Terrorism – Studies, Analyses, Prevention, 2025, special edition: 225–248

https://doi.org/10.4467/27204383TER.25.021.21524

Article

Cyber threats as hybrid activity against the European Union in light of the current geopolitical situation

MONIKA STODOLNIK
https://orcid.org/0009-0000-5319-7968
Internal Security Agency

Abstract

The article presents analysis of cyber threats as a manifestation of the hybrid threats facing Europe. The author analysed reports from European Union and NATO countries in terms of how the identified threats are presented by intelligence services, governments and national CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams). She also discussed the categorisation of cyber threats based on their source of origin and their purpose, including state-sponsored, hacktivist and cybercriminal groups. She pointed to the increasing frequency of cyber attacks, especially those conducted from Russia and China, and discussed their impact on the critical infrastructure and political stability of states. She presented the changing landscape of cyber threats in Europe, gave examples of cyber attacks and described the methods of reporting these incidents adopted in Denmark, Germany, Estonia, Lithuania, Latvia and Poland.

Keywords

hybrid threats, cyber attack, cyber security, disinformation, information operations

Introduction

The contemporary geopolitical situation makes hybrid threats one of the most serious challenges to Europe's security and stability. Hybrid threats represent a combination of conventional and unconventional tactics and aim, among other things, to destabilise the state, its democracy and undermine public confidence. Referring to Francis Fukuyama's definition, according to whom (...) *trust is a mechanism based on the assumption that other members of a given community are characterised by honest and cooperative behaviour based on professed norms*[1], it can be observed that manipulative psychological activities, disinformation violate this very mechanism and deepen divisions in society. In 2025, Europe is particularly vulnerable to such threats due to its close proximity to a potential adversary, as well as technological progress, the potential of which can be used for both defence and attack. Observations and lessons learned from the war in Ukraine point to possible vectors of activity of the Russian Federation (RF) in a situation where the conflict is extended to other European states. The dynamic development of artificial intelligence in recent years has supported hostile activity in cyberspace, in terms of generation of disinformation content and the development of tools to attack information and communication infrastructure.

The standard of living is increasing as technology advances. Due to the development of information and communication technologies (ICT) and growing dependence on automation of various industries, namely Industrial Control Systems (ICS), the society is at the all-time high risk of life threatening disruptions originating in the cyberspace. The energy sector, a key pillar of any modern country's economy, is particularly vulnerable to destructive actions[2]. As EnergiCERT, the Danish energy sector computer incident response team, points out, the number of attacks on this sector in Europe between 2015 and 2022 had a steady upward trend[3]. Attacks on energy sector actors can paralyse a country – regardless of whether the perpetrators of the attack have financial, ideological or political motives. At the same time, the amount and character of official documents

[1] F. Fukuyama, *Zaufanie. Kapitał społeczny a droga do dobrobytu* (Eng. Trust. The social virtues and the creation of prosperity), Warszawa 1997, p. 38.

[2] *Cybersecurity of Critical Sectors – Energy*, ENISA, https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy [accessed: 8.04.2025].

[3] *Cyber attacks against European energy & utility companies*, EnergiCERT, September 2022, https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf [accessed: 8.04.2025].

and correspondence that is created and processed electronically make them the prime target for espionage operations that put the national security at risk.

This paper examines the multifaceted nature of hybrid threats facing Europe. This was done on the basis of a review of reports on cyber threats and cyber attacks as a manifestation of hybrid activity, produced from selected EU and NATO countries. The subject of the research was how such threats are presented by the intelligence services, governments and national CERTs and CSIRTs of Denmark, Germany, Estonia, Lithuania, Latvia and Poland – countries located in close proximity to the RF and of interest to Russian cyber offensive group.

Landscape of cyber threats as hybrid threats

As defined by NATO: *Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies*[4]. The European Union in its *Joint framework on countering hybrid threats – a European Union response* by the European Commission, points out that *definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature*[5]. In turn, Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats) presents hybrid threats as activities (...) *used by authoritarian states and regimes, and by non-state actors (NSAs), which often act as proxies for authoritarian regimes. Examples of hybrid threat actors include Russia, China, and Iran. Non-state hybrid threat actors can include groups, movements or entities, which are used or co-opted to fulfil certain strategic objectives*[6].

[4] *Countering hybrid threats*, NATO, 7.05.2024, https://www.nato.int/cps/en/natohq/topics_156338.htm [accessed: 19.03.2025].

[5] *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response*, Brussels, 6.04.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018, p. 2 [accessed: 19.03.2025].

[6] *Frequently asked questions on hybrid threats*, Hybrid CoE, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [accessed: 19.03.2025].

When considering cyber threats in this context, they can be divided into general categories depending on who is the source of the threat and the methods they use to achieve their chosen objective:

- Nation-state actors, often highly sophisticated and technologically advanced:
  - cyber espionage,
  - cyber sabotage,
  - cyber-enabled information operations.
- Hacktivist collectives, ideologically motivated:
  - disruption of IT systems and services (DDoS attacks),
  - cyber sabotage (attacks that alter parameters, damage, affect the provision of the service other than through unavailability),
  - defacement of page content,
  - hack-and-leak attacks.
- Cyber criminals, financially motivated:
  - money extortion via ransomware,
  - money extortion via threatening to disclose data.

Nation-state actors, also called state-sponsored groups, often equated to advanced persistent threat (APT) groups[7], are government-backed entities, often units of special services, that conduct cyber offensive activities serving the state's interest[8]. Cyber espionage, being a natural extension to the traditional means of intelligence, are at the forefront of their activity, as the goal itself and also as a means for reconnaissance, necessary for staying unnoticed. Cyber espionage is often conducted by the means of phishing or spearphishing, that is by utilising social engineering through email in order to obtain certain information or infect workstation with malicious software. Other than phishing, cyber espionage can also be conducted by compromising a device or network using a vulnerability, that is a weakness of an IT system (a registered, well-known vulnerability, a zero-day vulnerability, a misused feature or a user error). Such attacks violate one element of the cybersecurity triad – confidentiality[9]. As for the integrity of data, such attacks are considered cyber sabotage – destructive in nature and with many more consequences.

[7] APT groups – organised entities that carry out sophisticated and long-lasting attacks in cyberspace.

[8] J. Kose, *Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage*, "ISSA Journal" 2021, vol. 19, no. 4, pp. 12–15.

[9] CIA triad: confidentiality, integrity, availability.

They have the potential to disrupt daily life of citizens when they affect CI and create blackouts or transport delays. More severely, when targeting navigation or health protection systems, they can be deadly.

Information operations are (...) *actions taken to affect adversary information and information systems while defending one's own information and information systems*[10]. Cyber-enabled information operations or influence campaigns – the terms being used interchangeably – (...) *sit at the nexus of intelligence-based deception and strategic-oriented delivered effects*[11]. Their goal is a (...) *deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes*[12]. Such activity can involve compromising news media IT systems in order to publish crafted material in a reputable source, creating own websites and social media profiles, mass sending of messages via email or text messages.

Hacktivism as a term is a combination of the words *hacking* and *activism*, therefore is (...) *a combination of grassroots political protest with computer hacking*[13]. In the most recent times, on the forefront of hacktivists one will find pro-Russian and pro-Palestinian groups organising and communicating on Telegram application, conducting a range of cyber attacks with varied results. However, for some the "grassroots" character is questionable, as XakNet Team, Infoccentr, Solntsepek and Cyber Army of Russia Reborn are assessed by some researchers to be cooperating with Russian Main Intelligence Directorate (GRU) and its affiliated cyber threat groups, namely APT28[14] and APT44[15].

---

[10] D.T. Kuehl, *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, "International Law Studies" 2022, vol. 76, p. 36.

[11] J. Vićić, R. Harknett, *Identification-imitation-amplification: understanding divisive influence campaigns through cyberspace*, "Intelligence and National Security" 2024, vol. 39, no. 5, pp. 897–914. https://doi.org/10.1080/02684527.2023.2300933.

[12] H. Lin, J. Kerr, *On Cyber-Enabled Information/Influence Warfare and Manipulation*, in: *The Oxford Handbook of Cyber Security*, P. Cornish (ed.), Oxford University Press 2021, pp. 251–272.

[13] T. Jordan, P. Taylor, *Hacktivism and cyberwars. Rebels with a cause?*, London 2004, p. 1.

[14] Mandiant Intelligence, *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant, 23.09.2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions [accessed: 19.03.2025].

[15] G. Roncone et al., *APT44: Unearthing Sandworm*, Mandiant, 17.04.2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [accessed: 19.03.2025].

The most well-known hacktivist groups' main modus operandi are *distributed denial-of-service* (DDoS) attacks with the goal of making the targeted websites or services unavailable for the general public. These groups also compromise infrastructure by unauthorised access. They are often not concerned with achieving some complex goal, but merely with demonstrating their technical capabilities. Along with the abovementioned, website *defacement* and *hack-and-leak* attacks are also tools used by the actors to spread their message. The former is used to replace the content of a website with a message from the hacker, while the latter is a form of attack where the data exfiltrated from the victim's networks and servers are shared publicly[16].

With the hacktivism being activism in the cyberspace, similarly, cybercrime (...) *consists of criminal acts committed online by using electronic communications networks and information systems*[17]. Such acts include, for example, attacks on information systems as the most critical for the state, not the citizens themselves. The most widely reported incidents related to cybercrime have to do with ransomware, which (...) *has grown to be a dominant cybersecurity threat*[18]. Ransomware is a type of malicious software that is used to extort a ransom from the attacked party by denying access to systems and data. Most current ransomware attacks are double-extortion attacks, where the attacker encrypts the data and also exfiltrates it. In doing so, they demands a ransom not only for decryption, but also to prevent their sale or publication[19]. Such ransomware can disrupt an entity's operations and, due to the effects of service interruption and data leakage, including customer data, can cause a loss of trust on the part of potential cooperation partners.

Between 2014 and 2024, the frequency of hybrid attacks, especially in the cyberspace, increased. The RF is by far the largest perpetrator

[16] D. Sancho, *Understanding Hacktivists. The Overlap of Ideology and Cybercrime*, Trend Micro, 4.02.2025, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/understanding-hacktivists-the-overlap-of-ideology-and-cybercrime [accessed: 19.03.2025].

[17] *Cybercrime*, European Commission, 31.10.2024, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en [accessed: 19.03.2025].

[18] T. McIntosh et al., *Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration*, "ACM Computing Surveys" 2024, vol. 57, no. 1, p. 1. https://doi.org/10.1145/3691340.

[19] *What is data exfiltration?*, IBM, https://www.ibm.com/think/topics/data-exfiltration [accessed: 19.03.2025].

of state-sponsored cyber attacks – including attacks by pro-Russian hacktivist – against European countries[20]. These have mainly targeted governmental systems and websites, critical infrastructure, state-owned and private companies, think tanks, non-governmental organisations (NGOs), journalists and politicians. In 2022, hacktivist groups, acting on behalf of Russia, carried out 61% of cyber attacks worldwide[21]. The biggest catalyst of such activity has been the war in Ukraine. From the beginning of 2022, various actors declare support for Russia and act in their interest, conducting cyber espionage, cyber sabotage and information operations against EU and NATO countries[22]. In addition to these politically motivated acts, many cybercrime actors active in attacks against Europe and USA are also associated with Russia. Some of them are Hunters International[23], Hive[24] or Conti[25]. Regardless of the attribution to an APT actor, hacktivist or cybercriminal collective, false-flag operations are also important to consider when it comes to Russian activity in the cyberspace. If one takes into account examples such as the activity of a group self-identifying as Cyber Berkut in 2014, the activities of Cyber Caliphate in 2015 and ransomware attacks in 2016 and 2017, all attributed to the Russian military

[20] *Microsoft Digital Defense Report 2024, The foundations and new frontiers of cybersecurity*, https://go.microsoft.com/fwlink/?linkid=2290930&clcid=0x409&culture=en-us&country=us, p. 13 [accessed: 19.03.2025].

[21] Thales Cyber Threat Intelligence, *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*, Thales, 29.03.2023, https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point [accessed: 8.04.2025].

[22] S.G. Jones, *Russia's Shadow War Against the West*, Center for Strategic & International Studies, 18.03.2025, https://www.csis.org/analysis/russias-shadow-war-against-west [accessed: 19.03.2025].

[23] R. Wolert, *RaaS group profile Hunters International*, CERT Orange, 28.10.2024, https://cert.orange.pl/wp-content/uploads/2024/11/CERTOPL_CTI_Hunters_International_en.pdf [accessed: 19.03.2025].

[24] *Russian National Charged with Ransomware Attacks Against Critical Infrastructure*, U.S. Department of Justice, 16.05.2023, https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure [accessed: 19.03.2025].

[25] *Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies*, U.S. Department of Justice, 7.09.2023, https://www.justice.gov/archives/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware [accessed: 19.03.2025].

intelligence service GRU[26], the reach of the Russian special services may be broader than one might have initially thought.

China, another important source of cyber threats, follows its political and ideological goals of greatness and a superpower status[27]. Their hacking serves strategic economic goals. According to China's Military Strategy (...) *cyberspace has become a new pillar of economic and social development*[28]. According to NATO experts (...) *Parts of the Chinese military have become useful tools for the government to conduct political and economic cyber espionage, and also to help reduce the PLA's* [People's Liberation Army] *own technological and strategic disadvantages relative to its competitors*[29]. Thus the most vulnerable economic sectors of European states are: energy, telecommunications and transport[30].

Denmark

One of the most extensive cyber attacks against Danish CI happened in May 2023. The actor, not openly attributed to the GRU, but suspected by SektorCERT to be related to Sandworm group[31], conducted thorough reconnaissance before the attack. It might have included, among cyber espionage, traditional means of collecting intelligence. SektorCERT reported, that the information about the vulnerable devices was not available on public services (such as Censys or Shodan) at the time

[26] A. Greenberg, *A Brief History of Russian Hackers' Evolving False Flags*, Wired, 21.10.2019, https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/ [accessed: 19.03.2025].

[27] A.H. Cordesman, *China's Emergence as a Superpower*, Center for Strategic & International Studies, 15.08.2023, https://www.csis.org/analysis/chinas-emergence-superpower [accessed: 19.03.2025].

[28] *China's Military Strategy*, Ministry of National Defense of the People's Republic of China, 23.06.2021, http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html [accessed: 19.03.2025].

[29] M. Raud, *China and Cyber: Attitudes, Strategies, Organization*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf, p. 21 [accessed: 19.03.2025].

[30] *Report on the state of Poland's cybersecurity in 2024*, in press.

[31] *The attack against Danish, critical infrastructure*, SektorCERT, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf, p. 15 [accessed: 19.03.2025].

of the attack, proving that the attackers had obtained such information via other means[32]. The Zyxel edge device software vulnerability that was exploited in this attack (CVE-2023-28771) received a score of 9.8 out of 10. This makes it a critical vulnerability – one that is easy to exploit and allows for a security breach that has serious consequences. The vulnerable devices manufactured by Zyxel were at that time largely utilised by small Danish CI operators for their OT[33] environments. Altogether, 22 energy companies were successfully compromised and several of them noted disruptions in their operations.

The most recent assessment of Denmark on the hybrid threats from Russia is that it (...) *uses hybrid means both in the run-up to and during a direct military conflict* (...) *hybrid means include political, economic, informational and military tools, which can be used in coordination to maximize their impact*[34]. Danish Defence Intelligence Service (Danish: Forsvarets Efterretningstjeneste) identifies that Russian hybrid operations involve both public authorities and private actors, with the former coordinating activities, which is often concealed as to who is behind it[35]. Following similar outlook on the present situation regarding threat level and goals, Danish Centre for Cyber Security (Danish: Center for Cybersikkerhed) assesses that (...) *it is likely that state-sponsored Russian hackers conduct cyber espionage against Danish CI in preparation for destructive cyber attacks in the future*[36]. At the same time China is also suspected to be conducting cyber espionage in order to gain information on technology and policies. Going further, this centre evaluates that the highest risk of cyber attacks, that result in death or injury, significant property damage or destruction or manipulation of information, data or software, comes from Russia, mainly state-sponsored groups.

[32] Ibid., p. 10.

[33] Operational technology – systems and equipment used to monitor, control and manage technological processes, such as production machinery, pumps, measuring devices or traffic management systems.

[34] *Intelligence Outlook 2024*, Danish Defence Intelligence Service, 22.01.2025, https://www.fe-ddis.dk/en/produkter/Risk_assessment/riskassessment/Intelligenceoutlook2024/, p. 26 [accessed: 19.03.2025].

[35] Ibid.

[36] *Threat assessment: the cyber Threat against Denmark 2024*, Centre for Cyber Security, September 2024, https://www.cfcs.dk/link/472c3cc8872446e59fa59eaf0f7ad945.aspx, p. 8 [accessed: 19.03.2025].

Germany

In May 2023, Germany's Federal Minister of the Interior stated: *We will absolutely not be intimidated by the Russian regime*[37]. These words were said in reference to cyber attacks conducted by the RF. The cause for such reaction was the announcement that the GRU and their threat group APT28 were behind the cyber attacks in January 2023. The targets of these attacks were the SPD party along with companies in the logistics, defense, aviation and IT sectors. The attack was possible due to a security gap in Microsoft Outlook, that made it possible for unauthorised actor to access email accounts of these entities. Germany stood behind the opinion that this attack was (...) *a serious interference with democratic structures*[38]. In general, the Federal Ministry of the Interior and Community (German: Bundesministerium des Innern und für Heimat) assesses that the war in Ukraine has changed the security situation in Germany in such a way, that the country needs better protection and awareness of vulnerability to cyber attacks and Russian disinformation[39].

German intelligence services state that Russia's espionage activities concern government and administration as well as military, technology, research, business and industry. *Russian cyber attacks, whether directed at individuals, organisations or government institutions, are primarily aimed at gaining a steady source of intelligence. In addition to such espionage, these attacks may also be used for sabotage, influence operations, disinformation or propaganda purposes*[40].

On the issue of cyber threats from China, Germany believes that the actions of the intelligence services serve the Chinese Communist Party's goal of China's status as a global leader and world power[41]. Federal Office for the Protection of the Constitution (German: Bundesamt für

[37] *Cyber attacks traced to Russian military intelligence agency*, Federal Ministry of the Interior and Community, 3.05.2024, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html [accessed: 19.03.2025].

[38] Ibid.

[39] *Heightened security situation in Germany*, Federal Ministry of the Interior and Community, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/ukrain/security_meldung.html [accessed: 19.03.2025].

[40] *Brief summary 2023 Report on the Protection of the Constitution (Facts and Trends)*, Bundesamt für Verfassungsschutz, https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2024-06-brief-summary-2023-report-on-the-protection-of-the-constitution.pdf, p. 60 [accessed: 19.03.2025].

[41] Ibid.

Verfassungsschutz) directly points to groups APT15 and APT31 as notable due to their complex techniques and tools they use. In early 2023, Germany's IT service providers for government networks were targeted in a supply chain attack by a Chinese threat actor[42]. However, the report did not specify what the attack consisted of.

Estonia

The first cyber attack publicly attributed by Estonian authorities was conducted in 2020 by the military intelligence service of Russia – GRU, specifically Unit 29155. CERT-EE team, the incident handling unit of the Information System Authority of Estonia, reported that the computer systems of the Ministry of Economic Affairs and Communications were breached with a backdoor malware. This resulted in exfiltration of 350 GB of data, including sensitive internal information – strategic documents and working papers, personnel details, and correspondence with businesses[43]. The same actor also attacked the Ministry of Foreign Affairs and the Health and Welfare Information Systems Centre. The public announcement and attribution only happened in late 2024 as a result of the Operation Toy Soldier by Estonia and several other countries, linking Unit 29155 to multiple cyber attacks against Ukraine, NATO and EU countries. *The objectives of GRU's cyber cell, Unit 29155, include gathering intelligence, causing reputational damage through the theft and leak of sensitive information, and systematic sabotage by destroying data and computer systems*[44].

In 2023, CERT-EE also published a thorough analysis of hacktivist-lead DDoS attacks that were carried out in 2022 and targeted public, transport and financial sector websites of Estonia. The attacks were increasing in relation to certain events, such as moving of the Soviet monuments in Narva or declaration by Estonian parliament Riigikogu that the Russian regime is terrorist[45]. CERT-EE announced that the impact of those attacks

[42] Ibid., p. 62.

[43] *Cyber Security in Estonia 2025*, Republic of Estonia Information System Authority, https://www.ria.ee/en/cyber-security-estonia-2025 [accessed: 19.03.2025].

[44] Ibid.

[45] *Cyber Security in Estonia 2023*, Republic of Estonia Information System Authority, https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf, p. 17 [accessed: 19.03.2025].

was marginal, sending the message that Estonia does not consider them as a serious threat, but rather as a nuisance. Most importantly, CERT-EE did not attribute these attacks to the Russian state, but to ideologically motivated hackers for whom the war was the catalyst. The attacks were often the result of actions not in line with the official Russian narration.

Presenting a general perception of sponsored threats in cyberspace, the Estonian Internal Security Service (Estonian: Kaitsepolitseiamet, KAPO) stated that hostile cyber intelligence activities (...) *are usually carried out by hostile nations' military and special services' cyber intelligence units that persistently work to advance their country's interests*[46]. According to KAPO (...) *both state institutions and companies providing critical services must recognise that their status as such renders them potential targets for* [cyber sabotage] *attacks*[47]. *KAPO considers it highly likely that the Russian special services will continue to attempt to gain illegal access to the computer networks of Estonia's critical service providers and key transport and logistics companies in order to gather information and be prepared to disrupt their operations with cyber measures if necessary*[48].

An important observation to public attitude and perception towards non-state actors such as cybercriminals or hacktivists is that (...) *Russian special services also use hackers who are indirectly related to them and appear to operate independently*[49]. KAPO assesses that such low-level, low-impact attacks, as opposed to APT groups directly tied to special services, enable Russia to generate an illusion of strong support and high capabilities[50].

Estonia also draws attention to threats from China. KAPO points out that technology produced there may contain malware and hardware backdoors, allowing for unauthorised access to Estonian networks and devices by the Chinese[51]. Therefore, despite the competitive prices of these technologies, it is important to consider Chinese-origin solutions as

[46] *Annual review 2023–2024*, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf, p. 26 [accessed: 19.03.2025].

[47] Ibid.

[48] *Annual review 2022–2023*, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf, p. 22 [accessed: 19.03.2025].

[49] *Annual review 2023–2024*..., p. 26.

[50] Ibid., p. 27.

[51] *Annual review 2022–2023*..., p. 24.

a potential threat to the information processed in the targeted systems and to carry out an analysis of the risks arising from their use on a case-by-case basis.

Lithuania

Preceding the war in Ukraine, Lithuania had been one of the prime targets of the "Ghostwriter" campaign, attributed to group UNC1151 and at that time associated with Russia[52]. This activity, which continues, albeit on a smaller scale, combines two spheres – cyber attacks and information operations, where compromised infrastructure is used to spread disinformation to the public. Numerous operations were mostly related to relations between Lithuania and Poland, e.g. information operations under the heading "Radioactive waste leaked from Lithuanian nuclear plant poses danger to Poles living near border" or "Poland trained extremists to destabilise Lithuania", but also between Lithuania and Germany or the US[53] In a statement on 23 September 2021, Vice Minister of National Defence Margiris Abukevičius said that *Lithuania firmly supports the joint European Union Declaration issued in a rigorous condemnation of the Ghostwriter cyber-information attacks associated with Russia that target democratic processes, institutions, politicians, media representatives and, generally, societies, of EU member states*[54]. In 2023, Lithuanian intelligence services – The Second Investigation Department under the Ministry of National Defence (Lithuanian: Antrojo Operatyvinių Tarnybų Departamento, AOTD) and State Security Department (Lithuanian: Valstybės Saugumo Departamentas, VSD) reported that cyber-enabled information operations against Lithuania by the Ghostwriter have subsided due to its redirected effort towards Ukraine.

[52] The current assessment of experts on the subject is that the group is equally likely to have ties to either Russia or Belarus. A false flag operation is also possible.

[53] *GhostWriter Update: Cyber Espionage Group UNC1151 Likely Conducts GhostWriter Influence Activity*, Mandiant, 28.04.2021, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf, pp. 12–14 [accessed: 19.03.2025].

[54] *Lithuania supports the EU declaration condemning Ghostwriter malicious cyber activities and calls to use more political tools*, Ministry of National Defence of the Republic of Lithuania, 23.09.2021, https://kam.lt/en/lithuania-supports-the-eu-declaration-condemning-ghostwriter-malicious-cyber-activities-and-calls-to-use-more-political-tools/ [accessed: 8.04.2025].

Lithuanian intelligence services assess that due to mass expulsions of Russian diplomats, or rather Russian intelligence officers under diplomatic cover, Russia will seek other means for information gathering and thus resort to, among others, cyber espionage. AOTD and VSD evaluated attacks as increasingly prevalent, mostly targeting governmental organisations and CI.

Lithuania, like Estonia, points to the cooperation of cyber criminals and non-state-supervised hackers with Russian special services. Criminals benefit financially and have technological support through this cooperation, while states gain from the fact that attribution becomes more difficult[55].

In 2024 Lithuania focused their reporting on the threat posed by China. It was pointed, that (...) *their activity in Lithuanian cyberspace has increased especially since 2021, when Lithuania announced the opening of the Taiwanese Representative Office*[56]. The most recent switch in targeting happened from the private sector to governmental institutions for internal affairs and foreign policy. Tactics have evolved towards social engineering, activities are conducted via social networks.

Latvia

Latvian government is not very open to naming perpetrators of cyber attacks, while still presenting the sectors that are the most targeted – in 2022 the same actors behind attacks on Ukrainian infrastructure tried to attack entities in telecommunication and energy sectors. The names or affiliation of the attackers were not disclosed due to security reasons[57]. As predicted by Latvian State Security Service (Latvian: Valsts drošības dienests, VDD)

[55] *National Threat Assessment 2023,* https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf, p. 55 [accessed: 19.03.2025].

[56] *National Threat Assessment 2024,* https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-EN-1.pdf, p. 57 [accessed: 19.03.2025].

[57] D. Antoniuk, *Latvia's cyberspace faces new challenges amid war in Ukraine*, The Record, 28.10.2022, https://therecord.media/latvias-cyberspace-faces-new-challenges-amid-war-in-ukraine [accessed: 19.03.2025].

in 2022[58] and manifested in 2023[59] and 2024[60], state-supported groups originating in Russia were behind supply chain attacks using malware-laced hardware or software as well as updates or maintenance services. According to the Constitution Protection Bureau (Latvian: Satversmes aizsardzības birojs, SAB), such supply chain attacks targeted, for one, a TV satellite of Tet, a Latvian telecom company, which resulted in brief Russian propaganda broadcast. Similarly, the hackers managed to obtain access to outsourced Balticom servers in Bulgaria and broadcast a Russian military parade[61] – in neither case the infrastructure was located in Latvia[62]. Nevertheless, Latvia's CERT.LV team emphasised that (...) *it is essential to prevent the involvement of Latvia's IT infrastructure in cyberattacks and the possibility of attacks from within the country, as Russian-linked telecommunications companies are deliberately building a presence in Latvia and other EU member states*[63].

The attacks that compromise transmission infrastructure for broadcasting propaganda blur the boundaries between a cyber attack and an information operation, where an entity gets breached in order to use its reach and reputation for distribution of disinformation. Compared to other means of such activity, cyber-enabled information operations can much more quickly reach the intended audience, thus making them an attractive vector for the perpetrators.

Similarly to other European countries, Latvia also supports the belief, that pro-Russian hacktivists are (...) *likely coordinated and financed to achieve the objectives of Russia's domestic and foreign policy influence operations*[64].

[58] *Annual Report on the activities of Latvian State Security Service (VDD) in 2022,* https://vdd.gov.lv/uploads/materials/33/en/annual-report-2022.pdf, pp. 13–14 [accessed: 19.03.2025].

[59] *Annual Report on the activities of Latvian State Security Service (VDD) in 2023,* https://vdd.gov.lv/uploads/materials/37/en/annual-report-2023.pdf, p. 15 [accessed: 19.03.2025].

[60] *Annual report on the activities of Latvian State Security Service (VDD) in 2024,* https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf, p. 17 [accessed: 19.03.2025].

[61] *Latvia mulls tightening security after recent TV propaganda hacks,* LSM+, 20.05.2024, https://eng.lsm.lv/article/society/crime/20.05.2024-latvia-mulls-tightening-security-after-recent-tv-propaganda-hacks.a554618/ [accessed: 19.03.2025].

[62] *2024 Annual Report,* Republic of Latvia Constitution Protection Bureau, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf, p.36 [accessed: 19.03.2025].

[63] *Latvian Cybersecurity and CERT.LV Technical Activities Annual Report 2023,* 26.07.2024, https://cert.lv/uploads/eng/Annual_Report_CERT-LV_2023.pdf, pp. 4–5 [accessed: 19.03.2025].

[64] Ibid., p. 6.

At the same time, reflecting on the events of 2022, VDD verified that the information published by such groups on their channels on Telegram is disinformation, as the damage they report did not actually occur[65].

In regards to Chinese intelligence, VDD assesses that China continues to consider Latvia primarily as a part of NATO and the EU, which it sees as the main rivals in the competition for global influence[66]. With this in mind, their goal is clear – collecting intelligence on strategic decisions and policy regarding relations between China and opponent countries. Latvia's intelligence services observe attempts from Chinese representatives to create and strengthen positive relations and influence with Latvian politicians, academics and researchers, which confirms their interest in new technologies, innovations and policies. This interest translates into cyber matters, where Chinese cyber units show their hacking activity.

Poland

Polish state security institutions do not make information available in the form of periodic reports on strategic or operational issues (only reports on technical issues), so in order to assess the government's position on hybrid threats it was necessary to reach for ad hoc announcements from spokespersons or publications appearing on the official government website gov.pl.

Such was the official statement of the Government Plenipotentiary for the Security of Information Space of the Republic of Poland in late 2022, where several cyber attacks were attributed to Russian hackers: (...) *through hostile operations in cyberspace Russia wants to exert pressure on Poland, as a frontline country and a key Ukraine's ally on the NATO eastern flank*[67]. Those included DDoS attacks carried out by the pro-Russian hacktivist group NoName057(16) as a response to a resolution of the Polish Parliament

[65] *Annual Report on the activities of Latvian State Security Service (VDD) in 2022*..., p. 13.

[66] Ibid.

[67] *Russian cyberattacks*, Serwis Rzeczypospolitej Polskiej, 30.12.2022, https://www.gov.pl/web/special-services/russian-cyberattacks [accessed: 19.03.2025].

of December 2022 recognising Russia as a state sponsor of terrorism[68], as well as the creation of data collection websites through phishing.

Similarly, the Spokesman for Poland's Minister-Special Services Coordinator stated in mid-2022 that (...) *intelligence operations involving hacking attacks, taking over information resources and using them to manipulate public opinion have been used by the Kremlin in recent years in its fight against NATO*[69]. He therefore clearly attributed these actions to Russia.

The year 2024 was the first year that the Report of the Government Plenipotentiary for Cybersecurity for the previous year was presented publicly[70]. Previously, it was a fully classified document. This thus served, along with CERT Polska and CSIRT GOV annual reports, as the only official resources for an overview of 2023.

During several months preceding the parliamentary elections in 2023, hacking group UNC1151 continued to carry out their personalised spearphishing activity against politicians, military personnel, journalists, lawyers, and various other people that might have a connection to Russia and Belarus. Such campaigns had the goal of cyber espionage and disinformation. In the Report on the state of Poland's cybersecurity in 2023 they were attributed to Belarus. The same group is thought to be behind a cyber-enabled information operation directly preceding the elections, where emails, text messages and mall info screens were utilised for spreading disinformation[71].

No direct attribution, but hints to the Russian provenience, were given by the Minister of Digital Affairs regarding the cyber attack on the Polish

[68] *Sejm uznał Rosję za państwo wspierające terroryzm* (Eng. The Sejm recognised Russia as a state supporting terrorism), Sejm Rzeczypospolitej Polskiej, 14.12.2022, https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC10C1258918007022FA [accessed: 8.04.2025].

[69] *Ataki hakerskie na RP operacją rosyjskich służb* (Eng. Hacker attacks in the Republic of Poland as an operation of Russian services), Serwis Rzeczypospolitej Polskiej, 20.07.2022, https://www.gov.pl/web/special-services/hacker-attacks-on-the-republic-of-poland-as-an-operation-of-russian-services [accessed: 19.03.2025].

[70] *Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok* (Eng. Report of the Government Plenipotentiary for Cyber Security for 2023), Ministerstwo Cyfryzacji (Eng. Ministry of Digital Affairs), 11.04.2024, https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni [accessed: 8.04.2025].

[71] *Report on the state of Poland's cybersecurity in 2024*, CSIRT GOV, https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf, p. 6 [accessed: 19.03.2025].

Press Agency and a false dispatch about a partial mobilisation in Poland that was published on the PAP website as a result of a hack. The minister stated about this event that its goal was (...) *to spread disinformation before the elections and to 'paralyse' society*[72]. It was about the European Parliament elections in 2024.

Reporting in Poland focuses more on the incidents themselves, such as various examples of phishing emails distributed by Russia-affiliated APT groups like APT28, APT29 or Gamaredon for the purpose of cyber espionage. Such reports are presented by the national CSIRTs. In Poland, little is said about the overall hybrid threat landscape from a counterintelligence perspective despite one national CSIRT team operating within the structures of the Internal Security Agency.

There is very little information published on threats originating from China in Poland. Only a few examples of such incidents can be found in the government sources. The assessment of the situation in 2023 was that due to the level of propaganda cooperation between China and Russia, (...) *it should be expected that the interests and activity of Chinese intelligence will not change, mainly due to the scale of support that the Republic of Poland provides to Ukraine in repelling Russian aggression, Warsaw's alliance with Washington, and the situation around Taiwan*[73].

Conclusions

The results of presented research as a whole provide an in-depth overview of the current cyber threats faced by the European Union. The position of the countries analysed is that the attacks originating in Russia have been on the rise since the beginning of the war in Ukraine in 2022. There are no signs suggesting that they might subside. On the contrary, the capabilities of the threat actors are evolving with their experience and the attacks are becoming more covert and sophisticated. In regards to China, the unanimous opinion is that the threats originating from this country are intensifying and may evolve from intelligence gathering into destructive.

[72] *Fake PAP report looks like cyberattack, says gov't official*, Polska Agencja Prasowa, 31.05.2024, https://www.pap.pl/en/news/fake-pap-report-looks-cyberattack-says-govt-official [accessed: 19.03.2025].

[73] *China's propaganda offensive*, 17.02.2023, https://www.gov.pl/web/special-services/Chinas-propaganda-offensive [accessed: 19.03.2025].

The other two states from the Big Four[74], that is Iran and North Korea, are rarely mentioned in relation to cyber threats.

The strategies for reporting and attributing the attacks adopted in the countries analysed can be divided into 3 categories: minimal, cautious and direct. Latvia, in the case of attacks on its telecommunications and energy sectors, only reported that the same actor was behind the attacks in Ukraine. It led the public to believe that this actor was linked to Russia, but did not name them directly. Denmark was careful to identify the name of the group potentially behind the critical infrastructure attack, while emphasising the high uncertainty and circumstantiality of the attribution. Germany however directly attributed the attacks against various sectors to a GRU-lead group APT28, openly speaking about Russian activity. At the same time, questions arise about how many similar attacks have not been made public? How many disruptions reported as accidents and malfunctions were in fact serious cyber attacks of foreign actors?

Each report on the technicalities of attacks is an important source of information for cyber security analysts and each report of intelligence services broadens the horizon of knowledge of security researchers, allowing for a better understanding of the threat landscape not only in one country, but also a whole region. It is imperative for Europe to build a unified and coherent stance on cyber treats for the common good.

Bibliography

Fukuyama F., *Zaufanie. Kapitał społeczny a droga do dobrobytu* (Eng. Trust. The social virtues and the creation of prosperity), Warszawa 1997.

Jordan T., Taylor P., *Hacktivism and Cyberwars. Rebels with a cause?*, London 2004.

Kose J., *Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage*, "ISSA Journal" 2021, vol. 19, no. 4, pp. 12–15.

Kuehl D.T., *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, "International Law Studies" 2022, vol. 76, pp. 35–58.

[74] The Big Four state actors, i.e. China, Russia, North Korea, Iran, are a group of states identified by cyber security analysts as the biggest sources of cyber threats.

Lin H., Kerr J., *On Cyber-Enabled Information/Influence Warfare and Manipulation*, in: *The Oxford Handbook of Cyber Security*, P. Cornish (ed.), Oxford University Press 2021, pp. 251–272. https://doi.org/10.1093/oxfordhb/9780198800682.013.15.

McIntosh T. et al., *Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration*, "ACM Computing Surveys" 2024, vol. 57, no. 1. https://doi.org/10.1145/3691340.

Vićić J., Harknett R., *Identification-imitation-amplification: understanding divisive influence campaigns through cyberspac*e, "Intelligence and National Security" 2024, vol. 39, no. 5, pp. 897–914. https://doi.org/10.1080/02684527.2023.2300933.

Internet sources

Antoniuk D., *Latvia's cyberspace faces new challenges amid war in Ukraine*, The Record, 28.10.2022, https://therecord.media/latvias-cyberspace-faces-new-challenges-amid-war-in-ukraine [accessed: 19.03.2025].

Ataki hakerskie na RP operacją rosyjskich służb (Eng. Hacker attacks in the Republic of Poland as an operation of Russian services), Serwis Rzeczypospolitej Polskiej, 20.07.2022, https://www.gov.pl/web/sluzby-specjalne/ataki-hakerskie-na-rp-operacja-rosyjskich-sluzb [accessed: 19.03.2025].

Brief summary 2023 Report on the Protection of the Constitution (Facts and Trends), Bundesamt für Verfassungsschutz, https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2024-06-brief-summary-2023-report-on-the-protection-of-the-constitution.pdf [accessed: 19.03.2025].

China's propaganda offensive, 17.02.2023, https://www.gov.pl/web/special-services/Chinas-propaganda-offensive [accessed: 19.03.2025].

Cordesman A.H., *China's Emergence as a Superpower*, Center for Strategic & International Studies, 15.08.2023, https://www.csis.org/analysis/chinas-emergence-superpower [accessed: 19.03.2025].

Countering hybrid threats, NATO, 7.05.2024, https://www.nato.int/cps/en/natohq/topics_156338.htm [accessed: 19.03.2025].

Cyber attacks against European energy & utility companies, EnergiCERT, September 2022, https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf [accessed: 8.04.2025].

Cyber attacks traced to Russian military intelligence agency, Federal Ministry of the Interior and Community, 3.05.2024, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html [accessed: 19.03.2025].

Cybercrime, European Commission, 31.10.2024, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en [accessed: 19.03.2025].

Cybersecurity of Critical Sectors – Energy, ENISA, https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy [accessed: 8.04.2025].

Fake PAP report looks like cyberattack, says gov't official, Polska Agencja Prasowa, 31.05.2024, https://www.pap.pl/en/news/fake-pap-report-looks-cyberattack-says-govt-official [accessed: 19.03.2025].

Frequently asked questions on hybrid threats, Hybrid CoE, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [accessed: 19.03.2025].

Greenberg A., *A Brief History of Russian Hackers' Evolving False Flags*, Wired, 21.10.2019, https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/ [accessed: 19.03.2025].

Heightened security situation in Germany, Federal Ministry of the Interior and Community, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/ukrain/security_meldung.html [accessed: 19.03.2025].

Intelligence Outlook 2024, Danish Defence Intelligence Service, 22.01.2025, https://www.fe-ddis.dk/en/produkter/Risk_assessment/riskassessment/Intelligenceoutlook2024/ [accessed: 19.03.2025].

Jones S.G., *Russia's Shadow War Against the West*, Center for Strategic & International Studies, 18.03.2025, https://www.csis.org/analysis/russias-shadow-war-against-west [accessed: 19.03.2025].

Latvia mulls tightening security after recent TV propaganda hacks, LSM+, 20.05.2024, https://eng.lsm.lv/article/society/crime/20.05.2024-latvia-mulls-tightening-security-after-recent-tv-propaganda-hacks.a554618/ [accessed: 19.03.2025].

Lithuania supports the EU declaration condemning Ghostwriter malicious cyber activities and calls to use more political tools, Ministry of National Defence of the Republic of Lithuania, 23.09.2021, https://kam.lt/en/lithuania-supports-the-eu-declaration-condemning-ghostwriter-malicious-cyber-activities-and-calls-to-use-more-political-tools/ [accessed: 8.04.2025].

Mandiant Intelligence, *GhostWriter Update: Cyber Espionage Group UNC1151 Likely Conducts GhostWriter Influence Activity*, Mandiant, 28.04.2021, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf [accessed: 19.03.2025].

Mandiant Intelligence, *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant, 23.09.2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions [accessed: 19.03.2025].

Microsoft Digital Defense Report 2024, The foundations and new frontiers of cybersecurity, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 [accessed: 19.03.2025].

Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies, U.S. Department of Justice, 7.09.2023, https://www.justice.gov/archives/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware [accessed: 19.03.2025].

Raud M., *China and Cyber: Attitudes, Strategies, Organization*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf [accessed: 19.03.2025].

Roncone G. et al., *APT44: Unearthing Sandworm*, Mandiant, 17.04.2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [accessed: 19.03.2025].

Russian cyberattacks, Serwis Rzeczypospolitej Polskiej, 30.12.2022, https://www.gov.pl/web/special-services/russian-cyberattacks [accessed: 19.03.2025].

Russian National Charged with Ransomware Attacks Against Critical Infrastructure, U.S. Department of Justice, 16.05.2023, https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure [accessed: 19.03.2025].

Sancho D., *Understanding Hacktivists. The Overlap of Ideology and Cybercrime*, Trend Micro, 4.02.2025, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/understanding-hacktivists-the-overlap-of-ideology-and-cybercrime [accessed: 19.03.2025].

Sejm uznał Rosję za państwo wspierające terroryzm (Eng. The Sejm recognised Russia as a state supporting terrorism), Sejm of the Republic of Poland, 14.12.2022, https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC10C1258918007022FA [accessed: 8.04.2025].

Thales Cyber Threat Intelligence, *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*, Thales, 29.03.2023, https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point [accessed: 8.04.2025].

The attack against Danish, critical infrastructure, SektorCERT, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [accessed: 19.03.2025].

What is data exfiltration?, IBM, https://www.ibm.com/think/topics/data-exfiltration [accessed: 19.03.2025].

Wolert R., *RaaS group profile Hunters International*, CERT Orange, 28.10.2024, https://cert.orange.pl/wp-content/uploads/2024/11/CERTOPL_CTI_Hunters_International_en.pdf [accessed: 19.03.2025].

Other documents

2024 Annual Report, Republic of Latvia Constitution Protection Bureau, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf [accessed: 19.03.2025].

Annual Report on the activities of Latvian State Security Service (VDD) in 2022, https://vdd.gov.lv/uploads/materials/33/en/annual-report-2022.pdf [accessed: 19.03.2025].

Annual Report on the activities of Latvian State Security Service (VDD) in 2023, https://vdd.gov.lv/uploads/materials/37/en/annual-report-2023.pdf [accessed: 19.03.2025].

Annual report on the activities of Latvian State Security Service (VDD) in 2024, https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf [accessed: 19.03.2025].

Annual review 2022–2023, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf [accessed: 19.03.2025].

Annual review 2023–2024, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf [accessed: 19.03.2025].

China's Military Strategy, Ministry of National Defence of the People's Republic of China, 23.06.2021, http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html [accessed: 19.03.2025].

Cyber Security in Estonia 2023, Republic of Estonia Information System Authority, https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf [accessed: 19.03.2025].

Cyber security in Estonia 2025, Republic of Estonia Information System Authority, https://www.ria.ee/en/cyber-security-estonia-2025 [accessed: 19.03.2025].

Latvian Cybersecurity and CERT.LV Technical Activities Annual Report 2023, 26.07.2024, https://cert.lv/uploads/eng/Annual_Report_CERT-LV_2023.pdf [accessed: 19.03.2025].

National Threat Assessment 2023, https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf [accessed: 19.03.2025].

National Threat Assessment 2024, https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-EN-1.pdf [accessed: 19.03.2025].

Report on the state of Poland's cybersecurity in 2023, CSIRT GOV, https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf [accessed: 19.03.2025].

Report on the state of Poland's cybersecurity in 2024, in press.

Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok (Eng. Report of the Government Plenipotentiary for Cyber Security for 2023), Ministerstwo Cyfryzacji (Eng. Ministry of Digital Affairs), 11.04.2024, https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni [accessed: 8.04.2025].

Threat assessment: the cyber Threat against Denmark 2024, Centre for Cyber Security, September 2024, https://www.cfcs.dk/link/472c3cc8872446e59fa59eaf0f7ad945.aspx [accessed: 19.03.2025].

Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response, Brussels, 6.04.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:-52016JC0018 [accessed: 19.03.2025].

Monika Stodolnik

Internal Security Agency officer.

Contact: monika.e.stodolnik@gmail.com