EU Cybersecurity Regulation and Military Security: State-Sponsored Cyberattacks, Hybrid Warfare, and Europe's Future Defence Capability

@Cryptis, Cryptix Network
18/04/2026

Abstract

This paper examines European technology regulation from the perspective of military cybersecurity, state-sponsored cyberattacks, and hybrid warfare. The central argument is that Europe's future security depends not only on conventional military strength but also on its ability to defend digital infrastructure against hostile states. Cyberattacks against parliaments, political parties, ministries, energy systems, satellite communication, logistics companies, defence contractors, and public institutions show that cyberspace has become a domain of geopolitical conflict. Russia's cyber operations against Ukraine, Germany, Czechia, Poland, Lithuania, Slovakia, Sweden, and other European actors demonstrate that cyberattacks are no longer hypothetical threats. They are already part of modern military and political conflict.

The paper argues that the European Union faces a strategic dilemma. On the one hand, the EU must regulate digital systems to improve cybersecurity, protect critical infrastructure, fight crime, and create resilience. Laws such as the NIS2 Directive, the Cyber Resilience Act, the Digital Operational Resilience Act, and the Cyber Solidarity Act are important steps toward stronger European cyber defence. On the other hand, regulation must not weaken the technological foundations of cybersecurity itself. Strong encryption, secure software development, cryptographic research, open-source security tools, decentralized resilience, and a strong developer ecosystem are essential for military communication, intelligence protection, critical infrastructure defence, and technological sovereignty.

The main thesis is that overregulation, anti-encryption pressure, excessive compliance burdens, and legal uncertainty may reduce Europe's ability to defend itself against hostile cyber operations. If European regulation drives away cybersecurity talent, discourages cryptographic innovation, or makes secure and decentralized technologies harder to develop, Europe risks becoming dependent on foreign technologies for the protection of its own military and civilian infrastructure. In an era of cyberwarfare and hybrid attacks, this dependency is a strategic vulnerability.

---

1. Introduction

Security in the twenty-first century is no longer limited to tanks, aircraft, ships, missiles, and soldiers. Modern states also depend on digital networks, satellites, software, cloud

infrastructure, encrypted communication, artificial intelligence, industrial control systems, financial platforms, and secure data flows. A country can be weakened not only by a conventional military attack, but also by cyberattacks against its power grid, hospitals, transport systems, government networks, military logistics, elections, and media environment.

This development is especially relevant for Europe. Since Russia's full-scale invasion of Ukraine in February 2022, cyber operations have become an obvious part of the wider security conflict between Russia and the West. Cyberattacks have targeted Ukrainian critical infrastructure, satellite communication systems, government institutions, logistics networks, media, and military-related systems. At the same time, European countries such as Germany and Czechia have publicly attributed malicious cyber campaigns to Russian state-linked actors, especially APT28, which is associated with Russia's military intelligence service GRU.

Germany provides a particularly important example. The German Bundestag was targeted in a major cyberattack in 2015, which the EU later linked to APT28. In 2024, Germany publicly attributed a cyber campaign against the Social Democratic Party and other targets to APT28. German security authorities have also warned that Russian cyber actors used compromised network devices to hide their attack infrastructure and gather information related to Germany's political strategy and military support for Ukraine. These examples show that cyberattacks are not abstract technical incidents. They are instruments of state power, espionage, destabilization, and military preparation.

The European Union has responded to the growing cyber threat with several regulatory instruments. The NIS2 Directive aims to raise cybersecurity standards across critical sectors. The Cyber Resilience Act introduces security requirements for digital products. The Digital Operational Resilience Act strengthens the financial sector's ability to withstand ICT disruptions. The Cyber Solidarity Act is intended to improve EU-level detection, preparedness, and response to large-scale cyber incidents. These measures show that the EU understands cybersecurity as a strategic issue.

However, this paper argues that Europe must avoid a regulatory contradiction. Cybersecurity regulation is necessary, but it must not weaken the very technologies and communities that make cybersecurity possible. Strong encryption, cryptographic research, open-source security tools, secure software development, decentralized networks, and privacy-preserving infrastructure are essential for national and military security. If European regulation creates pressure to weaken encryption, imposes excessive compliance costs on small security companies, or treats developers as risks rather than strategic assets, Europe may damage its own cyber-defence capability.

The research question of this paper is:

How does EU technology regulation affect Europe's ability to defend itself against state-sponsored cyberattacks, military cyber operations, and hybrid warfare?

The paper argues that Europe needs a security-oriented but capability-preserving regulatory model. The EU should strengthen cyber resilience, regulate critical sectors, and improve cooperation against hostile states. At the same time, it must protect encryption, support technical expertise, invest in cyber-defence capabilities, and prevent the loss of cybersecurity talent. In modern conflict, a state that cannot defend its networks cannot fully defend its territory, economy, or democracy.

2. Cybersecurity as a Military and Geopolitical Issue

Cybersecurity is often discussed as an economic or administrative issue, but it is increasingly a military and geopolitical issue. A hostile state can use cyber operations to steal intelligence, disrupt infrastructure, prepare the battlefield, weaken political trust, influence elections, and support conventional military operations. Cyberattacks can be used before, during, and after military conflict.

There are several reasons why cybersecurity has become central to national defence.

First, modern military systems depend on digital technology. Command-and-control networks, encrypted radios, satellite communication, drones, logistics platforms, intelligence systems, targeting tools, and defence procurement all rely on software and data. If these systems are hacked, manipulated, or disrupted, military effectiveness is reduced.

Second, civilian infrastructure is connected to military readiness. Railways, ports, energy grids, telecommunications, hospitals, and financial systems are not purely civilian in a crisis. They support troop movement, defence production, medical care, public order, and government continuity. A cyberattack against civilian infrastructure can therefore have military effects.

Third, cyber operations can remain below the threshold of open war. A state may attack another state's networks without sending troops across a border. This makes cyber operations attractive for hybrid warfare because they create damage, fear, and instability while leaving room for denial.

Fourth, cyberattacks can be combined with disinformation. A hostile state may hack institutions, leak selected information, spread manipulated narratives, use deepfakes, and undermine trust in elections or public authorities. This is not only a technical problem. It is a political security problem.

Fifth, cybersecurity determines technological sovereignty. If Europe depends on foreign cloud providers, foreign encryption systems, foreign cybersecurity tools, and foreign software supply chains, it becomes strategically vulnerable. In a crisis, dependency can limit political and military autonomy.

For these reasons, cybersecurity should be understood as part of national defence. Europe's ability to resist cyberattacks is part of its ability to resist military and political coercion.

3. State-Sponsored Cyberattacks Against Europe

3.1 Russia's Cyber Operations Against Ukraine

Ukraine has become one of the clearest examples of cyberwarfare in modern conflict. Russian cyber operations against Ukraine did not begin in 2022. They were visible years earlier, including attacks against Ukrainian power infrastructure. In 2015, Ukrainian electricity

distribution companies were attacked, causing power outages. This event became one of the first widely known cases of a cyberattack causing a physical disruption to an electricity grid.

In 2017, the NotPetya malware attack initially targeted Ukraine but spread globally, causing billions of dollars in damage across Europe, Asia, and the Americas. The United States publicly described NotPetya as a destructive and costly cyberattack launched by the Russian military. This case is important because it shows that a cyber operation aimed at one country can spill over into the global economy.

In February 2022, shortly before Russia's full-scale invasion of Ukraine, a cyberattack targeted the KA-SAT satellite network operated by Viasat. The European Union stated that the attack took place one hour before the invasion and caused communication outages affecting Ukrainian authorities, businesses, users, and several EU member states. This is a clear example of cyber operations being integrated with conventional military aggression. Disrupting satellite communication can support military operations by weakening command, control, and coordination.

These examples show that cyberattacks are not only about data theft. They can affect electricity, logistics, communication, public administration, and military readiness. Ukraine demonstrates that cyberwarfare is part of modern war.

3.2 Russian Cyberattacks Against Germany

Germany has also been a target of Russian-linked cyber operations. One of the most important cases was the 2015 cyberattack against the German Bundestag. The EU later imposed sanctions on actors responsible for APT28 attacks targeting the German Federal Parliament. The Bundestag attack was significant because it targeted a central democratic institution of a major European state.

In 2024, Germany publicly attributed a cyber campaign against email accounts of the Social Democratic Party executive to APT28. The EU condemned the campaign and stated that the same threat actor had also targeted institutions and entities in Poland, Lithuania, Slovakia, Sweden, and Czechia. According to the EU, this pattern showed Russia's irresponsible behaviour in cyberspace, including targeting democratic institutions, government entities, and critical infrastructure providers.

German authorities have also warned about APT28 using compromised routers and network devices to hide its attack infrastructure. According to the German domestic intelligence service, APT28 used such infrastructure for attacks against German targets. The focus included information about Germany's political strategy in relation to Russia and military support deliveries for Ukraine. This is especially important for the argument of this paper because it shows that cyber operations against Germany are connected to military and geopolitical questions.

These attacks are not random criminal acts. They are linked to intelligence gathering, political influence, and pressure on Germany's support for Ukraine. From a military-security perspective, this means Germany is already involved in a cyber conflict environment even without being in a conventional war with Russia.

3.3 Cyberattacks Against Logistics and Defence-Related Systems

Military support for Ukraine depends on logistics, transport, defence companies, technology providers, and government coordination. These networks are attractive targets for Russian intelligence services. Cyberattacks against logistics companies or defence-related technology firms can reveal supply routes, delay support, identify vulnerabilities, or support sabotage.

This means that cybersecurity is not only needed inside ministries or military bases. It is needed across the entire defence ecosystem. Private companies that manufacture components, transport equipment, maintain software, provide cloud services, or handle communications can become targets. In modern conflict, the boundary between civilian and military infrastructure becomes blurred.

This creates a major challenge for European regulation. Cyber defence cannot be limited to military institutions. It must include public-private cooperation, supply-chain security, secure software development, incident reporting, and resilience planning across critical sectors. Laws such as NIS2 and the Cyber Resilience Act are therefore important, but they must be implemented in a way that improves real security rather than merely creating paperwork.

3.4 Cyberattacks and Democratic Destabilization

State-sponsored cyber operations are often combined with disinformation and influence campaigns. Hacking political parties, leaking information, manipulating narratives, using deepfakes, and attacking election infrastructure can weaken public trust. This is a form of hybrid warfare because it targets the political stability of a society rather than only its military forces.

The goal is not always to destroy systems. Sometimes the goal is to create uncertainty. If citizens no longer trust elections, parties, media, or public institutions, a hostile state gains strategic advantage. Cybersecurity therefore protects democracy as well as infrastructure.

For Europe, this means that cyber defence must include the protection of democratic processes. Political parties, parliaments, election systems, media organizations, and civil society groups need strong cybersecurity support. They are strategic targets even if they are not traditional military institutions.

---

4. NATO, the EU, and Cyber Defence

NATO has recognized cyberspace as a military domain. In 2014, NATO leaders agreed that a cyberattack could trigger Article 5, the collective defence clause of the North Atlantic Treaty. In 2016, NATO recognized cyberspace as an operational domain alongside land, sea, and air. This means that cyberattacks can be relevant to collective defence, deterrence, and military planning.

This has important consequences. If a significant cyberattack against a NATO member state can be considered an armed attack, then cybersecurity becomes part of deterrence. A hostile state must know that a cyberattack could produce political, economic, cyber, or even military consequences. However, deterrence only works if member states have credible cyber capabilities and resilience.

The EU plays a different but complementary role. While NATO focuses on collective defence and military deterrence, the EU has strong regulatory and economic tools. The EU can set cybersecurity standards, regulate critical sectors, support information sharing, impose sanctions, fund cyber-resilience projects, and coordinate response mechanisms. This makes the EU important for building the civilian and industrial foundations of cyber defence.

However, Europe's security problem is not solved simply by creating more rules. Rules must be matched by capabilities. Member states need trained cyber professionals, secure networks, strong encryption, intelligence sharing, incident response teams, secure procurement, and cooperation with private technology companies. Cyber defence depends on people and tools, not only legal frameworks.

---

5. The EU Cybersecurity Regulatory Framework

5.1 NIS2: Protecting Critical Sectors

The NIS2 Directive is one of the most important EU cybersecurity laws. It aims to create a high common level of cybersecurity across the Union and applies to many essential and important sectors, including energy, transport, banking, health, drinking water, digital infrastructure, public administration, space, ICT service management, and manufacturing.

From a military-security perspective, NIS2 is important because many of these sectors are critical in a crisis. Energy, transport, communication, health, and digital infrastructure support both civilian life and military readiness. A cyberattack against these sectors could weaken a country's ability to respond to a security crisis.

NIS2 requires risk management measures, incident reporting, supply-chain security, and cooperation with authorities. This can improve resilience. However, the implementation must focus on real cybersecurity outcomes. If companies treat NIS2 only as a paperwork obligation, it will not provide meaningful defence against state-sponsored attackers.

5.2 Cyber Resilience Act: Securing Digital Products

The Cyber Resilience Act introduces cybersecurity requirements for products with digital elements. This is relevant because insecure software and hardware can become entry points for hostile actors. Routers, cameras, industrial devices, operating systems, software libraries, and connected products can all be exploited.

From a national security perspective, product security is essential. A state-sponsored attacker does not need to attack a ministry directly if it can compromise a widely used supplier or device. Therefore, improving the baseline security of digital products is a strategic necessity.

However, the Cyber Resilience Act must protect open-source security work. Many critical security tools and libraries are maintained by open-source communities. If liability rules are too broad, developers may stop publishing or maintaining code. That would weaken the entire cybersecurity ecosystem.

5.3 DORA: Financial Cyber Resilience

The Digital Operational Resilience Act strengthens the financial sector's ability to withstand ICT disruptions. Financial systems are critical infrastructure. A major cyberattack against payment systems, banks, or financial market infrastructure could create economic panic and affect national stability.

DORA is important because it treats ICT risk as a systemic issue. It includes incident reporting, resilience testing, third-party risk management, and oversight of critical ICT providers. This is especially important because many financial institutions depend on external cloud and software providers.

However, DORA also shows the problem of dependency. If European financial institutions rely heavily on a small number of foreign cloud providers, Europe's financial resilience partly depends on actors outside its own political control. Regulation can manage this risk, but Europe also needs domestic technological capability.

5.4 Cyber Solidarity Act: Collective European Response

The Cyber Solidarity Act aims to improve EU-level detection, preparedness, and response to large-scale cyber incidents. This is important because cyberattacks can spread across borders. A major incident in one member state may affect others through shared infrastructure, supply chains, or digital services.

The Act reflects the idea that cyber defence must be collective. Smaller member states may not have enough resources to respond to advanced state-sponsored attacks alone. EU-level cyber hubs, information sharing, and coordinated support can increase resilience.

However, collective response requires technical capacity. Information sharing is only useful if authorities, companies, and security teams can act quickly. Europe therefore needs both legal coordination and operational cyber expertise.

---

6. Encryption as a Military and National Security Asset

Encryption is the foundation of secure communication. It protects military orders, diplomatic messages, intelligence data, government communication, financial transactions, medical records, and private conversations. Without strong encryption, no modern state can securely operate.

End-to-end encryption is especially important because it ensures that only the sender and recipient can read the content of a message. This protects communication even if service providers are compromised. It is essential not only for citizens but also for journalists, soldiers, government officials, lawyers, companies, and activists.

The EU debate around the proposed Regulation to prevent and combat child sexual abuse online, often called "Chat Control" by critics, creates a major security question. Protecting children is a legitimate and urgent goal. However, if detection measures require scanning private communications or weakening encrypted systems, they can create cybersecurity risks.

From a military and state-security perspective, weakening encryption is dangerous. A vulnerability created for law enforcement can also be discovered or abused by hostile states. A scanning infrastructure built for one purpose can later be expanded or compromised. If European communication tools become less trustworthy, government officials, defence companies, journalists, and citizens may become easier targets.

This is the key point: strong encryption is not a problem for security. It is a requirement for security. Law enforcement needs should be addressed through targeted investigations, better digital forensics, judicially controlled device access, stronger international cooperation, and better resources for child-protection units. But Europe should not create systemic weaknesses in communication infrastructure.

A Europe facing Russian cyber operations, Chinese cyber espionage, ransomware groups, and hybrid warfare cannot afford weak encryption.

---

7. The Risk of Overregulation for Cyber Defence

The EU must regulate cybersecurity, but it must avoid overregulation that damages cyber capability. There are four major risks.

7.1 Talent Loss

Cybersecurity depends on highly skilled developers, cryptographers, malware analysts, reverse engineers, incident responders, and security researchers. These experts are globally mobile. If Europe creates legal uncertainty, high compliance costs, or hostility toward privacy-enhancing technologies, experts may move to the United States, Switzerland, Singapore, Israel, or other countries.

This would weaken Europe’s defence capability. The same people who build secure protocols, encryption libraries, detection tools, and decentralized systems are also needed for military and government cybersecurity. Losing them is not just an economic problem. It is a strategic security problem.

7.2 Weakening Open-Source Security

Modern cybersecurity depends heavily on open-source software. Many encryption libraries, operating system components, security tools, and infrastructure projects are open source. If EU regulation creates unclear liability for open-source maintainers, developers may stop contributing.

This could reduce transparency and security. Open-source software allows vulnerabilities to be discovered, audited, and fixed by a global community. Weakening this ecosystem would make Europe more vulnerable.

7.3 Compliance Instead of Real Security

Another risk is that companies focus on compliance documents instead of real security. State-sponsored attackers do not care whether a company has filled out forms. They exploit vulnerabilities, weak passwords, unpatched systems, insecure devices, and human mistakes.

Cybersecurity regulation must therefore focus on practical outcomes: patching, monitoring, backup systems, incident response, access controls, segmentation, encryption, supply-chain security, and testing. Paper compliance without technical security is not defence.

7.4 Centralization and Dependency

Regulation often favours large companies because they can afford compliance departments. Small security companies and start-ups may struggle. This can lead to market centralization. In cybersecurity, centralization can create systemic risk because a few providers become high-value targets.

Europe must also avoid excessive dependency on non-European cloud, software, and security providers. Foreign technology can be useful, but critical military and government infrastructure should not depend entirely on external actors. Sovereignty requires domestic capability.

---

8. Blockchain, Decentralization, and Military Resilience

Although blockchain and decentralization are often associated with cryptocurrency, they also have possible security relevance. Distributed systems can reduce single points of failure. Cryptographic ledgers can support tamper-resistant records, supply-chain verification, identity systems, and audit trails. Decentralized communication networks can be more resilient against censorship and disruption.

In a military or crisis context, resilience matters. If centralized communication or identity systems are disrupted, decentralized alternatives may help maintain coordination. If supply chains are targeted, cryptographic verification can help prove authenticity and traceability. If data integrity is critical, tamper-resistant logs can support trust.

This does not mean blockchain is a solution to every problem. Many blockchain projects are speculative, inefficient, or insecure. Smart contracts can be hacked. Crypto markets can enable fraud and money laundering. Therefore, regulation such as MiCA and AML rules has a legitimate role.

However, Europe should not treat all decentralized technologies only as financial risks. Some of the underlying expertise — cryptography, distributed systems, adversarial thinking, secure protocols, key management — is strategically relevant for cybersecurity and defence. Driving this expertise away would weaken Europe’s technical base.

---

9. Digital Sovereignty and Strategic Dependency

Digital sovereignty means that Europe can build, control, and secure essential digital infrastructure without excessive dependence on external powers. This does not mean isolation. Europe should cooperate with allies and international partners. But cooperation is different from dependency.

Strategic dependency becomes dangerous when Europe relies on foreign providers for critical cloud infrastructure, cybersecurity products, encrypted communication, identity systems, military software, or supply-chain security. In a geopolitical crisis, access, trust, legal jurisdiction, and political pressure can become serious problems.

The Draghi report on European competitiveness and the EU's Digital Decade reports show that Europe already faces challenges in digital technologies, productivity, semiconductors, cloud, AI, and digital skills. If Europe also loses cybersecurity talent through poor regulation, the problem becomes worse.

A serious European defence strategy must therefore include cybersecurity industrial policy. Europe needs investment in:

- cryptography and post-quantum cryptography;
- secure communication systems;
- military cyber capabilities;
- industrial control system security;
- secure cloud and data infrastructure;
- malware analysis and threat intelligence;
- secure software supply chains;
- open-source security maintenance;
- cyber education and talent retention.

Cybersecurity is not an optional supplement to defence policy. It is part of defence policy.

---

10. Policy Recommendations

10.1 Treat Cybersecurity as Defence Infrastructure

The EU and its member states should treat cybersecurity as part of national and European defence. Critical infrastructure, military logistics, public administration, defence companies, and democratic institutions should receive stronger cyber protection and support.

10.2 Protect Strong Encryption

Europe should explicitly protect strong end-to-end encryption. Law enforcement goals must not create systemic weaknesses that hostile states can exploit. Strong encryption is necessary for military communication, government secrecy, business security, and citizen privacy.

10.3 Build a European Cyber Defence Talent Strategy

Europe needs to train, attract, and retain cybersecurity experts. This includes university programs, vocational training, research funding, start-up support, scholarships, and pathways between civilian cybersecurity and public defence institutions.

10.4 Protect Open-Source Security Research

The EU should create clear legal protections for good-faith security researchers and open-source maintainers. Responsible vulnerability disclosure, cryptographic research, and security tool development should be encouraged, not punished.

10.5 Focus Regulation on Real Security Outcomes

NIS2, DORA, the Cyber Resilience Act, and other frameworks should be implemented in a way that rewards actual security improvements. Regulators should avoid turning cybersecurity into a paperwork exercise.

10.6 Strengthen Public-Private Cyber Cooperation

Most critical infrastructure is operated by private companies. Military cyber defence therefore requires cooperation with industry. Governments, companies, universities, and researchers should share threat intelligence and coordinate incident response.

10.7 Reduce Dependency on External Providers

Europe should develop more domestic capability in secure cloud services, encryption, cybersecurity tools, chip security, and critical software. Foreign allies remain important, but Europe should not depend entirely on external providers for critical infrastructure and defence systems.

10.8 Include Technical Experts in Lawmaking

Cybersecurity laws should be developed with engineers, cryptographers, incident responders, defence experts, open-source maintainers, and security researchers. Technically unrealistic laws can create vulnerabilities instead of solving problems.

---

11. Conclusion

Cybersecurity has become a central dimension of military and national security. Russia’s cyber operations against Ukraine, Germany, and other European countries show that state-sponsored cyberattacks are already part of modern conflict. Attacks against parliaments, political parties, satellite networks, critical infrastructure, logistics systems, and democratic processes demonstrate that cyberspace is a battlefield of hybrid warfare.

The European Union is right to strengthen cybersecurity regulation. NIS2, the Cyber Resilience Act, DORA, and the Cyber Solidarity Act can improve resilience if they are implemented effectively. However, Europe must avoid a dangerous contradiction. It cannot defend itself in cyberspace while weakening the technologies and communities that make cyber defence possible.

Strong encryption, open-source security tools, cryptographic research, decentralized resilience, and a strong cybersecurity talent base are strategic assets. They are not only economic resources. They are part of Europe's defence capability. If regulation pushes developers away, discourages security research, weakens encryption, or creates excessive compliance burdens, Europe may reduce its own ability to resist hostile states.

The future of European security will depend on whether Europe can become not only a regulator of digital technology but also a builder and defender of secure digital infrastructure. In an age of cyberwarfare, military conflict, disinformation, sabotage, and attacks on critical infrastructure, cybersecurity is no longer optional. It is a condition of sovereignty.

If Europe fails to develop and protect its own cyber capabilities, it risks becoming dependent on external powers for the security of its own governments, militaries, economies, and citizens. That dependency would not make Europe safer. It would make Europe more vulnerable.

References

Associated Press. (2026). *Germany summons Russian ambassador over alleged sabotage, cyberattacks and election interference*. https://apnews.com/article/germany-russia-sabotage-cyberattacks-2a2a2e03ba383a7876a71fd4f6514629

Bundesamt für Verfassungsschutz. (2024). *Sicherheitshinweis zu Cyberaktivitäten von APT 28*. https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2024/2024-02-28-joint-cyber-security-advisory.html

Council of the European Union. (2022). *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union*. https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

Council of the European Union. (2024). *Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation*. https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/

Council of the European Union. (2024). *Cyber resilience act: Council adopts new law on security requirements for digital products*. https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/

Cybersecurity and Infrastructure Security Agency. (2021). *Cyber-Attack Against Ukrainian Critical Infrastructure*. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

ENISA. (2025). *ENISA Threat Landscape 2025*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

European Banking Authority. (2026). *Digital Operational Resilience Act*. https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act

European Commission. (2024). *The future of European competitiveness: Draghi report*. https://commission.europa.eu/topics/competitiveness/draghi-report_en

European Commission. (2025). *Cyber Resilience Act*. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. (2025). *EU Cyber Solidarity Act*. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

European Commission. (2025). *State of the Digital Decade 2025 report*. https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report

European Commission. (2026). *NIS2 Directive: securing network and information systems*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Parliament. (2023). *Child sexual abuse online: effective measures, no mass surveillance*. https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass-surveillance

MITRE ATT&CK. (2026). *Sandworm Team*. https://attack.mitre.org/groups/G0034/

NATO. (2018). *Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference*. https://www.nato.int/en/news-and-events/events/transcripts/2018/05/15/speech

NATO. (2025). *Collective defence and Article 5*. https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5

The White House. (2018). *Statement from the Press Secretary on NotPetya*. https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/

U.S. Department of Defense. (2023). *2023 Department of Defense Cyber Strategy Summary*. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_CYBER_STRATEGY_SUMMARY.PDF