VEMUN 2026

Guaranteeing Governance in the Global Future: What Role for Europe?

March 13 – 15, 2026

SPC: (EU+)

Information Warfare

Expert Speaker: Jean-Marc Lieberherr Monnet

Chairs: Nina Chimenes and Clément Franco

Table of Contents

Introduction

In 2022, the Government of Costa Rica declared a national emergency after a ransomware attack brought 27 government bodies offline, disrupting everyday functions for months. In 2023, an employee of a multinational corporation in Hong Kong transferred $25.6 million after being instructed to do so during a Zoom call with colleagues he recognized. The other attendees, however, were deepfakes, and the money was sent to sham accounts. In France, on December 16, 2025, the Ministry of the Interior reported a cyberattack. An attacker gained access to sensitive police files, including those of wanted persons, as well as files relating to financial crimes and criminal records (TAJ), which contain information on approximately 16 million individuals. These incidents show that the technologies used by hackers can bypass security systems and therefore pose severe threats to populations and governments around the world.

Moreover, there is growing concern over the misuse of information and communications technologies (ICT) by terrorists, in particular the Internet and new digital technologies, to commit, incite, recruit, fund or plan terrorist acts. For example, in 2013, the Daesh militant organization, also known as the Islamic State of Iraq and Syria (ISIS), was created. The process of recruitment and radicalisation in Western Europe of Muslims and non-Muslims was mostly through the internet. Indeed, ISIS has gained worldwide attention as the most brutal Islamist terror group of our times, with the reach of broadband connectivity, even in war-torn cities and towns.

The frequency, sophistication, and costliness of cybercrimes have continued to increase in recent years, and they are becoming notoriously difficult to track. International consensus and cooperation are becoming more critical to address the rapidly evolving risks these crimes pose to States, businesses, and individuals.

In 2021, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes held its first organizational session, with the ultimate goal of drafting a convention to address cybercrime ("the Convention"). However, defining the precise purpose and scope of such a convention is fraught with complexities; balancing the need for effective law enforcement with the protection of privacy and human rights remains a significant challenge.

Indeed, investigating crimes committed via ICTs can be a highly invasive process and may be used to justify vast surveillance. Digital rights organizations and UN bodies, including the Office of the High Commissioner for Human Rights, have raised concern over how domestic cybercrime laws are often used to justify restricting freedoms of speech, assembly, and association. For instance, Russia's “sovereign internet” law aims to provide a legal basis for mass surveillance, allowing the government to effectively enforce online existing legislation that undermines freedom of expression and privacy, according to Human Rights Watch. This includes tracking, rerouting, and blocking, which is presented as an attempt to prevent “security threats”.

Definition of Key Terms

Cybercrime

There is no internationally agreed definition of cybercrime, and the current draft of the Convention does not set out a precise one. The term cybercrime nevertheless functions as an umbrella concept encompassing a broad range of unlawful activities carried out online. These activities are commonly divided into two main categories: cyber-enabled crimes and cyber-dependent crimes.

Cyber-enabled crimes refer to traditional forms of criminal conduct that are facilitated or amplified by digital technologies but do not inherently require them, such as drug and arms trafficking, identity theft, fraud, or incitement to violence.

Cyber-dependent crimes, on the other hand, are intrinsically linked to information and communication technologies and can only be committed through the use of Information and Communication Technology (ICT) devices, such as the spread of malware.

Cyberwarfare

This term is used to describe cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack. An armed attack intentionally causes destructive effects (i.e., death and/or physical injury to living beings and/or destruction of property).

Only governments, organs of the state, or state-directed or state-sponsored individuals or groups can engage in cyberwarfare. The right to self-defence serves as one exception to the general prohibition of the use of force against other states prescribed in Article 2(4) of the UN Charter. When engaging in cyberwarfare, *jus in bello* (i.e., the right conduct during war) is required. Here, the cyber acts that amount to a use of force must be: 1)proportionate (both to the threat that justified this response and in light of the potential collateral damage 2) aimed at minimizing casualties through the adoption of certain precautionary measure 3)discriminating in its targets (i.e., only the actual target should be subjected to the cyber act) and used only as a last resort, after lesser invasive means have been exhausted and/or ruled out as unfeasible options.

Information warfare

This term is used to describe the collection, distribution, modification, disruption, interference with, corruption, and degradation of information in order to gain some advantage over an adversary. The purpose of this information is to utilize and communicate it in a way that alters the target's perception of an issue or event in order to achieve some desired outcome.

Two tactics used in information warfare are disinformation (i.e., the deliberate spreading of false information) and fake news (i.e., propaganda and disinformation masquerading as real news). However, the latter term is not well defined and can be misused.

Declining levels of trust have contributed to the rapid spread and consumption of fake news by the public. Social media platforms enable disinformation to spread faster and to a larger audience than other online platforms; depending on the platform, this can occur in real-time (e.g., Twitter). Automated bot accounts assist in this endeavour by spreading information at a faster and more frequent rate than individual users can. Supporters of disinformation and bots also amplify disinformation and fake news online. Disinformation and fake news are believed to have influenced voter behaviour and ultimately, the outcome of elections.

Hacktivism

While there is no universally agreed upon definition of hacktivism, it has been described as the intentional access to systems, websites, and/or data without authorization or having exceeded authorized access, and/or the intentional interference with the functioning and/or accessibility of systems, websites, and data without authorization or having exceeded authorized access, in order to effect social or political change.

Numerous hacktivist groups exist with various social and political agendas. The cybercrimes hacktivists have committed include website defacements, website redirects, denial-of-service (DoS) attacks or distributed denial of service (DDoS) attacks, malware distribution, data theft and disclosure, and sabotage. All of these tactics involve unauthorized access to targets' systems, websites and/or data.

Cyberterrorism

Information and communication technology (ICT) can be used to facilitate the commission of terrorist-related offences (a form of cyber-enabled terrorism) or can be the target of terrorists (a form of cyber-dependent terrorism). Specifically, ICT can be used to promote, support, facilitate, and/or engage in acts of terrorism.

Particularly, the Internet can be used for terrorist purposes such as the spreading of "propaganda (including recruitment, radicalization and incitement to terrorism); [terrorist] financing; [terrorist] training; planning [of terrorist attacks] (including through secret communication and open-source information); execution [of terrorist attacks]; and cyberattacks" (UNODC, 2012, p. 3).

The term cyberterrorism has been applied by some to describe the use of the Internet for terrorist purposes. While certain countries have national cyberterrorism laws (e.g., India, Pakistan, and Kenya), cyberterrorism is not explicitly prohibited under international law.

Cyberespionage

While there is no single, universal definition of espionage, espionage has been described as a method of intelligence collection: particularly, as a "process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems)". Nonetheless, even intelligence collection has "no internationally recognized and workable definition".

Cyberespionage involves the use of information and communication technology (ICT) by individuals, groups, or businesses for some economic benefit or personal gain. Cyberespionage may also be perpetrated by government actors, state-sponsored or state-directed groups, or others acting on behalf of a government, seeking to gain unauthorized access to systems and data in an effort to collect intelligence on their targets in order to enhance their own country's national security, economic competitiveness, and/or military strength.

While espionage is not a new phenomenon, ICT have enabled illicit intelligence collection efforts directed and/or orchestrated by other countries at an unprecedented speed, frequency, intensity, and scale, as well as a reduction of risks associated with committing espionage (i.e., being caught by the country that is being targeted by the collection efforts).

Several cyberespionage campaigns have been attributed to advanced persistent threats (or APTs), which refer to "group[s] with both the capability and intent to persistently and effectively target a specific entity". However, APTs do not limit their acts to cyberespionage; they have also engaged in destruction of systems and/or data (sabotage), and disruption of operations. The primary tactics used by perpetrators of cyberespionage have been identified. These include (but are not limited to) malware distribution, social engineering, spear phishing, and watering hole attacks. Notably, in recent times, the French IT giant Cap Gemini was supplying information systems to facilitate Immigrations and Customs Enforcement (ICE) work in capturing foreigners in the USA. Its American subsidiary signed a deal with ICE to identify foreigners on US soil and track their locations.

General Overview

The roots of cyber warfare extend back to the 1980s when the U.S. recognized the potential of cyber tools for espionage, sabotage, and propaganda. This marked the realisation phase, followed by the take-off phase and the modern militarization phase, bringing about significant shifts like cyber threats. Early instances, such as the Solar Sunrise incident in 1998, the Moonlight Maze operation in 1999, and the Titan Rain campaign in 2003, exemplify the evolution of cyber warfare.

The 21st century has witnessed a barrage of major cyber-attacks and data breaches, each impacting national security, economic stability, and diplomatic relations. From the Stuxnet attack on Iran's nuclear program in 2010 to the SolarWinds hack in 2020, these incidents highlight the multifaceted challenges of responding to and preventing cyber attacks. The need for international cooperation, the development of cyber norms, and the attribution of responsibility are critical aspects of this ongoing battle.

The evolution of cyber warfare is intrinsically linked to rapid technological advancements, the proliferation of cyber actors, and the integration of cyber and physical domains. The consequences of cyber attacks, from financial loss to reputational damage and even physical harm, underscore the criticality of robust cyber security practices.

Cyber warfare has become an escalating concern for global security. Many nations actively engage in cyber warfare programs, underscoring the gravity of the situation. The intricate nature of cyber warfare impacts diverse domains of critical infrastructure, including network security, application security, and information security. However, attribution in cyber warfare remains challenging due to the use of techniques like proxies, encryption, and malware to conceal identities. The lack of consensus on the definition, legality, and ethics further complicates efforts to deter cyber threats.

Recent high-profile cyber attacks, such as the SolarWinds hack, Colonial Pipeline ransomware attack, and Microsoft Exchange Server hack, underscore the vulnerabilities in global cybersecurity frameworks.

Moreover, in today's digital and interconnected world, the spread of misinformation and disinformation poses a critical threat to the foundational elements of our societies. The rapid proliferation of misinformation and disinformation undermines trust in institutions and elections, fuels societal divisions, and jeopardises public health initiatives, thereby threatening the very fabric of democracy and informed decision-making.

New technologies present evolving opportunities and challenges to the information space. The development of the use of generative Artificial Intelligence will magnify changes to the information environment even further, and create new challenges.

The integration of artificial intelligence (AI) and machine learning (ML) into cyber warfare strategies introduces both opportunities and risks. AI enhances cyber defence capabilities by improving threat detection, analysis, and mitigation. It automates security processes, identifies anomalies in large datasets, and optimizes cybersecurity tools. Conversely, AI also fuels new forms of cyber offences, enabling the creation of adaptive malware, deepfakes for propaganda, and sophisticated cyber attacks.

The danger posed by cyber warfare isn't confined to just military concerns; it seeps into the economic and political realms, posing risks to national security. Cyber attacks can disrupt military operations, inflict economic losses, and manipulate political processes, jeopardizing the stability of a nation. The fallout may range from damaging critical infrastructure to harming citizens and eroding public trust. Effectively countering this complex threat requires a holistic approach through international cybersecurity strategies. These strategies should involve the creation of robust frameworks, the continuous improvement of cybersecurity capabilities, and active engagement in international cooperation to strengthen collective defences and coordination efforts.

However, the ability to draw international legal lines for legitimate and illegitimate forms of cyberinterventions (based on the principles of sovereign equality, non-intervention, and territorial integrity) is an extremely fraught issue. This is owed in part to the failure of States to sufficiently articulate how the customary international legal rules should be applied in cyberspace.

Indeed, in addressing rapid technological change, policymakers often treat digital space as a separate policy area. Yet information and communication technologies are simply tools through which a wide range of activities, harmful and lawful alike, are carried out. When these activities are already regulated, broad policies focused only on the technology risk being ineffective. A more targeted approach would be to strengthen existing issue-specific international instruments, such as those on crime or drug control, by better incorporating digital realities rather than regulating cyberspace in isolation.

Major Parties Involved

A – State Actors

China

China is associated with long-term cyber-espionage and strategic access operations, with groups like APT10, APT31 and APT41 targeting telecoms, ministries, defence industries and critical infrastructure across all continents. Moreover, Chinese-linked campaigns also experiment with covert influence on social media and diaspora communities, spreading narratives that favour Beijing's positions while discrediting critics or rival powers.

Russia

Russian military intelligence (GRU) units such as Sandworm (APT44) and APT28 ("Fancy Bear") have been repeatedly linked to destructive attacks, election interference and hack-and-leak operations targeting Ukraine, EU member states and NATO institutions. Furthermore, Russia's approach blends classic "active measures" (propaganda, forgeries, front organisations) with modern tools like botnets, troll farms and data-driven targeting, seeking to polarise societies and undermine trust in democratic institutions rather than simply steal data. Russia's cyber operations are directly coordinated with China through the Russia-China Information and Communication Technologies Forum (established in 2016). The two countries align their narratives through media coordination, simultaneously target democratic institutions (e.g. during the 2024/2025 EU elections, Russia deployed the "Portal Kombat" disinformation network with clone websites under "Pravda" branding spreading false content across nearly every European language), and share cyber threat intelligence. This partnership amplifies both nations' influence operations against Europe, with synchronized campaigns across multiple platforms designed to undermine NATO unity and erode public trust in democratic governments.

United States of America:

The United States combines defensive capabilities (CISA, NSA, FBI) with offensive capacity under US Cyber Command, whose "defend forward" doctrine aims to disrupt hostile actors in their own networks before they strike. While the US publicly emphasises responsible behaviour and the application of international law to cyberspace, leaked and open-source information confirms that it conducts offensive operations, including activities designed to deter adversaries or counter extremist propaganda. Other NATO members and close allies (e.g. UK, France, the Netherlands) have acknowledged possessing offensive cyber capabilities, signalling that major democracies also view cyber-operations as legitimate tools of statecraft.

Europe:

In Europe, several EU member states such as France, Germany and the Baltic states have emerged as leaders in cyber-defence and counter-disinformation, often drawing on their direct exposure to Russian and other foreign operations. At EU level, bodies like ENISA, CERT-EU, Europol's European Cybercrime Centre (EC3) and the European External Action Service (EEAS) coordinate incident response, support member states, and expose foreign information manipulation targeting EU audiences.

B- Non-State proxies, hacktivists and criminal groups

Proxies, criminals and mercenaries

Hacktivist groups, "patriotic hackers" and ransomware gangs carry out DDoS attacks, data leaks and extortion, sometimes for profit and sometimes in ways that align with state interests. Moreover, commercial "influence-as-a-service" firms and mercenary outfits sell disinformation campaigns, bot networks and tailored online harassment, making sophisticated information warfare accessible to clients who lack in-house capabilities.

Platforms, tech firms and media

Social media platforms, messaging apps and cloud providers host and transmit most of the content used in information operations, so their algorithms, content rules and security practices greatly shape the spread and visibility of attacks. Traditional media, journalists, NGOs and researchers can either expose disinformation and cyber-campaigns or, under pressure, unintentionally amplify them, making them both key defenders and potential vectors.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/

https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups

https://digital-strategy.ec.europa.eu/en/policies/online-disinformation

https://www.stopfake.org/en/the-rise-of-the-disinformation-for-hire-industry/

Timeline of Key Events

Year	Event	Type (cyber / disinfo / hybrid)	Importance
2007	Estonia cyber‑attacks on banks, media and government sites after a political dispute with Russia	Cyber	Often cited as the first large‑scale, politically motivated national cyber‑crisis; pushed NATO and the EU to treat cyber as a core security.
2008	Russo‑Georgian war accompanied by website defacements and cyber‑attacks on Georgian state entities	Hybrid	Illustrates how cyber‑operations can support kinetic war by disrupting communication and shaping international narratives.
2010	Stuxnet malware sabotages Iranian nuclear centrifuges	Cyber	Demonstrates that digital tools can cause physical destruction, blurring lines between covert operations and armed attack.
2014–2016	Ukraine electoral interference attempts; 2016 US election hack‑and‑leak and social‑media manipulation	Hybrid	Shows how hacking, leaks and targeted disinformation can be combined to influence democratic processes and trust in elections.

2017	WannaCry and NotPetya ransomware/wiper outbreaks hit hospitals, logistics and multinational firms	Cyber	Global economic damage and collateral harm to health systems reveal that poorly controlled malware can become a systemic risk.
2018	UN General Assembly establishes the first OEWG on ICT security (res. 73/27)	Norms / diplomacy	Marks the move from expert-only GGEs to an inclusive global negotiation track on norms of responsible state behaviour in cyberspace.
2020	SolarWinds supply-chain compromise gives suspected Russian actors long-term access to US government and company networks	Cyber / espionage	Highlights the vulnerability of widely used software and the difficulty of detecting sophisticated long-term intrusions.
2022–2024	Russian invasion of Ukraine accompanied by destructive wipers, satellite hacks and intensive information campaigns	Hybrid	Considered the first sustained war where cyber-attacks and information operations are systematically integrated into military strategy.
2021–2025	Second UN OEWG on ICT security and negotiations on a UN cybercrime treaty under UNODC	Norms / law	Demonstrates both progress (agreement on applicability of international law) and deep political divisions over sovereignty and content-related offences.
2024	Growing use of deepfakes in election contexts and harassment campaigns worldwide	Disinformation / tech	AI tools lower the cost of plausible video and audio manipulation, creating new challenges for verification and public trust.
2025	UN cyber negotiations move towards a permanent global mechanism on ICT security after OEWG's final report	Norms / diplomacy	Suggests that, despite tensions, states accept the need for a standing forum to address ICT security and capacity-building.

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

https://www.congress.gov/crs-product/R46974

https://en.wikipedia.org/wiki/List_of_cyberattacks

https://dig.watch/updates/un-oewg-concludes-paving-way-for-permanent-cybersecurity-mechanism

Previous Attempts to Resolve the Issue

UN‑level efforts

- Cyber norms and international law (GGE & OEWG):
  Since 2004, UN Groups of Governmental Experts and the Open‑Ended Working Group have confirmed that existing international law, including the UN Charter, applies to state behaviour in cyberspace and endorsed voluntary norms, such as protecting critical infrastructure and helping other states after major cyber incidents. These processes show broad recognition of the problem but remain non‑binding and often stuck on political disagreements over sovereignty, content regulation and how to attribute and respond to attacks.

- Resolutions on disinformation and human rights:
  The UN General Assembly's resolution 76/227 on "Countering disinformation for the promotion and protection of human rights and fundamental freedoms" and the Secretary‑General's follow‑up report collected examples of state and platform measures and stressed that counter‑disinformation efforts must respect freedom of expression, plural media and civil society. More recent Human Rights Council and expert documents continue to frame disinformation as a human‑rights and democracy issue, not only a security threat, and encourage transparency and safeguards against abuse of these policies.

European Union responses

- EU disinformation and platform regulation:
  The EU has built a layered approach: the 2018 Action Plan against Disinformation and the European Democracy Action Plan were followed by the Code of Practice on

Disinformation, a self-regulatory framework agreed with major platforms and other stakeholders. In 2022 the Code was strengthened, and in 2025 it was formally integrated into the Digital Services Act (DSA) as a Code of Conduct, making its commitments on demonetising disinformation, fact-checking cooperation, and transparency reports part of an enforceable EU regulatory system.

- EU cybersecurity and incident response:
  The EU Agency for Cybersecurity (ENISA) supports member states through threat-landscape reporting, crisis-management best practices and large-scale "Cyber Europe" exercises, and it helps run the CSIRTs Network and EU-CyCLONe for coordinated response to cross-border incidents. These mechanisms improve information-sharing and crisis coordination, but they do not fully solve political questions like how far the EU should go in offensive cyber-capabilities or joint responses to foreign information operations.

Societal and multi-stakeholder initiatives:

- Fact-checking, media literacy and research:
  International organisations, NGOs and research networks in Europe and beyond have expanded fact-checking, media-literacy programmes and tools to monitor disinformation campaigns. They help expose specific falsehoods and strengthen citizens' ability to spot manipulation, yet they struggle with limited resources, uneven reach and the rapid evolution of tactics such as AI-generated deepfakes and encrypted-channel mobilisation.

https://dig.watch/processes/un-gge

https://teaching.globalfreedomofexpression.columbia.edu/resources/countering-disinformation-promotion-and-protection-human-rights/

https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management

https://www.oecd.org/going-digital/governance-responses-to-disinformation.htm

Possible Solutions

- Clarifying international rules on information warfare:
  Establishing a shared understanding of what counts as information warfare, including cyber-attacks on critical infrastructure and coordinated disinformation campaigns, would make it easier for states to agree on red lines and acceptable behaviour.

- Addressing the absence of a dedicated mechanism:
  The complexity of information warfare suggests that a specialised international or regional mechanism may be needed to monitor major incidents, share technical findings and support states in prevention and response.

- Protecting societies during ongoing information operations:
  Regulating information warfare is more difficult when cyber-attacks and disinformation campaigns are already underway, so delegates could explore measures that specifically apply in crises, such as temporary coordination frameworks to protect elections and essential services.

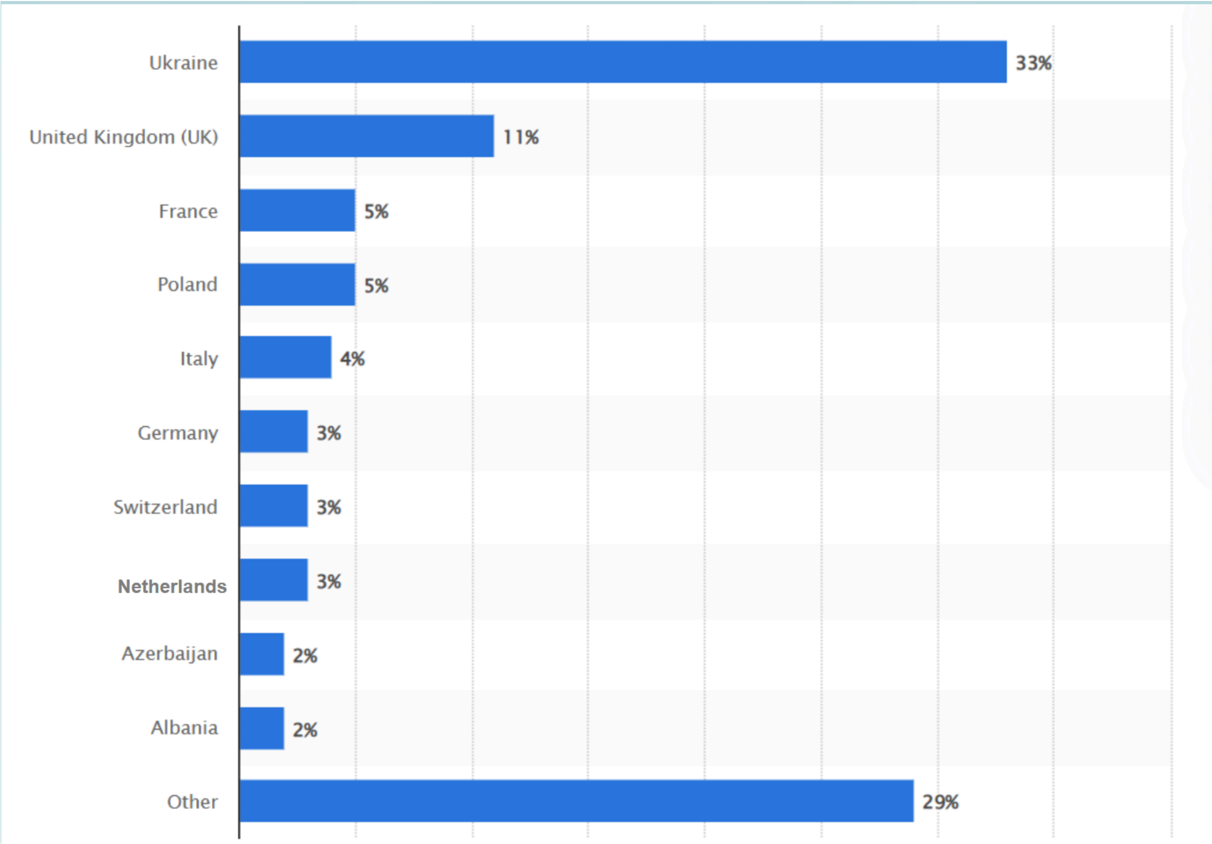
- Enhancing cooperation and transparency:
  Greater cooperation and transparency between states, platforms and relevant organisations about detected campaigns, technical methods, attribution processes and response measures can reduce mistrust and help build common approaches over time.

Questions delegates should consider during research:

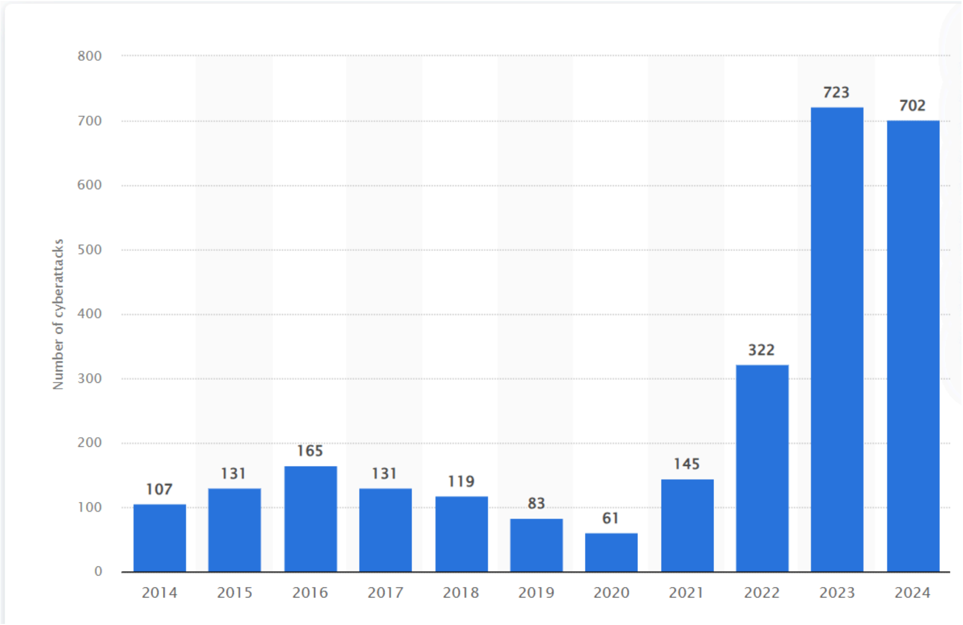
- Has my delegation's country been involved in or affected by major cyber-attacks or disinformation campaigns? If so, how?
- What is my delegation's country's official position on information warfare, cyber-operations and online disinformation?
- What capacities (technical, legal, diplomatic) does my delegation's country have to help tackle this issue at national, regional or UN level?
- What existing laws, policies or international commitments has my delegation's country adopted on cyber-security, information integrity or platform regulation?

Appendices

Appendix A: European countries most targeted by nation-state or state-affiliated cyber threat actors from July 2022 to June 2023



Appendix B: Annual number of cyber incidents with a political dimension worldwide from 2014 to 2024 YTD



Bibliography

- Plumb, C. (2024). Understanding the UN's New International Treaty To Fight Cybercrime. [online] United Nations University. Available at: https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime
- Office of Counter-Terrorism. (2024). Cybersecurity and New Technologies | Office of Counter-Terrorism. [online] Available at: https://www.un.org/counterterrorism/en/cybersecurity
- Kiener-Manu, K. (2019). Cybercrime Module 14 Key Issues: Responses to Cyberinterventions as Prescribed by International Law. [online] Unodc.org. Available at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/responses-to-cyberinterventions-as-prescribed-by-international-law.html
- Agarwal, D. (2026). UNSC_ Analysing the threat of cyber warfare in digital age. [online] Scribd. Available at: https://www.scribd.com/document/712980821/UNSC-Analysing-the-threat-of-cyber-warfare-in-digital-age
- United Nations Office on Drugs and Crime (2019). Cybercrime Module 14 Key Issues: Cyberespionage. [online] Unodc.org. Available at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html
- Plumb, C. (2024). Understanding the UN's New International Treaty To Fight Cybercrime. [online] United Nations University. Available at: https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime

- United Nations Office on Drugs and Crime (2019). Cybercrime Module 14 Key Issues: Cyberterrorism. [online] Unodc.org. Available at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html
- Kiener-Manu, K. (2019). Cybercrime Module 14 Key Issues: Hacktivism. [online] www.unodc.org. Available at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/hacktivism.html
- Kiener-Manu, K. (2019). Cybercrime Module 14 Key Issues: Information Warfare, Disinformation and Electoral Fraud. [online] www.unodc.org. Available at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare--disinformation-and-electoral-fraud.html
- UNODC (2019). Cybercrime Module 14 Key Issues: Cyberwarfare. [online] www.unodc.org. Available at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberwarfare.html
- Statista. (n.d.). Europe countries targeted by nation-state cyber threat actors 2023. [online] Available at: https://www.statista.com/statistics/1427845/nation-state-cyber-threat-most-targeted-countries-europe/
- Statista. (2024). Annual number of political intent cyberattacks global 2024 | Statista. [online] Available at: https://www.statista.com/statistics/1428487/number-political-intent-cyberattacks-annual/
- Human Rights Watch (2019). *Russia: New Law Expands Government Control Online. [online] Human Rights Watch*. Available at: https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online.
- Monde, L. (2026). *French IT giant Capgemini to sell US subsidiary after row over ICE links. [online] Le Monde.fr.* Available at: https://www.lemonde.fr/en/france/article/2026/02/01/french-it-giant-capgemini-to-sell-us-subsidiary-after-row-over-ice-links_6750021_7.html