including deploying Cyber Reaction Teams to support member countries.[373]

---

[367] NATO, *Resilience – A Core Element of NATO's Deterrence and Defence*, https://www.nato.int/cps/uk/natohq/topics_132722.htm, accessed: 16.02.2025.
CIMIC Centre of Excellence, *Resilience in the Cyber Domain*, https://www.cimic-coe.org/ccoe_events/seminars/10-Feb-2022/, accessed: 16.02.2025.
M. Tikk, *Civil-Military Relations and International Military Cooperation in Cyber Security*, NATO CCDCOE, https://ccdcoe.org/uploads/2018/10/Art-05-Civil-Military-Relations-and-International-Military-Cooperation-in-Cyber-Security.pdf, accessed: 16.02.2025.

[368] MSSPAlert, *Escalating Cyber Threats Faced by NATO Countries*, https://www.msspalert.com/brief/escalating-cyber-threats-faced-by-nato-countries, accessed: 18.02.2025.

[369] U.S. Department of Defense, *2023 DoD Cyber Strategy Summary*, September 12, 2023.

[370] Christian-Marc Liflände r, "*NATO's Cyber Resilience: Proactive Defense Strategies*," The Record, February 2025, https://therecord.media/nato-resilience-cyberdefense-liflander-cycon, accessed: 15.02.2025.

[371] M. Machiels, *Active Cyber Defence and NATO: NATO's Innovative Offensive Strategy Towards Russia and China*, The Atlantic Forum, https://www.atlantic-forum.com/atlantica/active-cyber-defence-and-nato-natos-innovative-offensive-strategy-towards-russia-and-china, accessed: 16.02.2025.

[372] R. Bossong, *Cyber Attacks and Article 5: A Note on a Blurry but Consistent Position of NATO*, Center for Security Studies (CSS), ETH Zürich, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf, accessed: 16.02.2025.

[373] A. Marrone, E. Sabatino, *Cyber Defence in NATO Countries: Comparing Models*, Istituto Affari Internazionali (IAI), February 2021, p. 26.

Equipping the Alliance with cutting-edge technology necessitates collaboration with the private sector,[374] while cooperation with the EU on cybersecurity issues has become increasingly vital.[375] Furthermore, as individual member states continue to expand their cyber capabilities, NATO envisions training its personnel for the cyber battlefield in much the same way as soldiers are trained for traditional warfare, reflecting the growing importance of cyberspace in modern conflict.[376]

As the idea of developing cyber forces (or cyber soldiers) emerges, it must be emphasised that, in future cybernetworks, highly interconnected systems, isolated defence vehicles, sensors, effectors, and critical infrastructures with extremely low failure rate requirements will pose challenges. Human security operators may struggle to access these systems quickly and respond fast enough to cyber attacks. Therefore, the development of an active, autonomous, and AI-enabled cyber defence architecture will be essential.[377] It is worth noting that Ukraine is working on establishing its cyber forces as another type of armed force.[378]

The research presented in this article highlights the growing development of cyber capabilities, including the expansion of cyber forces. This trend has become increasingly evident in recent years, as member states' respective cyber strategies are more often focused on the military aspects of cybersecurity.[379] The author contends that the findings of this report clearly demonstrate that there will be continuous evolution among the thirty-two allies toward prioritising their collective military capabilities in cyberspace.

In conclusion, as cyber threats continue to evolve at different levels, NATO's proactive approach must be highlighted, as it is clearly demonstrated that the Alliance is effectively addressing emerging issues.[380] While significant progress has been made in enhancing cyber cooperation among members, there remain many areas in which cooperation must be improved, including reactive cyber capabilities, perceptions of law, the potential to act offensively as well as defensively, and the readiness to respond when cyber warfare begins.

Furthermore, concerning cyber-related forces, the role of NATO should be perceived through the eyes of individual members of the Alliance, as they are the most cognisant of threats. Each nation encounters distinct challenges and types of assaults. Consequently, each member should persist in investing in its own robust CIS infrastructure, cultivating robust partnerships (both bilateral and multilateral, as well as

---

[374] NATO, *NATO Industry Cyber Partnership*, https://www.nato.int/cps/en/natohq/news_113121.htm, accessed: 16.02.2025.
[375] European External Action Service, *European Union and NATO Hold First Structured Dialogue on Cyber*, https://www.eeas.europa.eu/eeas/european-union-and-nato-hold-first-structured-dialogue-cyber-0_en, accessed: 16.02.2025.
[376] T. Stevens, J. Burton, *NATO and Strategic Competition in Cyberspace*, NATO Review, https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html, accessed: 16.02.2025.
[377] IEEE, *Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture, NATO Science and Technology Organization IST Panel activity IST-152-RTG, "Intelligent, Autonomous and Trusted Agents for Cyber Defense and Resilience"*, https://ccdcoe.org/library/publications/towards-an-active-autonomous-and-intelligent-cyber-defense-of-military-systems-the-nato-aica-reference-architecture/, accessed: 14.10.2024.
[378] V. Romanenko, Ukraine may establish another branch of the military, https://www.pravda.com.ua/eng/news/2024/10/24/7481146/, accessed: 24.02.2025/
[379] A. Niedermeier, *Same Threat, Different Answers? Comparing and Assessing National Cyber Defence Strategies in Central-Eastern Europe*, Security and Defence Quarterly, 2017, vol. 16, no. 3, pp. 57.
[380] Marios P. Efthymiopoulos, *NATO: Time to Adopt a Pre-emptive Approach to Cyber Security in New Age Security Architecture*, GJIA, 9.03.2024, https://gjia.georgetown.edu/2024/03/09/nato-time-to-adopt-a-pre-emptive-approach-to-cyber-security-in-new-age-security-architecture, accessed: 16.02.2025.

with the private sector), attend to its legal frameworks, and establish a strategic vision for cyber development. All measures are implemented to effectively counter the evolving threats of cyberspace or ICT/IE. The concept of cyber forces is thus integral to the cyber development of NATO members in response to the escalating prevalence of cyber conflicts encountered by numerous nations.

7. Conclusion

Taking into account the simultaneous development of cyber-related capabilities, including the establishment of dedicated cyber forces and/or units, a common ground between nations is emerging. The increased commitment to resource allocation is also part of fulfilling obligations to NATO, wherein the resilience of each member state contributes to the collective strength of the entire Alliance. Based on the conducted research, countries should focus on developing national cyber-related forces while also strengthening their CIMICs. It is therefore critical that cyber-related defence budgets are increased to support, among other things, investment in new technologies, training of cyber personnel, and the development of necessary infrastructure. At the same time, governments should adopt a multi-phased approach, recognising that cyber-related defence is not solely a military responsibility but also an essential, integrated part of national security.

Country	Type and size	Subordination
Albania	Military Cyber Security Unit. Size n/a.	General Staff of the Albanian Armed Forces
Belgium	CDU incorporated into BeCyberCom. Size n/a.	MoD
Bulgaria	The CICDSC. Size n/a.	Chief of the General Staff of the Bulgarian Army
Canada	CAFCYBERCOM. Size n/a.	DND
Croatia	Centre for Communication and Information Support incorporated into Cyber Command. Size n/a.	General Staff of the Croatian Armed Forces
Czech Republic	Cyber and Information Warfare Command. Size n/a.	General Staff of the Czech Armed Forces
Denmark	CFCS. Size n/a.	Danish Defence Intelligence Service
Estonia	Estonian Cyber Command. Size – Approx. 300 personnel.	Estonian Defence Forces
Finland	C5 Agency. Size - approximately 500 employees.	CHOD
France	French CDC (COMCYBER). Size – 3,502 cyber operators (2023)	CHOD Staff
Germany	Cyber and Information Domain Service (CIR). Size - 16,000 military and civilian personnel.	Bundeswehr

Greece	Unit 1864 and CDD. Size n/a.	HNDGS
Hungary	Hungarian Defence Forces Cyber Operations Command and CyOC of the Military National Security Service. Size n/a.	MoD
Iceland	No separate cyber unit. Cooperation with NATO CCDCOE.	Ministry of Foreign Affairs
Italy	The 9th Cyber Security Regiment "Rombo". Size n/a.	Italian Armed Forces
Latvia	National Guard CDU. Size n/a.	MoD
Lithuania	Lithuanian Cyber Command (LTCCYBERCOM). Size n/a.	Lithuanian Armed Forces
Luxembourg	LHC size n/a.	Department of Communication and Information Systems
Montenegro	CIRT, 17 personnel, including one Head of Cybersecurity, one Head of Cyber Operations, 5 Cyber Analysts, and 8 advisers.	MoD
Netherlands	DCC. Size n/a.	CHOD of the Armed Forces
North Macedonia	MIL-CERT size n/a.	MoD
Norway	Cyber Defence Force (Cyberforsvaret). Size: 1,500 military and civilian members.	Norwegian Armed Forces
Poland	Cyber Forces Command. Size approximately 5,000 personnel (military and civilian).	Ministry of National Defence
Portugal	Joint Cyber Defence Operations Command (COCiber). Size n/a.	Armed Forces General Staff
Romania	CDC (CApC). Size n/a.	Ministry of National Defence
Slovakia	Cyber Defence Centre of the Slovak Republic. Size n/a.	MoD of the Slovak Republic
Slovenia	Cybersecurity Department. Size n/a.	Slovenian Armed Forces
Spain	Joint Cyber Command (MCCE). Size - approximately 300 military personnel and 100 civilians.	Minister of Defence
Sweden	Cyber Units, e.g. ITF, 2ITF. Size n/a.	Swedish Armed Forces
Turkey	Cyber Emergency Response Team of Turkish Armed Forces (TAF – CERT);	Ministry of National Defence

	Turkish Armed Forces CDC (TSKSSK). Size n/a.	
United Kingdom	Defence Cyber Operations Group (JFCyQ) incorporated into British Strategic Command (StratCom). Size n/a.	Secretary of State for Defence
United States	US Cyber Command (USCYBERCOM). Over 6,200 personnel (Cyber Mission Force and supporting units).	Department of Defense

TABLE 1. NATO COUNTRIES – MILITARY CYBER UNITS AND COMMAND STRUCTURE.

This report demonstrates that an increasing number of NATO members are enhancing their cyber capabilities, among other initiatives, by establishing specialised cyber forces. Although not every member state has established such units, there is a clear trend toward expansion, especially in the wake of Russia's invasion of Ukraine. The continued strengthening of cyber forces will significantly contribute to their evolution within NATO countries, enhancing their ability to address emerging threats. This, in turn, reinforces cyberspace as a vital domain of modern conflict and cooperation, as challenges in this sphere grow increasingly complex.

Through this analysis of each of the 32 constituent NATO member states, the structure and role of entities responsible for cyber defence, crucial to the development of national cyber forces, have been detailed. The primary emphasis of this comprehensive report has been to identify those allies that have already formed specialised cyber forces and those which are in the process of doing so. The frequency of hostile cyber attacks has escalated in recent years, especially following the Russian invasion of Ukraine. Consequently, an increasing number of NATO member states are forming cyber forces, designing national cyber strategies, or establishing specialised entities aimed at combating cyber threats within the cyber domain—many of which may develop into fully operational cyber forces in the future.

In conclusion, the future of NATO's security lies not only in its tanks, aircraft, and submarines, but increasingly in its firewalls, encryption systems, cyber forces, and even its combined cyber-electromagnetic forces. Building an integrated, resilient, and proactive cyber defence structure must be seen as an urgent strategic imperative for national governments and the Alliance itself. This research indicates that NATO member states are collectively enhancing and integrating their cyber capabilities. In the future, these dedicated forces will be a crucial and fundamental component of NATO's collective security.

8. Abbreviations

AG	Aggression
C&C&InfSh	Cooperation, collaboration and information sharing
C&C	Cooperation and Collaboration
CA	Cyber attack

CCDCOE	Cooperative Centre of Excellence for Cyber Defence
CD	Cyber Defence
CDC	Cyber Defence Centre
CDO	Cyber Defensive Operation
CI	Cyber Incident
CIP	Critical Infrastructure Protection
CIS	Communication and Information System
CIS CIP	Communication and Information System Critical Infrastructure Protection
CO	Cyber Operation
COO	Cyber Offensive Operation
CR	Cyber Resilience
CRI	Critical Infrastructure
CS	Cyber Security
CSP	Cyberspace
DODIN	Department of Defense Information Network
EET	Education, Exercise and Training
ENISA	European Union Agency for Cybersecurity
EU	European Union
HO	Hybrid Operation
HRM	Human Resource Management
IA	Information Assurance
ICRC	International Committee of the Red Cross
IE	Information Environment
IEEE	Institute of Electrical and Electronics Engineers
IHL	International Humanitarian Law
ICT	Information Communication Technology
IO	Information Operation
INFOSEC	Information Security
IS	Information System
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
MoD	Ministry of Defence
NAF	National Armed Forces
NATO	North Atlantic Treaty Organisation
NCF	National Cyber Force
NCIE	National Cyber and Information Security Entity

NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
UN	United Nations

9. List of Figures

10. List of Tables

11. References

- ANSSI. ANSSI publishes the 2023 Cyber Threat Overview, French Cybersecurity Agency, 14 May 2024, https://cyber.gouv.fr/en/actualites/anssi-publishes-2023-cyber-threat-overview, accessed: 17.03.2025.
- Antoniuk, Daryna. Cyberattack disrupts Bulgarian government websites over 'betrayal to Russia', The Record, 18 October 2022, https://therecord.media/cyberattack-disrupts-bulgarian-government-websites-over-betrayal-to-russia, accessed: 17.03.2025.
- Army of the Republic of North Macedonia. History of the Army, https://mil.mk/history/?lang=en#1495112660340-dd2e5790-d213, accessed: 17.03.2025.
- Army of the Republic of North Macedonia. Participation of Army members in the exercise "Cyber Unity 2023.", 20 September 2023, https://mil.mk/general-staff-activities/uchestvo-na-pripadnici-na-armijata-na-vezhbata-cyber-unity-2023/?lang=en, accessed: 17.03.2025.
- Arnaut, José, Luis. and Figueiredo, João, Leitão. Data protection and cybersecurity in Portugal: challenges ahead through 2023, The Legal 500, https://www.inhouselawyer.co.uk/legal-briefing/data-protection-and-cybersecurity-in-portugal-challenges-ahead-through-2023/, accessed: 17.03.2025.
- Asere, Anda. National Guard CDU – the best of the best, Labs of Latvia, 18 July 2024, https://labsoflatvia.com/en/news/national-guard-cyber-defense-unit-the-best-of-the-best, accessed: 17.03.2025.
- Ayliffe, Chris. Safeguarding Iceland's Digital Horizon: The Urgent Call for Proactive Cybersecurity, Nanitor, 25 June 2024, https://nanitor.com/resources/blog/cyber-exposure-alerts/safeguarding-icelands-digital-horizon-the-urgent-call-for-proactive-cybersecurity/, accessed: 17.03.2025.
- Bencsik, András, Karpiuk, Mirosław. The legal status of the cyberarmy in Hungary and Poland. An overview, "Cybersecurity and Law", no. 2, vol. 10.
- Bianchi, Tiago. Distribution of cyber-attacks in Spain in 2023, by type, Statista, 21 March 2024, https://www.statista.com/statistics/1458071/spain-share-cyber-attacks-by-type/ accessed: 17.03.2025.
- Blessing, Jason., Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain, NATO 2030 and Beyond: A Handbook for the Next Generation of Transatlantic Leaders, Johns Hopkins University SAIS, 2021.
- Blessing, Jason. The Global Spread of Cyber Forces, 2000–2018, in 13th International Conference on Cyber Conflict: Going Viral, T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.), NATO CCDCOE Publications, Tallinn, 2021.
- Boeke, Sergei., Veenendaal, Matthijs., Heinl, Caitriona, Civil-Military Relations and International Military Cooperation in Cyber Security, NATO CCDCOE, https://ccdcoe.org/uploads/2018/10/Art-05-Civil-Military-Relations-and-International-Military-Cooperation-in-Cyber-Security.pdf, accessed: 16.02.2025
- Bojarski, Kamil. France and its doctrine of cyber operations - offensive actions, Counterintelligence.co.uk, 8 July 2022, https://counterintelligence.pl/en/2022/08/francja-i-jej-doktryna-operacji-cyber-dzialania-ofensywne/, accessed: 17.03.2025.
- Brno Daily. Czech Republic Spent 1.37% of GDP on Defence in 2023, Says Defence Minister Cernochova, 13 May 2024, https://brnodaily.com/2024/05/13/news/politics/czech-republic-spent-1-37-of-gdp-on-defence-in-2023-says-defence-minister-cernochova/, accessed: 17.03.2025.
- Bundeswehr. Cyber and Information Domain Service, https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service, accessed: 17.03.2025.

- Canadian CFCS. National Cyber Threat Assessment 2023-2024, 2023, accessed: 17.03.2025.
- Canadian CFCS. Russian Military Cyber Actors Target US and Global Critical Infrastructure, https://www.cyber.gc.ca/en/news-events/russian-military-cyber-actors-target-us-global-critical-infrastructure, accessed: 17.03.2025.
- Canadian Global Affairs Institute. Emerging Technology and Five Eyes: Implications for Canadian Defence, https://www.cgai.ca/emerging_technology_and_five_eyes_implications_for_canadian_defence, accessed: 17.03.2025.
- Cedeira, Brais. El jefe de ciberseguridad del CNI: "El 45% de ataques graves a España este año viene de Rusia", El Español, 20 May 2023, https://www.elespanol.com/espana/20230520/ciberseguridad-cni-ataques-graves-espana-viene-rusia/764423880_0.html accessed: 17.03.2025.
- CFCS. The Cyber Threat Against Denmark 2024, 20 September 2024.
- Centre for Cybersecurity Belgium. Organisation, 2024, https://ccb.belgium.be/en/organisation?utm_source, accessed: 17.03.2025.
- Centre for Cybersecurity Belgium. Protect, Strengthen, Prepare, 2024, https://ccb.belgium.be/en/protect-strenghten-prepare?utm_source, accessed: 17.03.2025.
- CFCS, Danish Ministry of Defence. CFCS, 3 November 2022, https://www.fmn.dk/en/topics/cyber-security/centre-for-cyber-security/, accessed: 17.03.2025.
- Centro Criptológico Nacional. "CCN-CERT IA-04/24: Ciberamenazas y Tendencias. Edición 2024", October 2024, https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html accessed: 17.03.2025.
- Centro Criptológico Nacional. 'CCN functions', https://www.ccn.cni.es/en/menu-ccn-en/functions-of-the-ccn accessed: 17.03.2025.
- Centro Nacional de Cibersegurança. National Strategy for Cyberspace Security 2019–2023, June 2019, https://cncs.gov.pt/docs/portugal-ncss-2019-2023-en-2.pdf, accessed: 17.03.2025.
- Centro Nacional de Cibersegurança. NCC-PT - Centro Nacional de Coordenação, https://www.cncs.gov.pt/en/ncc-pt-centro-nacional-de-coordenacao/, accessed: 17.03.2025.
- CERTCOOP. Initiatives to improve Cyber Defence capabilities – development of NATO cyber forces – The CDD. https://www.certcoop.gr/index.php/hcdd/, accessed: 17.03.2025.
- CIMIC Centre of Excellence, Resilience in the Cyber Domain, https://www.cimic-coe.org/ccoe_events/seminars/10-Feb-2022/, accessed: 16.02.2025.
- Clausnitzer, J. Number of malware incidents in Finland Q3 2019–Q3 2023, Statista, 30 November 2023, https://www.statista.com/statistics/733010/number-of-malware-incidents-per-quarter-in-finland/, accessed: 17.03.2025.
- Colatin, Samuele. De Tomas. National Cybersecurity Organisation: ITALY, NATO CCDCOE, Tallinn, 2020.
- Comando de Operações de Ciberdefesa - COCiber. República Portuguesa Defesa Nacional, 2024, https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro/Paginas/default.aspx, accessed: 17.03.2025.
- Commisions des affaires etrangeres et de la Défense. Pour une coordination de la cyberdéfense plus offensive dans la loi de programmation militaire 2024–2030, 24 May 2023.
- Couillard, Jeffrey. Beyond USCYBERCOM: The Need to Establish a Dedicated US Cyber Military Force, Cyber Defense Review, Spring 2024,

https://cyberdefensereview.army.mil/Portals/6/Documents/2024_Spring/Couillard_CDRV9N1-Spring-2024.pdf accessed: 16.02.2025.

- Council of Europe. Turkey, https://www.coe.int/en/web/octopus/-/turkey accessed: 17.03.2025.
- CSIS, Significant Cyber Incidents, Significant Cyber Incidents Since 2006 (2006-2025), https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents, accessed: 18.02.2025.
- CSIRT.MIL.SK. Cyber Defence Centre of the Slovak Republic, https://ckosr.sk/75688/?mne=3149, accessed: 17.03.2025.
- CyberDefence24. Polska i Słowenia będą współpracować w zakresie cyberbezpieczeństwa i AI, 2024, https://cyberdefence24.pl/technologie/polska-i-slowenia-beda-wspolpracowac-w-zakresie-cyberbezpieczenstwa-i-ai accessed: 17.03.2025.
- Cyber Commande la Défense. La Défense.be, 2024, https://www.mil.be/fr/a-propos-de-la-defense/cyber-command/, accessed: 17.03.2025.
- Cyber Defence Centre of the Slovak Republic. Cyber Defence https://ckosr.sk/75689/?mne=3146, accessed: 17.03.2025.
- Cyber Forces Command. Ministry of Defence & Armed Forces, 25 October 2024, https://www.mo.gov.cz/en/armed-forces/organisational-structure/cyb/cyber-forces-command-218593/, accessed: 17.03.2025.
- Cyberlands.IO. Top 10 Cybersecurity Breaches in Norway, https://www.cyberlands.io/topsecuritybreachesnorway, accessed: 17.03.2025.
- Cyber.Mil.PL. Cyber Defence Forces, https://www.cyber.mil.pl/wojska-obrony-cyberprzestrzeni/, accessed: 17.03.2025.
- Cyber Security. Danish Ministry of Defence, 3 November 2022, https://www.fmn.dk/en/topics/cyber-security/cyber-security/, accessed: 17.03.2025.
- Cyber Security. Security and Intelligence Agency of the Republic of Croatia, https://www.soa.hr/en/areas-of-activity/cyber-security/, accessed: 17.03.2025.
- Cybersecurity and Infrastructure Security Agency. #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities, February 09, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a accessed: 05.02.2025.
- Cybersecurity and Infrastructure Security Agency. IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities, December 18, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a accessed: 05.02.2025.
- Cybersecurity and Infrastructure Security Agency. North Korea State-Sponsored Cyber Threat: Advisories, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/north-korea/publications accessed: 05.02.2025.
- Cybersecurity and Infrastructure Security Agency. People's Republic of China Cyber Threat, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china accessed: 05.02.2025.
- Cybersecurity and Infrastructure Security Agency. SVR Cyber Actors Adapt Tactics for Initial Cloud Access, February 26, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a accessed: 05.02.2025.
- Cybersecurity in the UK. House of Commons, 19 April 2024.
- Cyberwiser.eu. Iceland, https://cyberwiser.eu/iceland, accessed: 17.03.2025.

- Daily Sabah. Türkiye becomes world's most cyber-targeted region in 2023, 7 December 2023, https://www.dailysabah.com/turkiye/turkiye-becomes-worlds-most-cyber-targeted-region-in-2023/news accessed: 17.03.2025.
- Danish Ministry of Defence. The Danish National Strategy for Cyber and Information Security, 3 November 2022, https://www.fmn.dk/en/topics/cyber-security/danish-national-strategy/, accessed: 17.03.2025.
- Danish Ministry of Defence. Will and Ability to take responsibility. Danish Defence and Security 2024-2033, 28 June 2023.
- Data Guidance. Croatia: ZSIS adopts action plan to implement National Cyber Security Strategy, https://www.dataguidance.com/news/croatia-zsis-adopts-action-plan-implement-national, accessed: 17.03.2025.
- Dewar, Robert S. National Cybersecurity and Cyberdefence Policy Snapshots, Centre for Security Studies, September 2018.
- Diário da República. Decreto Regulamentar n.º 214/2023, 17 July 2023, https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-regulamentar/2023-214064876, accessed: 17.03.2025.
- Dzakula, Branko., Mihailovic, Andreja., Zaric, Nikola. Current Cybersecurity Capacities and Digital Rights in Montenegro, 2021.
- E-Estonia. A year of advanced threats and global tensions: Estonia's cybersecurity scene in 2023, 9 April 2024, https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats/, accessed: 17.03.2025.
- Efthymiopoulos, Marios P., NATO: Time to Adopt a Pre-emptive Approach to Cyber Security in New Age Security Architecture, GJIA, 9.03.2024, https://gjia.georgetown.edu/2024/03/09/nato-time-to-adopt-a-pre-emptive-approach-to-cyber-security-in-new-age-security-architecture, accessed: 16.02.2025.
- Eitan, Ofir. Turkey-Challenges to the Struggle against Cyber Threats, Cyber, Intelligence and Security, vol. 2, no. 1, May 2018.
- Enota za komunikacijske in informacijske sisteme (EKIS). GOV.SI, accessed: 17.03.2025.
- ENR. Europe in brief: Slovenia sees rise in cyberattacks, 30 June 2023, https://europeannewsroom.com/europe-in-brief-slovenia-sees-rise-in-cyber-attacks/, accessed: 17.03.2025.
- État-major des armées. #NotreDéfense : Le COMCYBER, une unité opérationnelle en charge de la manœuvre cyber globale, 17 March 2021, https://www.defense.gouv.fr/ema/actualites/notredefense-comcyber-unite-operationnelle-charge-manoeuvre-cyber-globale, accessed: 17.03.2025.
- European Commission. Slovenia - 2024 Digital Decade Country Report, accessed: 17.03.2025.
- European External Action Service, European Union and NATO Hold First Structured Dialogue on Cyber, https://www.eeas.europa.eu/eeas/european-union-and-nato-hold-first-structured-dialogue-cyber-0_en, accessed: 16.02.2025.
- European External Action Service (EEAS). Montenegro Report 2024, 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/Montenegro%20Report%202024.pdf, accessed: 17.03.2025.
- Evsyukova, Oksana., Karpiuk, Mirosław., Kelemen, Miroslav. Cyberthreats in Ukraine, Poland and Slovakia, Cybersecurity and Law, no. 1, vol. 11, 2024.

- Fakti.bg. Angel Naydenov Recalled That the Bulgarian Soldier Is Poor and Homeless, 12 April 2024, https://fakti.bg/en/bulgaria/872598-angel-naydenov-recalled-that-the-bulgarian-soldier-is-poor-and-homeless, accessed: 17.03.2025.
- Federal Office for Information Security. The State of IT Security in Germany, 2 November 2023, https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html, accessed: 17.03.2025.
- Finnish Defence Forces. Finnish Defence Forces C5 Agency, https://puolustusvoimat.fi/en/about-us/c5-agency, accessed: 17.03.2025.
- French Embassy in Montenegro. CyberCenter, https://me.ambafrance.org/-CyberCenter, accessed: 17.03.2025.
- Gallery: Eesti küberväejuhatus asus tööle. ERR, 1 August 2018, https://www.err.ee/850643/galerii-eesti-kubervaejuhatus-asus-toole, accessed: 17.03.2025.
- Gibadło, Lidia, Gotkowska, Justyna. Nowy plan restrukturyzacji Bundeswehry, Ośrodek Studiów Wschodnich, 11 April 2024, https://www.osw.waw.pl/pl/publikacje/analizy/2024-04-11/nowy-plan-restrukturyzacji-bundeswehry, accessed: 17.03.2025.
- Government of Canada. Canadian Armed Forces establishes a new Cyber Command, 26 September 2024, https://www.canada.ca/en/department-national-defence/news/2024/09/canadian-armed-forces-establishes-a-new-cyber-command.html, accessed: 17.03.2025.
- Government of Canada. Communications Security Establishment Act, https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html, accessed: 17.03.2025.
- Government Cyber Security Strategy. Building a cyber resilient public sector, Cabinet Office, 2022.
- Government of Iceland, Icelandic National Cybersecurity Strategy 2022-2027, February 2022.
- Government of the Republic of Slovenia. Cyber Security Strategy of the Republic of Slovenia, 2016, https://www.gov.si/assets/ministrstva/MDP/DID/Cyber_Security_Strategy_Slovenia.pdf, accessed: 17.03.2025.
- Gregory, Jennifer. Poland spending $760 million on cybersecurity after attack, Security Intelligence, https://www.ibm.com/think/news/poland-cybersecurity-spending-increases, accessed: 17.03.2025.
- Hadrian. Statistics Netherlands releases Cyber Security Monitor 2022, 2023, https://hadrian.io/blog/statistics-netherlands-releases-cyber-security-monitor-2022, accessed: 17.03.2025.
- Halisdemir, Emre. National Cybersecurity Organisation: Turkey, NATO CCDCOE, Tallinn, 2021.
- Hałys, Piotr., Cyberspace as a Domain of Operational Activities and the Resulting Challenge, Faculty of Mechanical Engineering, Wrocław University of Science and Technology, 2021, Volume 53, Number 2(200).
- Himka, Sophie. Analyzing Finland's and NATO's Cybersecurity Strategies, The Henry M. Jackson School of International Studies, 20 October 2023, https://jsis.washington.edu/news/analyzing-finlands-and-natos-cybersecurity-strategies/, accessed: 17.03.2025.
- Hungary Today, New Military Cyberspace Command Inaugurated, 3 October 2023, https://hungarytoday.hu/new-military-cyberspace-command-inaugurated/, accessed: 17.03.2025.
- Hurt, Martin and Sõmer, Tiia. Cyber Conscription Experience and Best Practice from Selected Countries, International Centre for Defence and Security, February 2021.

• Iceland Monitor. Iceland among the best countries in the field of cyber security, 15 September 2024, https://icelandmonitor.mbl.is/news/news/2024/09/15/iceland_among_the_best_countries_in_the_field_of_cy/, accessed: 17.03.2025.

• IEEE, Towards an active, autonomous and intelligent cyber defence of military systems: The NATO AICA reference architecture, NATO Science and Technology Organisation IST Panel activity IST-152-RTG, "Intelligent, Autonomous and Trusted Agents for Cyber Defense and Resilience", https://ccdcoe.org/library/publications/towards-an-active-autonomous-and-intelligent-cyber-defense-of-military-systems-the-nato-aica-reference-architecture/, accessed: 14.10.2024.

• IFEMA Madrid. 68% of Spanish companies have no defence against cyber-attacks, 2024, https://www.ifema.es/en/sicur/news/defense-against-cyberattacks accessed: 17.03.2025.

• INCIBE. What is INCIBE, Instituto Nacional de Ciberseguridad (INCIBE), https://www.incibe.es/en/incibe/corporate-information/what-is-incibe accessed: 17.03.2025.

• Information and Communication Technology Centre. Cyber Command: Republic of Estonia Defence Forces, https://mil.ee/en/landforces/cyber-command/information-and-communication-technology-centre/, accessed: 17.03.2025.

• Initiatives to improve Cyber Defence capabilities - development of NATO cyber forces – Slovenia. Accessed: 17.03.2025.

• Initiatives to improve Cyber Defence capabilities - development of NATO cyber forces - Spain. Accessed: 17.03.2025.

• Instytut Kościuszko. Poland ranks 6th in the global cybersecurity ranking, 2 February 2024, https://ik.org.pl/en/2024/02/02/cyber-coalition-key-role-of-poland-in-nato-cyber-warfare-exercises/, accessed: 17.03.2025.

• IntelliNews. North Macedonia Steps Up Security After Cyberattacks and Bomb Hoaxes Linked to Ukraine War, 22 February 2023, https://www.intellinews.com/north-macedonia-steps-up-security-after-cyber-attacks-and-bomb-hoaxes-linked-to-ukraine-war-270736/, accessed: 17.03.2025.

• International Press Institute. Hungary: DDoS cyberattacks pose major new threat to media freedom, 29 August 2023, https://ipi.media/hungary-ddos-cyber-attacks-pose-major-new-threat-to-media-freedom/, accessed: 17.03.2025.

• International Trade Administration. Bulgaria - Country Commercial Guide. Safety and Security, 01 February 2024, https://www.trade.gov/country-commercial-guides/bulgaria-safety-and-security, accessed: 17.03.2025.

• Istituto Superiore di Stato Maggiore Interforze 25° Corso – 3a Sezione – 9° Gruppo di Lavoro. Il Dominio cyber: il quadro normativo nazionale ed internazionale per la conduzione di operazioni cibernetiche, tra limiti di sviluppo e impiego dell'arma cibernetică, 2024, https://www.difesa.it/assets/allegati/46666/9_gdl_25_issmi_-as_smd_05-_as_sdm_16.pdf, accessed: 17.03.2025.

• Ivanovic, Ivan. Montenegro's Proposed New Cybersecurity Structure Raises Concerns, Balkan Insight, 2 October 2024, https://balkaninsight.com/2024/10/02/montenegros-proposed-new-cybersecurity-structure-raises-concerns/, accessed: 17.03.2025.

• Janofsky, Adam. Cyber Command deployed 'hunt forward' defenders to Croatia to help secure systems, The Record, 18 August 2022, https://therecord.media/cyber-command-deployed-hunt-forward-defenders-to-croatia-to-help-secure-systems, accessed: 17.03.2025.

• Kaczmarek, Krzysztof. Finland in the light of cyber threats in the context of Russia's aggression against Ukraine, "Cybersecurity and Law", vol. 9, no.1, War Studies University.

- Kaczmarek, Krzysztof. Nordic Countries in the Face of Digital Threats, Cybersecurity and Law, 2024
- Kadyrzhanova, Aidą. Croatia struggles with surge in cyberattacks, Bne Intelli News, 1 July 2024, https://www.intellinews.com/croatia-struggles-with-surge-in-cyber-attacks-331784/, accessed: 17.03.2025.
- Kaska, Kaska. National Cybersecurity Organisation: Romania, NATO CCDCOE, Tallinn, 2020
- Kirby, Paul. Sweden blames Iran for cyber-attack after Quran burnings, BBC, 24 September 2024, https://www.bbc.com/news/articles/c0lw0081e1yo accessed: 17.03.2025.
- Kobzová, Lucia. Russian hackers have attacked several EU countries. Slovakia was also a victim, Adapt Institute, 1 July 2024, https://www.adaptinstitute.org/russian-hackers-have-attacked-several-eu-countries-slovakia-was-also-a-victim/01/07/2024/, accessed: 17.03.2025.
- Kozłowski, Andrzej., NATO in Cyberspace After Madrid Summit, Pulaski Commentary, https://pulaski.pl/en/pulaski-commentary-nato-in-cyberspace-after-madrid-summit-andrzej-kozlowski/, accessed: 16.02.2025.
- Kozłowski, Andrzej. Polish 'cyberclaws'. Building of the cyberarmy of the rising military power in Europe, Casimir Pulaski Foundation, 26 June 2023, https://pulaski.pl/en/polish-cyberclaws-building-of-the-cyberarmy-of-the-rising-military-power-in-europe/, accessed: 17.03.2025.
- Kovacs, Laszlo and Szentgali, Gergely. National Cyber Security Organisation: Hungary, NATO CCDCOE, Tallinn, 2015.
- Król, Paweł. Czarnogóra oskarża Rosję o cyberatak, Kresy.pl, 4 September 2022, https://kresy.pl/wydarzenia/czarnogora-oskarza-rosje-o-cyberatak, accessed: 17.03.2025.
- Kybermittari. TRAFICOM, https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter, accessed: 17.03.2025.
- L'Armée luxembourgeoise. Service de cyberdéfense, 21 February 2024, https://armee.public.lu/fr/missions/service-cyberdefense.html, accessed: 17.03.2025.
- Latvijas Republikas Saeima. New law significantly strengthens cybersecurity in Latvia, 20 June 2024, https://www.saeima.lv/en/news/saeima-news/33693-new-law-significantly-strengthens-cybersecurity-in-latvia, accessed: 17.03.2025.
- Lekidis, Alexios. Cyber-attack TTP analysis for EPES systems, arXiv, 17 February 2023, https://doi.org/10.48550/arXiv.2302.09164, accessed: 17.03.2025.
- Lemos, Robert. Nigeria & Romania Ranked Among Top Cybercrime Havens, Dark Reading, 18 April 2024, https://www.darkreading.com/cybersecurity-analytics/nigeria-romania-ranked-among-top-cybercrime-havens, accessed: 17.03.2025.
- Lifländer, Christian-Marc, NATO's Cyber Resilience: Proactive Defence Strategies, The Record, February 2025, https://therecord.media/nato-resilience-cyberdefense-liflander-cycon, accessed: 15.02.2025.
- Liszkowska, Dominika. Turkey's Cybersecurity Policy Framework, Cybersecurity and Law, no. 11, vol. 1.
- LSM. CERT: Latvia sees highest level of cyberattacks in two years, 15 October 2024, https://eng.lsm.lv/article/society/crime/15.10.2024-cert-latvia-sees-highest-level-of-cyberattacks-in-two-years.a572581/, accessed: 17.03.2025.
- Machiels, Maaike., Active Cyber Defence and NATO: NATO's Innovative Offensive Strategy Towards Russia and China, The Atlantic Forum, https://www.atlantic-forum.com/atlantica/active-cyber-defence-and-nato-natos-innovative-offensive-strategy-towards-russia-and-china, accessed: 16.02.2025.

- Magrani, Eduardo. Cybersecurity in Portugal: Trends and Compliance, CCA, 30 October 2023, https://www.cca.law/en/insights-and-media/newsletters/Cybersecurity-in-Portugal-Trends-and-Compliance/9147/, accessed: 17.03.2025.
- Makowiec, Paweł. Tysiące zagrożeń, gigantyczne wzrosty? Tezy kontra statystyki CERT Polska, Cyberdefence24, https://cyberdefence24.pl/cyberbezpieczenstwo/tysiace-zagrozen-gigantyczne-wzrosty-tezy-kontra-statystyki-cert-polska, accessed: 17.03.2025.
- Marrone, Alessandro., Sabatino, Ester., Cyber Defence in NATO Countries: Comparing Models, Istituto Affari Internazionali (IAI), February 2021.
- Marrone, Alessandro, Sabatino, Ester, Credi, Ottavia. Italy and Cyber Defence, IAI, September 2021, https://www.iai.it/sites/default/files/iai2112_en.pdf, accessed: 17.03.2025.
- Mattelaer, Alexander. Belgian Cyber Command and Legal Framework, Egmont Policy Brief 295, Egmont Institute, November 2022, https://www.egmontinstitute.be/app/uploads/2022/11/PB-295-Alexander-Mattelaer_Cyber-Command.pdf, accessed: 17.03.2025.
- Matishak, Martin. NATO members commit to creating new cyber centre in Belgium, The Record, 11 July 2024, https://therecord.media/nato-cyberdefense-center-belgium-announcement, accessed: 17.03.2025.
- Mazepa, Diana. Narodowa Strategia Bezpieczeństwa Cybernetycznego Republiki Macedonii Północnej i Plan Działania 2018-2022, Wschodnioznawstwo, vol. 13, 2019, pp. 77–90, https://ejournals.eu/czasopismo/wschodnioznawstwo/artykul/narodowa-strategia-bezpieczenstwa-cybernetycznego-republiki-macedonii-polnocnej-i-plan-dzialania-2018-2022, accessed: 17.03.2025.
- Ministere des Armées. Brigade d'Appui Numérique et du Cyber (BANC), https://www.defense.gouv.fr/terre/unites-larmee-terre/nos-brigades/brigade-dappui-numerique-du-cyber-banc, accessed: 17.03.2025.
- Ministerio de Defensa de España. Mando Conjunto del Ciberespacio (MCCE), https://emad.defensa.gob.es/unidades/mcce/ accessed: 17.03.2025.
- Ministry of Defence. Podstawowe informacje o budżecie resortu obrony narodowej na 2024 r., March 2024.
- Ministry of Defence. Wojska Obrony Cyberprzestrzeni, https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni, accessed: 17.03.2025.
- Ministry of Defence of the Republic of Bulgaria. Communications and Information Support and Cyber Defence Command, https://www.mod.bg/en/ba.html, accessed: 17.03.2025.
- Ministry of Defence of the Republic of Bulgaria. Programme for the development of the defence capabilities of the Bulgarian Armed Forces 2032.
- Ministry of Defence of the Republic of Croatia. Initiatives to improve Cyber Defence capabilities - development of NATO cyber forces – Croatia.
- Ministry of Defence, Republic of Latvia. Cybersecurity, 2024, https://www.mod.gov.lv/en/cybersecurity, accessed: 17.03.2025.
- Ministry of Defence, Republic of Latvia. Ministry of Defence launches Military Computer Emergency Readiness Team, 28 November 2018, https://www.mod.gov.lv/en/news/ministry-defence-launches-military-computer-emergency-readiness-team, accessed: 17.03.2025.
- Ministry of National Defence of Portugal. EMGFA, https://www.defesa.gov.pt/pt/defesa/organizacao/forcasarmadas/emgfa, accessed: 17.03.2025.
- Ministry of National Defence, Republic of Lithuania. Budget Statement, 5 July 2024, https://kam.lt/en/facts-and-trends/budget-statement/, accessed: 17.03.2025.

- Ministry of National Defence, Republic of Lithuania. Lithuanian Cyber Defence Command opened, 3 January 2025, https://kam.lt/en/lithuanian-cyber-defence-command-opened/, accessed: 17.03.2025.
- Ministry of National Defence, Republic of Lithuania. Overview of the cybersecurity status in Lithuania: key information 2023,
- Ministry of National Defence, Republic of Lithuania. The Ministry of National Defence is establishing Lithuanian Armed Forces Cyber Defence Command. 9 April 2024, https://kam.lt/en/the-ministry-of-national-defence-is-establishing-lithuanian-armed-forces-cyber-defence-command/, accessed: 17.03.2025.
- Ministerul Apărării Naționale. Cyber Command https://cybercommand.ro/webroot/en/pages/structure, accessed: 17.03.2025.
- Ministry of Transport and Infrastructure of the Republic of Turkey. National Cyber Security Strategy and Action Plan (2024-2028), https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2024-2028.pdf accessed: 17.03.2025.
- MLT Aikins. Pro-Russian Hackers Ramp Up Attacks on Canadian Infrastructure, https://www.mltaikins.com/insights/pro-russian-hackers-ramp-up-attacks-on-canadian-infrastructure, accessed: 17.03.2025.
- MSSPAlert, Escalating Cyber Threats Faced by NATO Countries, https://www.msspalert.com/brief/escalating-cyber-threats-faced-by-nato-countries, accessed: 18.02.2025.
- National Cyber Security Strategy. Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx, p.5, accessed: 17.03.2025.
- National Cyber and Information Security Agency. 2023 Report on the State of Cybersecurity in the Czech Republic, 11 September 2024.
- National Cyber and Information Security Agency. National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025, 18 March 2021.
- National Cybersecurity Strategy 2020–2025. National Cybersecurity Authority
- National Security Strategy of the Republic of Croatia, The Republic of Croatia, 2017.
- NATO, Industry Cyber Partnership, https://www.nato.int/cps/en/natohq/news_113121.htm, accessed: 16.02.2025.
- NATO. NATO and EU Meet to Enhance Cooperation on Cyber Defence, 8 March 2023, https://www.nato.int/cps/en/natohq/news_212621.htm, accessed: 17.03.2025.
- NATO. NATO and North Macedonia strengthen responses to cyber threats, 19 February 2021, https://www.nato.int/cps/en/natohq/news_181656.htm, accessed: 17.03.2025.
- NATO, Resilience – A Core Element of NATO's Deterrence and Defence, https://www.nato.int/cps/uk/natohq/topics_132722.htm, accessed: 16.02.2025.
- NATO, Statement by the North Atlantic Council on recent Russian hybrid activities, http://nato.int/cps/en/natohq/official_texts_225230.htm?selectedLocale=en7, accessed: 16.02.2025.
- NATO ACT, Cyber Coalition: NATO's Flagship Cyber Exercise, https://www.act.nato.int/activities/cyber-coalition, accessed: 14.02.2025.

• NATO CCDCOE, NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit, accessed: 14.02.2025.

• NATO JFCBS. Cyber Coalition 2024 – Strengthening NATO Cyber Defence, https://jfcbs.nato.int/page5964943/2024/cyber-coalition-2024--strengthening-natocyber-defence accessed: 16.02.2025.

• NCSI. Montenegro, 2024, https://ncsi.ega.ee/country/me/, accessed: 17.03.2025.

• NCSI. Netherlands, 30 April 2024, https://ncsi.ega.ee/country/nl/, accessed: 17.03.2025.

• Niedermeier, Alexander., Same Threat, Different Answers? Comparing and Assessing National Cyber Defence Strategies in Central-Eastern Europe, Security and Defence Quarterly, 2017, vol. 16, no. 3.

• Norwegian Armed Forces, The Norwegian Cyber Defence, https://www.forsvaret.no/en/organisation/norwegian-cyber-defence, accessed: 17.03.2025.

• Norwegian Ministry of Defence. Norwegian Defence 2013: Facts and Figures, 2013

• Official Gazette of the Republic of Slovenia [Uradni list RS]. Nos. 30/18 and 95/21; Nos. 29/18 and 131/20, https://pisrs.si/pregledPredpisa?id=ZAKO7707 accessed: 17.03.2025.

• Olech Aleksander, Zagraniczna aktywność militarna Republiki Francuskiej, Poznań, Wydawnictwo Kontekst, 2022.

• Olech Aleksander, Izrael-Palestyna. Rywalizacja w cyberprzestrzeni zaognia się, https://cyberdefence24.pl/cyberbezpieczenstwo/izrael-palestyna-rywalizacja-w-cyberprzestrzeni-zaognia-sie, accessed: 17.03.2025.

• Olejnik, Lukasz. French doctrine of information operations – engaging over information space, https://blog.lukaszolejnik.com/french-doctrine-of-information-operations-engaging-over-information-space/?fbclid=IwAR3QJwPjd8MJCDLij3CFlBlaYBGRwa-PREuv3E00fBeWYc9Zvh_PDJxRH7I, accessed: 17.03.2025.

• Petcu, Ioana and Barbu, , Dragoş-Cătălin. The New Challenges of Romania's Cyber Security Policy, Romanian Cyber Security Journal, May 2022.

• Petrosyan, Ani. Total number of cyberattacks in Iceland from 2020 to 2023, Statista, 18 June 2024, https://www.statista.com/statistics/1473652/denmark-cyberattacks-number/, accessed: 17.03.2025.

• Pomerleau, Mark. House lawmakers receive first briefing on Cybercom 2.0 model: Members heard from top DOD officials on the plan to mature US Cyber Command, DefenseScoop, https://defensescoop.com/2025/02/12/cybercom-2-0-model-house-lawmakers-receive-first-briefing accessed: 23.02.2025.

• Popov, Cristina. Catalonia is the most cyber-attacked region in Spain, Bitdefender, 12 October 2023, https://www.bitdefender.com/en-us/blog/hotforsecurity/catalonia-is-the-most-cyber-attacked-region-in-spain/ accessed: 17.03.2025.

• Port Technology. Cyberattacks Hit Canada: Websites Down for Three Major Ports, https://www.porttechnology.org/news/cyber-attacks-hit-canada-websites-down-for-three-major-ports/, accessed: 17.03.2025.

• Prime Minister's Office, Helsinki. Finland's Cyber Security Strategy 2024-2035, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf, accessed: 17.03.2025.

- Psychogiou, Vasiliki. Cyberspace: Is NATO Doing Enough?, https://finabel.org/wp-content/uploads/2023/01/Cyberspace_Is-NATO-doing-enough-_-Vasiliki-Psychogiou_DAN.pdf accessed: 16.02.2025.
- Radio Free Europe. Spain Detains 3 Over Cyberattacks On Pro-Ukrainian Nations, 20 July 2024, https://www.rferl.org/a/cybercrime-nato-russia-spain-ukraine/33044049.html accessed: 17.03.2025.
- Reddick, James. Chinese state-backed hackers breached 20 Canadian government networks over four years, agency warns, The Record, https://therecord.media/canada-20-government-agencies-hacked-china-last-four-years, accessed: 17.03.2025.
- Report Difesa. Difesa: la Joint Stars 25 si terrà in Sardegna nel mese di aprile, sotto la guida del Comando Operativo di Vertice Interforze. Schierati numerosi assetti delle Forze Armate, Corpi Armati dello Stato e altri Dicasteri e Agenzie, 23 January 2025, https://www.reportdifesa.it/difesa-la-joint-stars-25-si-terra-in-sardegna-nel-mese-di-aprile-sotto-la-guida-del-comando-operativo-di-vertice-interforze-schierati-numerosi-assetti-delle-forze-armate-corpi-armati-dello-stato-e/, accessed: 17.03.2025.
- Republic of Bulgaria Council of Ministers. National plan for increasing the defence spending to 2% of the gross domestic product until 2024,
- Republic of Estonia Defence Forces. Cyber Command, https://mil.ee/en/landforces/cyber-command/, accessed: 17.03.2025
- Republic of Macedonia National Cyber Strategy 2018–2022, Republic of Macedonia, July 2018, https://eucyberdirect.eu/atlas/sources/republic-of-macedonia-national-cyber-strategy-2018-2022, accessed: 17.03.2025.
- Reuters. Denmark raises threat level for destructive cyberattacks to 3 on 5-level scale, 4 June 2024, https://www.reuters.com/technology/cybersecurity/denmark-raises-threat-level-destructive-cyber-attacks-3-5-level-scale-2024-06-04/, accessed: 17.03.2025.
- Reuters. Norway government ministries hit by cyberattack, 24 July 2023, https://www.reuters.com/technology/norway-government-ministries-hit-by-cyber-attack-2023-07-24/, accessed: 17.03.2025.
- Ria Estonia. Cyber Security in Estonia 2020, 10 May 2020, https://ria.ee/en/news/cyber-security-estonia-2020#The-Estonian-Defence-Forces-Cyber-Command, accessed: 17.03.2025.
- Rojoef, Manuel. Canada Debuts New Armed Forces Cyber Command, The Defence Post, 30 September 2024, https://thedefensepost.com/2024/09/30/canada-debuts-armed-forces-cyber-command/, accessed: 17.03.2025.
- Romanenko, Valentyna., Ukraine may establish another branch of the military, https://www.pravda.com.ua/eng/news/2024/10/24/7481146/, accessed: 24.02.2025.
- Royal Danish Defence College. Joint Doctrine for Military Cyberspace Operations, September 2019.
- Rudolph, Alexander. Canada's Active Cyber Defence is Anything But Active, Canadian Global Affairs Institute, July 2021, https://www.cgai.ca/canadas_active_cyber_defence_is_anything_but_active#Canadian, accessed: 17.03.2025.
- Štrucl, Damjan. National Cybersecurity Organisation: Slovenia, NATO CCDCOE, Tallinn, 2021.
- Sas, Adriana. Number of cybersecurity incidents handled by CERT in Poland from 1996 to 2023, Statista, 22 May 2024, https://www.statista.com/statistics/1028557/poland-cybersecurity-incidents/, accessed: 17.03.2025.

• Sengputa, Kim. UK is nearly ready to launch a force to hit hostile countries with cyberattacks, 10 January 2020, https://www.independent.co.uk/news/uk/home-news/cyber-warfare-security-force-iran-crisis-ministry-of-defence-a9278591.html accessed: 17.03.2025.

• Shepard. Sweden steps up cyber efforts, 19 January 2022, https://www.shephardmedia.com/news/digital-battlespace/sweden-steps-up-cyber-efforts/ accessed: 17.03.2025.

• Sigholm, Johan., Magnússon, Bjarni., Skjöld, Magnús., Gislason, Theodor., Falco, Gregory. The Case for an Icelandic Cyber Exploitation and Defence (ICED) Force for NATO Coalition Operations, 2024, 23rd Workshop on the Economics of Information Security.

• Smeets, Max. The challenges of military adaptation to the cyberdomain: a case study of the Netherlands, Small Wars & Insurgencies, 2023, vol. 34, no. 7.

• Space Watch. Turkey Establishing a 'Cyber Army' To Counter National Cyber Threats, 13 June 2017, https://spacewatch.global/2017/06/turkey-establishing-cyber-army-counter-national-cyber-threats/ accessed: 17.03.2025.

• Spaulding, Suzanne., Montgomery, Mark., NATO and Cyber: Outrunning the Bear, CSIS, 24.07.2024, https://www.csis.org/analysis/nato-and-cyber-outrunning-bear, accessed: 14.02.2025.

• STARPlan. 2022 Security & Service, Technology, Ambition, Resilience, La Défense.be, 2022

• Statista. Cybersecurity – Portugal, https://www.statista.com/outlook/tmo/cybersecurity/portugal, accessed: 17.03.2025.

• Statistics Canada. Impact of cybercrime on Canadian businesses, 2023, https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm, accessed: 17.03.2025.

• Stamatouku, Eleni. Greece Moves to Enhance Cyber Security Amid Frequent Attacks, Balkan Insight, 11 December 2023, https://balkaninsight.com/2023/12/11/greece-moves-to-enhance-cyber-security-amid-frequent-attacks/, accessed: 17.03.2025.

• Stevens, Tim., Burton, Joe., NATO and Strategic Competition in Cyberspace, NATO Review, https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html, accessed: 16.02.2025.

• Stevensson, Alex. Luxembourg businesses facing ever more cyberattacks, Luxembourg Times, 21 October 2024, https://www.luxtimes.lu/businessandfinance/luxembourg-businesses-facing-ever-more-cyberattacks/23606264.html, accessed: 17.03.2025.

• Surfshark. Most cyber incidents in France have unidentified origins, 3 September 2024, https://surfshark.com/research/chart/cyber-attacks-france, accessed: 17.03.2025.

• Törn, Maria. Försvarsmakten har fått ett nytt förband, Försvarsmakten, 28 January 2016, https://www.forsvarsmakten.se/sv/aktuellt/2016/01/forsvarsmakten-har-fatt-ett-nytt-forband/ accessed: 17.03.2025.

• The Cybersecurity Strategy of Latvia 2023–2026.

• The Brussels Times Newsroom. Belgian military's Cyber Command to be operational in 2024, The Brussels Times, 12 October 2024, https://www.brusselstimes.com/310607/belgian-militarys-cyber-command-to-be-operational-in-2024?utm_source, accessed: 17.03.2025.

• The International Institute for Strategic Studies. Cyber Capabilities And National Power Volume 2, 7 September 2023.

• The International Institute For Strategic Studies. Cyber Capabilities and National Power: A Net Assessment, 2021

• The Luxembourg Government. Cyber Defence, https://defense.gouvernement.lu/en/la-defense/cyber.html, accessed: 17.03.2025.

• The Slovenia Times. Slovenia hit by another cyberattack, 11 April 2024, https://sloveniatimes.com/40402/slovenia-hit-by-another-cyberattack, accessed: 17.03.2025.

• Toucas, Boris. With Its New 'White Book,' France Looks to Become a World-Class Player in Cyber Space, War on the Rocks, 29 March 2018, https://warontherocks.com/2018/03/with-its-new-white-book-france-looks-to-become-a-world-class-player-in-cyber-space/, accessed: 17.03.2025.

• Tovima.com. Greek Armed Forces Take Part in NATO 2023 Cyber Exercise, 5 December 2023, https://www.tovima.com/politics/greek-armed-forces-take-part-in-nato-2023-cyber-exercise/, accessed: 17.03.2025.

• Trading Economics. Bulgaria Military Expenditure, https://tradingeconomics.com/bulgaria/military-expenditure, accessed: 17.03.2025.

• TRAFICOM. E-services, https://www.kyberturvallisuuskeskus.fi/en/contact-us/e-services, accessed: 17.03.2025.

• TRAFICOM. What to do in case of ransomware incident – instructions for management, 15/2022, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/What%20to%20do%20in%20case%20of%20a%20ransomware%20incident%20-%20instructions%20for%20management.pdf, accessed: 17.03.2025.

• Twenty-Four IT. UK Cybercrime Statistics 2024, 25 October 2024, https://www.twenty-four.it/services/cyber-security-services/cyber-crime-prevention/cybercrime-statistics-uk/ accessed: 17.03.2025.

• TVP World. Pro-Russian hackers target Italian government and public service websites, https://tvpworld.com/84466557/-pro-russian-hackers-target-italian-government-and-public-service-websites, accessed: 17.03.2025.

• United Nations Office on Drugs and Crime. Report on South Eastern Europe: Regional Assessment of the Impact of Cybercrime on Crime Prevention and Criminal Justice Systems, https://www.unodc.org/documents/southeasterneurope//202404_UNODC_Report_SPF_ENG_FINAL.pdf, accessed: 17.03.2025.

• US Army Cyber Command. About Army Cyber, https://www.arcyber.army.mil/About/About-Army-Cyber/ accessed: 05.02.2025.

• US Cyber Command. Our History, https://www.cybercom.mil/About/History/ accessed: 05.02.2025.

• US Department of Defense, 2023 DoD Cyber Strategy Summary, September 12, 2023.

• US Department of Defense. US Can Respond Decisively to Cyber Threat Posed by China, February 1, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3663799/us-can-respond-decisively-to-cyber-threat-posed-by-china/ accessed: 05.02.2025.

• US Embassy in Bulgaria. US Donates Cyber Defence Centre to Bulgaria, 14 September 2023, https://bg.usembassy.gov/u-s-donates-cyber-defence-center-to-bulgaria-09-14-2023/, accessed: 17.03.2025.

• US Fleet Cyber Command/Navy Space Command. Command Description, https://www.fcc.navy.mil/ accessed: 05.02.2025.

• US International Trade Administration. Greece - Country Commercial Guide – Defense, 28 December 2023, https://www.trade.gov/country-commercial-guides/greece-defense, accessed: 17.03.2025.

• US International Trade Administration. Greece Information Technology National Cybersecurity Strategy,7 October 2024, https://www.trade.gov/market-intelligence/greece-information-technology-national-cybersecurity-strategy, accessed: 17.03.2025.

• US International Trade Administration. Poland ICT the most cyberattacked country in the world, 28 February 2024, https://www.trade.gov/market-intelligence/poland-ict-most-cyber-attacked-country-world, accessed: 17.03.2025.

• United States Cyber Command. Fiscal Year 2025 Budget Estimates, March 2024, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/CYBERCOM_OP-5.pdf accessed: 05.02.2025.

• Wiedemar, Sarah., Cyber Attacks and Article 5: A Note on a Blurry but Consistent Position of NATO, Center for Security Studies (CSS), ETH Zürich, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf, accessed: 16.02.2025.

• Vlada Republike Slovenije. Obrambna strategija Republike Slovenije, datum: 24.04.2024, http://www.vlada.si/ accessed: 17.03.2025.

• Zelinka, Ivo. Fighting for the enemy's will and the support of its own population: the Cyber Forces and Information Operations Group in Olomouc, CZ Defence, 29 March 2024, https://www.czdefence.com/article/fighting-for-the-enemys-will-and-the-support-of-its-own-population-the-cyber-forces-and-information-operations-group-in-olomouc, accessed: 17.03.2025.

• Zotz, Philippe, Mitsuya. National Cybersecurity Organisation: Luxembourg, NATO CCDCOE, Tallinn, 2021, https://ccdcoe.org/uploads/2021/05/NCS_organisation_LUX-2021-FINAL.pdf, accessed: 17.03.2025.