BATHMUN

Conference 2025

EC Study Guide

Preparing the European Union for Cyberspace Threats

Table of Contents

Table of Contents

Message from the Chairs

Esteemed Members of the European Council,
First and foremost, we wish you all a very warm welcome to BATHMUN 2025, and to the European Council itself! We hope you are all as excited to be debating on our committee as we are to be chairing it for what promises to be a brilliant weekend in Bath

As delegates on an advanced level committee, we expect that you will all have a strong grasp of the topic and the committee as a whole, so whilst this study guide is a great starting point for debate (and you should read it in full), we strongly encourage you do further research in order to get the most out of the weekend. Beyond debating this weekend, we encourage you to make the most of your time in the beautiful and historic city of Bath. Where possible you should use your free time to explore the many brilliant sights of the city, and especially visit its wealth of pubs and cafes as you form friendships with your fellow delegates.

We cannot wait to meet you all soon,
Warmest Regards,

Sam, Arya, and Jubilee

Introduction to the Dais

Sam Fuller
President

Hello everyone, I'm Sam, and I will be the President of the European Council for BathMUN 2026. I'm a Physics graduate from the University of Southampton, currently studying for a Post Graduate Certificate of Education in Secondary School Science at the same university. This will be my fourth year doing MUN, third time doing BathMUN, and second time chairing BathMUN; I'm very much looking forward to it. Outside of MUN, my hobbies include being an Explorer Scout leader, playing Orks and Black Templars in Warhammer 40,000 (and Kharadron Overlords in Age of Sigmar), hiking up mountains, and in what little time remains playing action-adventure RPGs on my PC. I look forward to meeting you all in Bath, seeing you all debate, and eventually enjoying a well-earned drink at the socials!

Arya Sharma
Vice President

I'm Arya, a fourth-year European Studies student at KCL, from East London. I got indoctrinated into Model UN in my first year at university, having been to various conferences as a delegate and chair, but haven't managed to escape just yet.

I love sports, especially handball and football, being a lifelong Dagenham & Redbridge fan. I also have a passion for languages and foreign cultures, knowing Spanish and currently learning Catalan, which links to my favourite part of MUN - meeting so many different people with cool and diverse perspectives to learn from!

I'm looking forward to getting to know you all :3

Jubilee Kothari
Vice President

Hello everyone, I'm Jubilee, and I'll be serving as Vice President of the European Council at BathMUN 2025. I'm going into my second year of Biological and Medicinal Chemistry at the University of Nottingham, and this will be my second year in MUN. I first joined out of curiosity, but quickly stayed for the fast-paced debates, the diplomacy, and the chance to engage with global issues in a meaningful way. Outside of MUN, I'm passionate about healthcare and the pharmaceutical world, particularly how science translates into real-world impact. I'm also a qualified yoga teacher, and when I'm not on the mat, I'm usually spending time with my seven dogs (yes, seven!). I'm really looking forward to meeting you all in Bath, seeing the debates unfold, and enjoying the socials afterwards!

Introduction to the Committee

The European Council (EC) is the principal of the four main institutions of the European Union (EU), responsible for determining the EU's political direction, without getting tied up in the details of law-making, which are left to its sister institutions: the European Parliament, the Council of Europe, and the European Commission (European Union, 2025b). It is composed of the heads of state or government of all EU members in order to promote high-level political co-operation between EU members (European Union, 2025a).

History of the Committee

Table 1: Timeline of Key Events in the History of the European Council and the European Union.

Year	Event
1950	The French foreign minister Robert Schuman announced the creation of a European Coal and Steel Community (ECSC), which would become the foundation of the European Union (European Council, 2025b).
1952	The Paris Treaty formally established the ECSC as a common market for coal and steel, and was the first founding treaty of the European Community, finally expiring in 2002 (European Council, 2025b).
1958	The European Economic Community (EEC) was established by the Rome treaties, holding its first meeting on 25th January 1958 (European Council, 2025b).
1974	The European Council was created. Its initial purpose was as an informal forum for discussions between heads of state or government, to resolve international issues smoothly. Its first meeting was held in March of the following year in Dublin (European Council, 2025b).

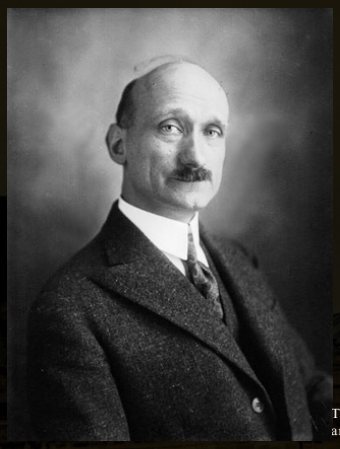

Table 1: Timeline of Key Events in the History of the European Council and the European Union.

Year	Event
1985	The Schengen Agreement on the elimination of border controls was signed between Belgium, Germany, France, Luxembourg, and the Netherlands. The agreement gradually allowed people to travel internally through Europe without needing their passports to be checked at every border (European Council, 2025b). The EC adopted the EU flag as the official logo of the European Communities (European Council, 2025b).
1987	On 1st July the Single European Act (SEA) was signed, establishing the single market for the free movement of goods, persons, services and capital. It was also the legal basis for the EC (European Council, 2025b).
1993	The Maastricht Treaty came into force, formally establishing the European Union as a body. As well as creating the economic and monetary union, it also established the concepts of common foreign and security policy, and co-operation in justice and home affairs (European Council, 2025b).
1996	The European Council moved from biannual to quarterly meetings (European Council, 2025b).
1999	On 1st May the Amsterdam Treaty was signed, integrating the Schengen Agreement into EU Law (European Council, 2025b).
2002	The euro entered circulation (European Council, 2025b).

Figure 2: Official Portrait of Herman Van Rompuy from his time as President of the European Council (Hendryckx, 2012).

Year	Event
2009	Herman Van Rompuy was unanimously elected as the first permanent President of the European Council (European Council, 2025b). Later in this year the Treaty of Lisbon came into force, creating the European Council as a fully-fledged institution of the EU, instead of its previous existence as an informal body (European Council, 2025b).
2020	The United Kingdom became the first nation to withdraw from the European Union, following a national referendum to leave held on 23rd June 2016 (European Council, 2025b).
2024	António Costa was elected president of the European Council. (European Council, 2025b)

Structure and Function of the EC

Figure 3: Current Membership of the European Council (European Council, 2025a).

European Council Conclusions

The European Council fulfills its role in determining the EU's political direction, and its short and long term priorities, by adopting conclusions at each meeting. EC conclusions are used to identify concerning issues for the EU, and outline what action should be taken, or what goals should be attained (European Council, 2025c).

Strategic Agenda

Every five years, the European Council agrees a strategic agenda for the next five years, which guide how all of the EU's institutions - including the EC itself - will work for the next five years (European Council, 2024).

At its meeting on 27th June 2024, the EC agreed its current strategic agenda, with the aim of facing up to the challenges of Russia's aggression, the unstable situation of the Middle East, fighting climate change, and mitigating the impact of the COVID-19 pandemic. It is structured around three pillars:

- A free and democratic Europe
- A strong and secure Europe
- A prosperous and competitive Europe (European Council, 2024)

Specialised Rules of Procedure

Article 4 - Composition of the European Council

The European Council consists of the Heads of State or Government of the Member States, together with the President of the European Council and the President of the European Commission (2009/882/EU).

Article 6 - Adoption of Positions, Decisions, and Quorum

The Quorum of the European Council is set to two-thirds of its members (2009/882/EU). Procedural decisions taken by the European Council will be adopted by a simple majority (2009/882/EU).

Voting Procedure

Due to this topic falling under the EU's Common Security and Defence Policy, any resolution voted on will have to be passed unanimously, meaning that there must be no votes against the resolution for it to pass. In practice, this means that each country possesses veto power.

Topic Introduction

In the 21st century, cyberspace has become a central pillar of the European Union's (EU) economic growth, social infrastructure, and political governance. Digitalisation has transformed how industries operate, how governments deliver services, and how individuals interact across borders. The EU's Digital Decade Policy Programme 2030 highlighted that digital technologies are now key to competition, resilience, and function, all of which are required to live in a democratic society (European Commission, 2025b). This interconnectivity has brought immense benefits, from increased efficiency and innovation to enhanced global competitiveness. Yet, it has also created new and complex vulnerabilities to aggressive cyber activities (European Commission, 2022).

Europe's "attack surface" now spans millions of connected devices, cloud infrastructures, industrial control systems, and communication platforms. The speed, anonymity, and cross-border nature of cyberattacks could cascade from a single entry point to entire sectors and regions within a matter of hours (ENISA, 2023). Recent incidents have shown the scale of the threat. Ransomware campaigns have crippled hospitals and public transport (NHS England, 2017); state-sponsored operations have sought to influence elections and undermine democratic processes (European External Action Service, 2022); and large-scale data breaches have targeted critical infrastructure such as power grids, water distribution systems, and financial institutions, amongst many others (European Court of Auditors et al., 2019).

The minds behind these threats are no longer limited to lone hackers or small criminal groups. They include white collar, well-resourced cyber gangs and state-linked entities with geopolitical agendas. Europol's Internet Organised Crime Threat Assessment reports the growing cleverness of transnational ransomware networks (Europol, 2023), while researchers argue that state-sponsored cyber operations increasingly form part of broader strategic competition (Rid and Buchanan, 2015). For EU member states, this presents a shared challenge: how to secure heavily interconnected systems while also respecting national sovereignty, protecting democratic freedoms, and ensuring political, economic, and societal resilience for the decades to come (Once Upon a Time in... Europe's Digital Decade, 2025).

Definitions

Attack Surface and Attack Vectors
Attack vectors are paths, methods, or scenarios that can be exploited to break into IT systems. The attack surface is the sum of all these points.

Denial-of-service (DoS) Attacks
A cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to intended users. This is typically done by flooding the target with superfluous requests to overload systems.

Distributed Denial-of-Service (DDoS) Attacks
In distributed denial-of-service (DDoS) attacks the incoming traffic originates from many different sources.

Doxing
Searching for and publishing private or identifying information about a particular individual on the internet.

Internet of things (IoT)
The internet of things refers to physical objects that are embedded with sensors, processing ability, and software that connect and exchange data with other devices and systems over the internet or other communication networks.

Open source
In software this is source code which is publicly accessible for anyone to use, study, modify, and distribute.

Phishing
A type of online fraud where criminals impersonate trusted companies or individuals to trick people into revealing sensitive information.

Social Engineering
The use of psychological influence of people into performing actions or divulging confidential information. Phishing is a common form of social engineering.

Evolution of the Threat Landscape

In the early 2000s, most EU cyber concerns centred on economic crimes, including phishing scams, credit card fraud, and intellectual property theft. These were usually opportunistic, financially motivated attacks by individuals or small groups (European Commission et al., 2001; European Union, 2004). However, over the past two decades, the threat environment has shifted rapidly towards highly coordinated, well-funded campaigns with broader objectives. These include destabilising governments, undermining public trust, and disrupting critical infrastructure, as evidenced by the rise of state-sponsored cyber operations and hybrid threats documented in recent EU policy reports (European External Action Service, 2022; Europol, 2023).

Timeline

Table 2: Timeline of major cybersecurity incidents in Europe.

Year	Incident
2007	Estonia Cyberattacks: A wave of distributed denial-of-service (DDoS) attacks targeted Estonia's government ministries, banks, and media outlets. Western policy circles later linked these attacks to actors sympathetic to Russia, making it one of the first large-scale cyber campaigns against a sovereign state (NATO Strategic Communication Centre of Excellence et al., 2007).
2015	Ukraine Power Grid Attack: Although outside the EU, the incident brought to light the vulnerability of industrial control systems. Following the attack, around 230,000 Ukrainian people were left without power for several hours, which served as a warning for European critical infrastructure (Lee, Assante and Conway, 2016; CISA, 2016).
2017	WannaCry Ransomware: A global ransomware campaign exploited a Microsoft Windows vulnerability, disrupting companies across Europe and severely affecting hospitals in the UK's NHS (NHS England, 2023). NotPetya Malware: Initially appearing as ransomware, it was later identified as a destructive malware campaign. Several Western governments attributed it to Russian military intelligence, it caused billions in losses, severely impacting EU logistics and manufacturing (Greenberg, 2018).

Year	Incident
2019 - pres.	Election Interference Campaigns: Targeted hacking operations and coordinated disinformation efforts have attempted to influence voter behaviour and distrust in democratic processes within the EU (European Commission, 2019).

Current Situation

Modern Cyberthreats

State-sponsored Cyber Operations

These often form a part of broader geopolitical strategies, which typically involve espionage, election interference, and sabotage of critical infrastructure. This may be carried out by nation-states, or on their behalf by non-state actors. These operations aim to disrupt systems, spread mistrust and utilise strategic influence (Rid and Buchanan, 2015).

Organised Cybercrime

Transnational criminal groups have developed increasingly sophisticated ransomware and fraud networks. These target high-value sectors including healthcare, finance, and transportation, where disruption can yield significant financial gain or systemic disruption (Europol, 2023).

Hybrid Threats

A mix of cyberattacks with other tools such as disinformation, propaganda, and economic pressure, etc. For example, cyberattacks on media outlets may be combined with social media disinformation campaigns designed to alter narratives and destabilise political systems during elections (European External Action Service, 2022).

This phenomenon is known as Foreign Information Manipulation and Interference (FMI), with Russia being the most active actor as identified by the EU, mostly targeting Ukraine, France, Germany, Poland, and the Baltic countries (Olejnik, 2025).

Current Cyberspace Vulnerabilities

Despite its advances in policy and infrastructure, the EU continues to face vulnerabilities. These become painfully more evident when cyberattacks intersect with public safety, economic security, and national defence.

Table 3: Current cyberspace vulnerabilities and the risks they pose.

Vulnerability	Risk
Uneven Security Measures Across Member States	Wealthier member states often have the resources to invest in advanced cyber defences, while smaller or less resourced members may rely on outdated systems. This imbalance creates exploitable "weak links" that attackers can use to infiltrate the EU's wider digital ecosystem (Directive (EU) 2022/2555; ENISA, 2024).
Crucial Infrastructure Exposure	Energy grids, transport networks, water systems, and healthcare facilities across Europe are increasingly connected to the internet. However, insufficient safeguards against advanced persistent threats (APTs) leave such critical systems highly vulnerable to sabotage. Events such as the 2015 Ukraine power grid attack have underscored the risks of cyber sabotage against industrial control systems (Lee, Assante and Conway, 2016; CISA, 2016).
Supply Chain Weaknesses	A compromise at the level of a subcontractor, ICT vendor, or even an open-source code library can provide attackers with access to multiple EU institutions and private operators simultaneously, amplifying the scale of disruption (ENISA, 2024).
Human Factor Risks	Technical security can be bypassed when attackers exploit human error. Phishing campaigns, misinformation, and social engineering are some of the most common and successful vectors of attack, as seen during ransomware incidents like WannaCry, which spread quickly through human interactions with malicious attachments (NHS England, 2017; Europol, 2023).
Policy Coordination Gaps	Although the EU has introduced frameworks such as the NIS Directive and NIS2, national sovereignty over security matters can slow down collective response during crises. Disorganised policy frameworks make it difficult to mount an immediate and coordinated EU-wide response to cross-border cyber incidents (Council of the EU, 2017; Regulation (EU) 2019/881).

Actions Already Taken

The Cyber Diplomacy Toolbox

The EU adopted the Cyber Diplomacy Toolbox to strengthen its joint response to hostile cyber activities. This allows the EU to impose sanctions on individuals, or groups deemed responsible for cyberattacks, signalling that malicious activity in cyberspace carries tangible political and economic consequences (Council of the EU, 2017).

EU Cybersecurity Act

The Cybersecurity Act reinforced the role of the European Union Agency for Cybersecurity (ENISA) by granting it a permanent mandate and greater authority to coordinate resilience-building measures. It also introduced the first EU-wide cybersecurity certification framework for ICT products, services, and processes, designed to boost consumer trust and standards across the Union (Regulation (EU) 2019/881).

NIS and NIS2

The original Directive on Security of Network and Information Systems (NIS) set baseline cybersecurity obligations for operators of essential services. The updated NIS2 Directive, adopted in 2022, broadened its scope to cover more sectors and imposed stricter requirements on both essential and important service providers. This shift reflects the EU's recognition of growing interdependencies across critical infrastructure and supply chains (Directive (EU) 2022/2555).

EU Cybersecurity Strategy for the Digital Decade

As part of its wider Digital Decade agenda, the EU launched a cybersecurity strategy that focuses on resilience, securing supply chains, and improving crisis response coordination. The strategy highlights the importance of cooperation between member states and global partners to build collective defences against increasingly complex cyber threats (Once Upon a Time in... Europe's Digital Decade, 2025).

European Cybersecurity Competence Centre

Established to coordinate research, innovation, and funding in the field of cybersecurity, the ECCC serves as a central hub for strengthening Europe's technological and industrial capabilities in cyber defence. It plays a crucial role in bridging the gap between policymakers, academia, and private industry, ensuring that research findings are translated into practical tools and policies (European Commission / ENISA, 2021).

Actions to Discuss

Offensive Cyber Capabilities

The EU's cyberdefence regime is defensive. Offensive cyber capabilities remain a domestic policy area, with vast policy disparities and a complete lack of interoperability - meaning that offensive cyber functions are not the same across EU member states, making cooperation in the case of a crisis much more difficult (Olejnik, 2025).

The European Commission's White Paper for European Defence this year has recognised the importance and urgency of updating this doctrine, stating that, "Both defensive and offensive cyber capabilities are needed to ensure the protection and freedom of manoeuvre in cyberspace", as there is currently almost no risk of retaliation for those who target the EU in cyberattacks, which may attack as a much more powerful deterrent than sanctions (Eureporter, 2025).

The idea of developing EU-wide offensive cyber capabilities has been proposed in the European Council before, but has not gained enough traction to become a reality. In 2023, Charles Michel (then President of the European Council) proposed the idea of a 'European cyber force [...] equipped with offensive capabilities', however some issues raised in the session included how the chain of command would be decided, whether it would be stepping on the toes of NATO's cyber defence structure (of which not all EU member states are apart), and sovereignty - a key pillar in defence matters (Martin, 2023).

A differing view of how offensive cyber cooperation could be envisioned is through the EU's PESCO framework, which is a voluntary program, allowing willing and able EU members to work more closely in security and defence. This framework has already created Cyber Rapid Response Teams (CRRT), which pool together 8-12 cybersecurity professionals from the six voluntary participating countries in the project (Croatia, Estonia, Lithuania, the Netherlands, Poland, and Romania) to provide assistance in the event of cyber incidents around EU members, institutions, and partner countries (Eureporter, 2025).

While the CRRTs are only defensive and for crisis response purposes, a widening of this structure to include joint offensive practices and other information / knowledge sharing is a potential avenue. Of course, this structure's main limitation is that it is currently voluntary, with not every country participating. A formalisation of this structure could be a method of creating long-term strategies and institutional expertise for these activities, if all countries in the committee were to agree on how this would look.

Sanctions

In 2019, the EU established a framework to put sanctions on those responsible for cyberattacks. They cover cyberattacks that:

- Have a significant impact on the EU,
    - The definition of this is established as affecting critical infrastructure essential to the vital functioning of society, the storage of processing of classified information, or government response teams
- originate or are carried out from outside the EU,
- use infrastructure outside the EU,
- are carried out by persons or entities established or operating outside the EU,
- are carried out with the support of persons or entities operating outside the EU.

Currently, this sanctions regime is applied to 17 individuals and 4 entities, extended until the 18th of May 2026, including Russian nationals responsible for a series of cyber-attacks carried out against Estonia in 2020.

Sanctions include a ban on travelling to the EU and an asset freeze on the individuals and entities. Additionally, the provision of funds or economic resources, directly or indirectly, to the sanctioned individuals and entities or for their benefit is prohibited.

Whether or not to extend this sanction regime, if any definitions require changing, or if new activities should be the subject of sanctions is a potential topic of debate, as a form of deterrence and punishing those involved (Council of the European Union, 2025b).

Regulation of Social Media Platforms & Artificial Intelligence

The regulation of Social Media and Artificial Intelligence may be an avenue to explore, in order to counter Foreign Information Manipulation and Interference (FMI). 88% of FMI activity identified by the EU between November 2023 and November 2024 took place on 'X', due to its importance as an opinion-shaping platform, with around 28,000 accounts identified as part of bot networks that spread misinformation through impersonating institutions, public figures, or legitimate media. They adjust narratives to regional culture, local languages and current events - but all aligned with Russia's geopolitical goals (Olejnik, 2025).

Artificial Intelligence is also playing an increasingly large role in these incidents, at least 41 incidents of those identified. Its main uses are the creation of deepfakes and synthetic audio, and automating the large-scale dissemination of FMI. While its capability is still basic, it has made FMI much more scaleable, lowering cost and boosting output greatly, and its quality is increasing rapidly (Olejnik, 2025).

Putting potential regulation on social media platforms to make them responsible for the content they put out may be a way to combat the hybrid warfare threat, however, these must be balanced against concerns over freedom of speech and tech innovation. Similarly, potential regulation on AI models and their usage could be a potential solution to stop it becoming a powerful tool for disinformation, but should be balanced against hampering innovation and economic growth.

Key Stakeholders and Blocs

This section will cover some of the important stakeholders (be them institutions or countries) that are not represented in the committee, but are still recommended for delegates to consider during debate.

ENISA

ENISA is the European Union Agency for Cybersecurity. It was established in 2004, for the purpose of improving cybersecurity integration across the European Union through sharing knowledge, developing staff and structures, and raising awareness (European Union, n.d.).

The EU Cybersecurity Act, in 2019, created a permanent mandate for ENISA, which includes:

- Giving out cybersecurity certifications
- Increasing operational cooperation at an EU level
- Helping EU states that request it to handle their cybersecurity incidents
- Supporting the coordination of the EU in case of large-scale cross-border cyberattacks and crises (European Commission, 2025a)

However, ENISA's mandate is currently under review by the European Commission (as of August 2025). In this committee, you may want to consider if ENISA's current mandate is built-for-purpose, and what changes (if any) are necessary to prepare the EU for upcoming cyber threats.

Hungary & Slovakia

Hungary and Slovakia are the main outliers in this committee in terms of their general alignment, which are much more favourable towards Russia's government compared to most. For example, Hungary's Head of Government, Viktor Orban, has offered to host a summit between Trump and Putin, repeatedly vetoes the advance of Ukraine's accession to the EU and consistently opposes EU measures against Russia. Slovakia's Head of Government, Robert Fico, has also vetoed a wave of sanctions on Russia in October 2025, at least until other issues, such as improving competitiveness for key Slovak industries, are tackled first, not seeing measures against Russia as a priority (Liboreiro, 2025).

Navigating these differences will be necessary for the committee, given the veto power each country has, which both countries have been willing to use often in the European Council.

Points of Discussion & Guiding Questions

A Conclusion Should Address

Many proposals face delays because they require political agreement at the EU level, funding, legal regulation, and cooperation from private stakeholders, as well as varying levels of readiness among countries (European Court of Auditors, 2019).
Below are matters which delegates may wish to consider and discuss as part of the adoption of a conclusion.

Measures Already Under Consideration

- EU-Wide Rapid Cyber Response Teams to assist member states in containing large-scale incidents (Council of the EU, 2022).
- Mandatory Cyber Resilience Standards for IoT (Internet of Things) devices and critical software (European Commission, 2024).
- Enhanced Public-Private Partnerships, which encourage industry collaboration to share threat intelligence quickly (ENISA, 2023).
- Joint Cyber Exercises, which are simulation-based training for cross-border response coordination. E.g., "Cyber Europe" in which ENISA organises recurring large-scale Cyber Europe exercises to test cross-border responses (recent editions include 2018, 2020, 2022 and 2024) (ENISA, 2024).
- Increased Investment in Cyber Workforce Development to address the shortage of trained cybersecurity professionals (European Union, 2025).

Measures Already Under Consideration

- How can the EU balance national sovereignty with the need for centralised cybersecurity coordination?
- Should EU cyber defence capabilities be integrated into the Common Security and Defence Policy (CSDP)?
- How can smaller and less digitally advanced member states be supported in building cyber resilience?
- How should the EU address the human factor in cyber vulnerabilities, including education, awareness, and workforce skills?
- How can the EU strengthen partnerships with NATO, the UN, and private tech companies to respond to cross-border cyber incidents?

Additional Resources

Curious delegates with too much free time can read the minutes of the first meeting here:
https://www.consilium.europa.eu/media/20440/1975_march_dublin_eng_.pdf

The full text of the strategic agenda 2024-2029 can be found here:
https://www.consilium.europa.eu/media/yxrc05pz/sn02167en24_web.pdf

Bibliography

2009/882/EU. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D0882 [Accessed 6 Aug. 2025].

Agence de presse Meurisse (1929). Portrait of Robert Schuman 1929. [Online Image] Website. Available at: https://gallica.bnf.fr/ark:/12148/btv1b9055554h/f1 [Accessed 7 Aug. 2025].

CISA (2021). Cyber-Attack Against Ukrainian Critical Infrastructure. [online] Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [Accessed 20 Aug. 2025].

Council of the European Union (2025a). Hybrid threats / Russia: Statement by the High Representative on behalf of the EU condemning Russia's persistent hybrid campaigns against the EU, its Member States and partners. [online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2025/07/18/hybrid-threats-russia-statement-by-the-high-representative-on-behalf-of-the-eu-condemning-russia-s-persistent-hybrid-campaigns-against-the-eu-its-member-states-and-partners/ [Accessed 15 October 2025].

Council of the European Union (2025b). Sanctions against cyber-attacks. [online]. Available at: https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/ (Accessed 15 October 2025).

Council of the European Union (2017). EN CYBER 98 RELEX 554 POLMIL 77 CFSP/PESC 557 OUTCOME OF PROCEEDINGS From: General Secretariat of the Council. [online] consilium.europa.eu. Available at: https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf [Accessed 20 Aug. 2025].

Directive (EU) 2022/2555. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng [Accessed 20 Aug. 2025].

ENISA (2023) Threat Landscape Report 2023. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023?utm_source#contentList (Accessed: 20 August 2025).

ENISA (2024). Cyber Europe 2024 After Action Report. [online] enisa.europa.eu. Available at: https://www.enisa.europa.eu/publications/cyber-europe-2024-after-action-report [Accessed 20 Aug. 2025].

ENISA (2025). ENISA. [online] enisa.europa.eu. Available at: https://www.enisa.europa.eu [Accessed 20 Aug. 2025].

Eureporter (2025). On strengthening cyber offensive capabilities, EU member states cannot wait after Brussels. [online]. Available at: https://www.eureporter.co/defence/cybercrime-2/2025/05/09/on-strengthening-cyber-offensive-capabilities-eu-member-states-cannot-wait-after-brussels/ (Accessed: 21 October 2025).

European Commission (2001) Communication on Network and Information Security: Proposal for a European Policy Approach. COM(2001) 298 final. Available at: https://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF (Accessed: 20 August 2025).

European Commission / ENISA (2021) European Cybersecurity Competence Centre (ECCC). Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre (Accessed: 20 August 2025).

European Commission (2025a). Cybersecurity Act | Shaping Europe's digital future. [online] ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act [Accessed 23 Aug. 2025].

European Commission (2025b). The State of the Digital Decade. [online] ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report [Accessed 20 Aug. 2025].

European Commission, Council of the European Union, European Parliament, European Economic and Social Committee and Committee of the Regions (2001). EUR-Lex - 52001DC0298 - EN - EUR-Lex. [online] eur-lex.europa.eu. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52001DC0298 [Accessed 20 Aug. 2025].

European Council (2024). Strategic agenda 2024-2029. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/strategic-agenda-2024-2029/ [Accessed 15 Aug. 2025].

European Council (2025a). Current Membership of the European Council. [Online Image] Website. Available at: https://epthinktank.eu/2025/06/25/outlook-for-the-european-council-meeting-on-26-27-june-2025/current-membership-european-council-june-2025/ [Accessed 15 Aug. 2025].

European Council (2025b). History. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/history/?taxonomyId=6b7901c5-1094-4713-add8-3364400eee98 [Accessed 7 Aug. 2025].

European Council (2025c). How the European Council works. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/how-the-european-council-works/ [Accessed 15 Aug. 2025].

European Council (2025d). What are the top cyber threats in the EU? [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/policies/top-cyber-threats/ [Accessed 20 Aug. 2025].

European Court of Auditors (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf [Accessed 29 Sept. 2025].

European Court of Auditors, Jakobsen, B., Costa de Magalhaes, D., Garcia de Parada, I., Ballester-Gallardo, A., Sweerts, M., Dennet, S., Petliza, A., Iaconisi, M., Scardone, M., Monteiro Da Cunha, S. and Bolkart, J. (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed 20 Aug. 2025].

European Cybersecurity Competence Centre (2025). European Cybersecurity Competence Centre and Network. [online] cybersecurity-centre.europa.eu. Available at: https://cybersecurity-centre.europa.eu/index_en [Accessed 20 Aug. 2025].

European External Action Service (2024). Countering Hybrid Threats. [online] eeas.europa.eu. Available at: https://www.eeas.europa.eu/sites/default/files/documents/2024/2024-countering-Hybrid-Threats.pdf [Accessed 20 Aug. 2025].

European External Action Service (EEAS) (2022) Hybrid Threats Strategy. Available at: https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en (Accessed: 20 August 2025).

European Union (2024) Cyber Resilience Act. Digital Strategy – Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (Accessed: 20 August 2025).

European Union (2025) A European outlook from the ISACA 2024 State of Cybersecurity Report. Digital Skills and Jobs Platform. Available at: https://digital-skills-jobs.europa.eu/en/latest/news/european-outlook-isaca-2024-state-cybersecurity-report (Accessed: 20 August 2025).

European Union (2025a). European Council – role and powers | European Union. [online] european-union.europa.eu. Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-council_en [Accessed 7 Aug. 2025].

European Union (n.d.). European Union Agency for Cybersecurity | European Union. [online] european-union.europa.eu. Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en [Accessed 23 Aug. 2025].

European Union (2004) Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. Official Journal of the European Union, L 77, 13 March 2004, pp. 1–11. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML (Accessed: 20 August 2025).

European Union (2025b). Types of institutions and bodies. [online] european-union.europa.eu. Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/types-institutions-and-bodies_en [Accessed 7 Aug. 2025].

Europol (2023). Internet Organised Crime Threat Assessment. [online] europol.europa.eu. Available at: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023 [Accessed 20 Aug. 2025].

Greenberg, A. (2018). White House Blames Russia for NotPetya, the 'Most Costly Cyberattack In History'. [online] WIRED. Available at: https://www.wired.com/story/white-house-russia-notpetya-attribution/ [Accessed 20 Aug. 2025].

Hendryckx, M. (2012). Herman Van Rompuy - Official Portrait. [Online Image] Website. Available at: https://en.wikipedia.org/wiki/File:Herman_Van_Rompuy_675_(cropped).jpg [Accessed 15 Aug. 2025].

Lee, R.M., Assante, M.J. and Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. [online] nsarchive.gwu.edu. Available at: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf [Accessed 20 Aug. 2025].

Liboreiro, J. (2025). EU pushes Slovak PM Fico to lift veto on new Russia sanctions package [online] euronews.com. Available from: European Council (2024). Strategic agenda 2024-2029. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/strategic-agenda-2024-2029/ [Accessed 15 Aug. 2025].

European Council (2025a). Current Membership of the European Council. [Online Image] Website. Available at: https://epthinktank.eu/2025/06/25/outlook-for-the-european-council-meeting-on-26-27-june-2025/current-membership-european-council-june-2025/ [Accessed 15 Aug. 2025].

European Council (2025b). History. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/history/?taxonomyId=6b7901c5-1094-4713-add8-3364400eee98 [Accessed 7 Aug. 2025].

European Council (2025b). History. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/history/?taxonomyId=6b7901c5-1094-4713-add8-3364400eee98 [Accessed 7 Aug. 2025].

European Council (2025c). How the European Council works. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/how-the-european-council-works/ [Accessed 15 Aug. 2025].

European Council (2025d). What are the top cyber threats in the EU? [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/policies/top-cyber-threats/ [Accessed 20 Aug. 2025].

European Court of Auditors (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf [Accessed 29 Sept. 2025].

European Court of Auditors, Jakobsen, B., Costa de Magalhaes, D., Garcia de Parada, I., Ballester-Gallardo, A., Sweerts, M., Dennet, S., Petliza, A., Iaconisi, M., Scardone, M., Monteiro Da Cunha, S. and Bolkart, J. (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed 20 Aug. 2025].

European Cybersecurity Competence Centre (2025). European Cybersecurity Competence Centre and Network. [online] cybersecurity-centre.europa.eu. Available at: https://cybersecurity-centre.europa.eu/index_en [Accessed 20 Aug. 2025]. (Accessed 21 October 2025).

NATO Strategic Communication Centre of Excellence, Pamment, J., Sazonov, V., Granelli, F., Aday, S., Andžāns, M., Bērziņa-Čerenkova, U., Gravelines, J.-P., Hills, M., Holmstrom, M., Klus, A., Martinez-Sanchez, I., Mattiisen, M., Molder, H., Morakabati, Y., Sari, A., Simmons, G. and Terra, J. (2019). Hybrid Threats: 2007 cyber attacks on Estonia. [online] stratcomcoe.org. Available at: https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86 [Accessed 20 Aug. 2025].

Martin, A. (2023). EU Council president proposes 'European cyber force' with 'offensive capabilities'. [online] therecord.media. Available at: European Council (2024). Strategic agenda 2024-2029. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/strategic-agenda-2024-2029/ [Accessed 15 Aug. 2025].

European Council (2025a). Current Membership of the European Council. [Online Image] Website. Available at: https://epthinktank.eu/2025/06/25/outlook-for-the-european-council-meeting-on-26-27-june-2025/current-membership-european-council-june-2025/ [Accessed 15 Aug. 2025].

European Council (2025b). History. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/history/?taxonomyId=6b7901c5-1094-4713-add8-3364400eee98 [Accessed 7 Aug. 2025].

European Council (2025c). How the European Council works. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/how-the-european-council-works/ [Accessed 15 Aug. 2025].

European Council (2025d). What are the top cyber threats in the EU? [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/policies/top-cyber-threats/ [Accessed 20 Aug. 2025].

European Court of Auditors (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf [Accessed 29 Sept. 2025].

European Court of Auditors, Jakobsen, B., Costa de Magalhaes, D., Garcia de Parada, I., Ballester-Gallardo, A., Sweerts, M., Dennet, S., Petliza, A., Iaconisi, M., Scardone, M., Monteiro Da Cunha, S. and Bolkart, J. (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed 20 Aug. 2025].

European Cybersecurity Competence Centre (2025). European Cybersecurity Competence Centre and Network. [online] cybersecurity-centre.europa.eu. Available at: https://cybersecurity-centre.europa.eu/index_en [Accessed 20 Aug. 2025]. (Accessed 21 October 2025).

NHS England (2023). NHS England business continuity management toolkit case study: WannaCry attack. [online] england.nhs.uk. Available at: https://www.england.nhs.uk/long-read/case-study-wannacry-attack/ [Accessed 20 Aug. 2025].

Once Upon a Time in... Europe's Digital Decade (2025) YouTube. Available at: https://www.youtube.com/watch?v=waP8GgHWKiI (Accessed: 20 August 2025). Regulation (EU) 2019/881. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng [Accessed 20 Aug. 2025].

Rid, T. and Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies, [online] 38(1-2), pp.4–37. doi:https://doi.org/10.1080/01402390.2014.977382.

Olejnik, L. (2025) Russian cyber and information warfare and its impact on the EU and UK [online]. Available from: European Council (2024). Strategic agenda 2024-2029. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/strategic-agenda-2024-2029/ [Accessed 15 Aug. 2025].

European Council (2025a). Current Membership of the European Council. [Online Image] Website. Available at: https://epthinktank.eu/2025/06/25/outlook-for-the-european-council-meeting-on-26-27-june-2025/current-membership-european-council-june-2025/ [Accessed 15 Aug. 2025].

European Council (2025b). History. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/history/?taxonomyId=6b7901c5-1094-4713-add8-3364400eee98 [Accessed 7 Aug. 2025].

European Council (2025c). How the European Council works. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/how-the-european-council-works/ [Accessed 15 Aug. 2025].

European Council (2025d). What are the top cyber threats in the EU? [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/policies/top-cyber-threats/ [Accessed 20 Aug. 2025].

European Court of Auditors (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf [Accessed 29 Sept. 2025].

European Court of Auditors, Jakobsen, B., Costa de Magalhaes, D., Garcia de Parada, I., Ballester-Gallardo, A., Sweerts, M., Dennet, S., Petliza, A., Iaconisi, M., Scardone, M., Monteiro Da Cunha, S. and Bolkart, J. (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed 20 Aug. 2025].

European Cybersecurity Competence Centre (2025). European Cybersecurity Competence Centre and Network. [online] cybersecurity-centre.europa.eu. Available at: https://cybersecurity-centre.europa.eu/index_en [Accessed 20 Aug. 2025]. (Accessed 15 October 2025).

Zsiros, S. (2025). Hungary's Orbán claims 'EU has decided to go to war' in petition call. [online] euronews.com. Available from: European Council (2024). Strategic agenda 2024-2029. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/strategic-agenda-2024-2029/ [Accessed 15 Aug. 2025].

European Council (2025a). Current Membership of the European Council. [Online Image] Website. Available at: https://epthinktank.eu/2025/06/25/outlook-for-the-european-council-meeting-on-26-27-june-2025/current-membership-european-council-june-2025/ [Accessed 15 Aug. 2025].

European Council (2025b). History. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/history/?taxonomyId=6b7901c5-1094-4713-add8-3364400eee98 [Accessed 7 Aug. 2025].

European Council (2025c). How the European Council works. [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/european-council/how-the-european-council-works/ [Accessed 15 Aug. 2025].

European Council (2025d). What are the top cyber threats in the EU? [online] consilium.europa.eu. Available at: https://www.consilium.europa.eu/en/policies/top-cyber-threats/ [Accessed 20 Aug. 2025].

European Court of Auditors (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf [Accessed 29 Sept. 2025].

European Court of Auditors, Jakobsen, B., Costa de Magalhaes, D., Garcia de Parada, I., Ballester-Gallardo, A., Sweerts, M., Dennet, S., Petliza, A., Iaconisi, M., Scardone, M., Monteiro Da Cunha, S. and Bolkart, J. (2019). Challenges to effective EU cybersecurity policy. [online] eca.europa.eu. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed 20 Aug. 2025].

European Cybersecurity Competence Centre (2025). European Cybersecurity Competence Centre and Network. [online] cybersecurity-centre.europa.eu. Available at: https://cybersecurity-centre.europa.eu/index_en [Accessed 20 Aug. 2025]. (Accessed 21 October 2025)