DRAFT GENERAL REPORT
COMMITTEE ON DEMOCRACY AND SECURITY (CDS)

DEMOCRACY UNDER DIGITAL THREAT: BOLSTERING THE CYBERSECURITY OF ALLIED ELECTIONS

General Rapporteur: Dimitrios KAIRIDIS (Greece)

Founded in 1955, the NATO Parliamentary Assembly acts as a consultative interparliamentary organisation which is institutionally separate from NATO. This working document only represents the views of the Rapporteur until it has been adopted by the Committee on Democracy and Security. It is based on information from publicly available sources or NATO PA meetings – which are all unclassified.

010 CDS 25 E rev. 1 – Original: English – 16 July 2025

EXECUTIVE SUMMARY

Democracy is at risk when electoral processes and the actors that underpin them – political parties, candidates, media, and civil society, among others – are exposed to the dangers of cyberattacks. As information and communication technologies become increasingly integral to democratic systems, new vulnerabilities arise that malicious actors can exploit. Allied democracies constantly face such threats from authoritarian states, criminal groups, and rogue individuals.

The cyberattacks that these actors carry out not only jeopardise the integrity of election processes but also seek to erode public trust in democratic institutions and fuel political instability. In response, stepping up efforts to safeguard the democratic processes and values that define NATO and the Allies is an absolute necessity. Secure and credible elections are important to national stability, and thereby to collective resilience, making it imperative to address these threats.

This draft report begins by outlining the most common targets for cyberattacks within election contexts and detailing the main cyber threat actors, their motivations, and tactics. It further examines the challenges democracies face in strengthening electoral cybersecurity and reviews recent measures undertaken by Allied countries and NATO to prevent, mitigate, and respond to cyberattacks against elections and the broader democratic ecosystem. The draft report concludes with policy recommendations aimed at bolstering these efforts to ensure that Allied democracies remain secure.

TABLE OF CONTENTS

Acknowledgement: The Rapporteur extends appreciation to the Committee's Director, Nathan Robinson Grison, and its Researcher, Anaïs Fiault, for their contributions to this report.

I- INTRODUCTION

1. In today's increasingly digitalised world, technology has woven itself into the very fabric of daily life, touching every corner of our existence. Democratic processes are no exception. **Elections**, the very embodiment of the people's will and the cornerstone of democracy, now **increasingly rely on information and communication technologies**. Yet, with the undeniable strides in technological advancement come new vulnerabilities, that can be exploited by malicious actors. These risks are further exacerbated by the emergence of cyber space as a new frontier for strategic competition and criminal activity. As a result, **the spectre of cyber interference in elections has loomed ever larger in recent years**. In 2022 alone, over a quarter of national elections worldwide were marred by at least one reported cyber incident (Canadian CSE, 2023).

2. Today, technology is embraced by various democratic actors throughout the election cycle. States rely on it **to plan and administer their elections.** During the pre-election phase, it may be used to prepare voter registries, register candidates, delineate constituency boundaries, and plan the location and staffing of polling stations. During the voting period, it may assist with voter identity verification, ballot casting and vote counting, transmission, and tabulation, extending to result publication and display. Other essential election stakeholders – such as political parties and candidates – rely on digital tools as well **to communicate, organise their activities, and safeguard critical information.** In many cases, the integration of technology into elections has brought **tangible benefits** – from the increased efficiency and accuracy in the election process to greater accessibility for voters, improved communication with citizens, and the prevention of certain types of electoral fraud. However, the broader digitalisation of democratic processes has introduced a **new array of risks and vulnerabilities for all democracies**.

3. Cyberattacks on elections and the broader democratic ecosystem that underpins them are particularly insidious, **threatening both democracy and national security**. Secure and credible elections are the bedrock of government legitimacy. Regardless of their eventual success, cyberattacks cast a shadow of doubt over election outcomes. This may erode the legitimacy of elected officials, threaten orderly democratic transitions, and even trigger civil unrest. Additionally, cyberattacks may undermine broader trust in democratic systems, paving the way for the rise of anti-democratic sentiments and foreign interferences. Given their profound impact on a country's stability, it is essential to regard the electronic systems used throughout electoral processes as **critical national infrastructure**. While Allies have started taking measures to enhance the cybersecurity of their democratic processes, it is crucial to further bolster those efforts to face this rapidly growing threat.

4. **While elections are fundamentally a national prerogative, NATO can assist Allies** in strengthening their cyber defence. This is crucial not only for the stability of individual Allied countries, but also for **the resilience of the Alliance as a whole.** As highlighted in the Alliance's 2022 Strategic Concept, authoritarian forces are actively seeking to interfere in Allied democratic processes through hybrid tactics, both directly and via proxies (NATO, 2022). They seek to exploit the openness and transparency inherent to democratic societies to weaken Allied countries. As a result, 25% of elections affected by election-related cyberattacks worldwide were held in NATO countries between 2015 and 2022 (Canadian CSE, 2023). As new cyber threat actors continue to emerge, further complexifying Allied responses, NATO can help coordinate collective responses to cyber threats and thereby indirectly enhance the cyber resilience of Allied democratic processes.

5. More broadly, **defending democratic principles and values is woven into the very identity of the Alliance**, as enshrined in the 1949 North Atlantic Treaty. An attack on elections is fundamentally an attack on democracy itself. NATO and the Allies must vigilantly safeguard their democratic way of life against the relentless onslaughts of malevolent forces intent on undermining

democracy and promoting their authoritarian models of governance both within our Alliance and beyond.

6. Despite the growing number of cyberattacks targeting election processes, many cyber threat actors have struggled so far to achieve significant effects when interfering with elections. Even when their cyberattacks do succeed, malicious actors rarely succeed in reaching their overarching goals. Still, should they succeed, the effects would be devastating to any democracy, which is why **Allies must rapidly step-up their efforts to protect their election processes** from current and emerging cyber threats.

II- ELECTORAL CYBERSECURITY: TARGETS AND THREATS

A. THE ELECTORAL INFRASTRUCTURE AND THE DEMOCRATIC ECOSYSTEM AS TARGETS FOR CYBERATTACKS

7. Election cyber infrastructure is a key target for cyber threat actors. **Core election infrastructure** includes machines and electronic systems directly managed by election management bodies, typically involving hardware and software for voter registration systems, voting equipment, and result tabulation and transmission technology. In addition, election management bodies often rely on the internet and third-party suppliers to host and manage their core infrastructure. This **supporting infrastructure** constitutes an additional vulnerability for election management bodies. Hardware, such as computers and mobile devices, as well as internet-connected platforms, like websites, social media accounts, and messaging applications, may constitute attractive targets for attackers. Because they are usually accessible via the internet, voter registration databases and results tabulation and transmission systems have been especially vulnerable to attacks in recent years (USAID, 2022).

8. Beyond these assets that are integral to the voting process, cyber attackers increasingly target actors belonging to the wider **democracy ecosystem** (OSET Institute, 2020). Although these actors operate independently from public authorities, they play an essential role in democratic processes, with their actions impacting election outcomes. A successful cyberattack against these actors may undermine the integrity of elections, sway results and undermine public trust in the broader process. Among those actors, **political parties and candidates** are the most frequent targets during and around elections. In June 2024, for example, cyberattacks targeted several political parties and candidates in Germany and the Netherlands during the European Parliament elections (Reuters, 2024; Hartog, 2024). Attacks on email accounts especially have been on the rise (NCSC, 2023). In another example, in 2021 for instance, the German Foreign Office reported an email phishing campaign aimed at parliamentarians. The goal was reportedly to take control of their accounts and leak confidential information to sway election results (Cerulus and Klingert, 2021). In May 2025, Polish Prime Minister Donald Tusk said that his party's computer systems had been targeted in a cyberattack during the presidential election campaign (Blackburn, 2025). **Media outlets and journalists** are another frequent target for cyberattacks, as they play a crucial role in covering the electoral process and reporting on the results. **Fundraising and civil society organisations**, especially those involved in election monitoring activities, may also constitute valuable targets for cyber attackers. Overall, because their cyber infrastructure is often less secure, targeting these electoral stakeholders is a low-cost high-impact strategy for cyber attackers (Vanderlee and Collier, 2024).

9. Women often face unique challenges when subjected to gender-based cyberviolence, which is increasingly **used as a tactic to intimidate and harass women** involved in public and political life, including politicians, journalists, and activists. These cyberattacks can inflict serious reputational damage and psychological harm, deterring women from running for office or fully engaging in

democratic processes. Such targeted harassment undermines not only individual participation but also the broader legitimacy and inclusiveness of elections, as the full participation of women is essential for a healthy and representative democracy. Addressing this issue is crucial to safeguarding the integrity of democratic systems.

B. TYPOLOGY OF THREATS TO ELECTORAL PROCESSES

10. Malicious cyber operations pose distinct, yet interconnected, threats to elections. First, cyberattacks may **disrupt electoral processes by interfering with their preparation and proper functioning**. Cyber attackers may try to do so by compromising the availability or integrity of core election infrastructure. In 2019, for instance, a ransomware attack targeted the North Macedonian State Election Commission one month before the presidential election. As a result, the Commission's key information and communication systems temporarily stopped functioning, impacting the accessibility of the voter registry and the email servers and database used by public employees to appoint electoral boards at a critical time (van der Staak and Wolf, 2019). Blocking or tampering with voting registration systems can result in voters being turned away from polling stations. In addition, stolen information from electronic voter databases may also be used to dissuade voters from voting or provide them with misleading information about when, how, or where to vote. Attackers may also disrupt the electoral process by targeting actors from the broader democracy ecosystem. For instance, cyber intrusions may prevent political parties or candidates from running their campaigning operations smoothly. Many distributed denial of service (DDoS) attacks have targeted high-profile campaign and political party websites in recent years, including in 2024 during elections in France, the UK, the Netherlands, and the U.S. (Tomé and Woolbright, 2024).

11. Second, cyber operations may **subvert elections by falsifying or swaying results**. Attackers may tamper with electronic voting systems to alter how votes are recorded, for example. In recent years, attacks have especially targeted tabulation and result transmission systems to alter the results of the vote. DDoS attacks have also targeted websites used by election management bodies to publish vote tallies on election day, including in the Czech Republic in 2017, Finland in 2019, and Sweden in 2018 and 2022 (Reuters, 2017; Pohjanpalo, 2019; NIS Cooperation Group, 2024). Furthermore, attackers may engage in targeted voter suppression by using stolen information to reduce the turnout of specific groups with known voting preferences. During the 2020 U.S. presidential elections, for instance, according to a U.S. Justice Department investigation, two Iranian hackers broke into voter registration systems and used the stolen data to send threatening emails to thousands of Democratic voters (U.S. Department of Justice, 2021). More often, however, cyber intrusions seek to sway public opinion and influence voting intentions by damaging the reputation and popularity of certain candidates. Leaking sensitive information can discredit candidates and derail their message at a crucial turning point in their campaigns. Although it is not assessed as having had an impact on the result of the election, a well-known example of this is the release of 20,000 internal emails from the Democratic National Committee and Hillary Clinton's team during the 2016 U.S. presidential campaign, attributed to hackers affiliated to Russian intelligence services by the U.S. Department of Justice (U.S. Department of Justice, 2019).

12. Third and lastly, cyberattacks may **harm trust in electoral processes and democracy**. Cyberattacks can directly undermine public perceptions about the integrity of elections and the legitimacy of their outcome. In turn, this can weaken the legitimacy of elected officials and result in disenchantment with democratic processes as a whole. Whether they are successful or not, cyberattacks are always disruptive as they showcase the vulnerability of electoral processes. For instance, in 2024, the British government disclosed that Chinese-backed hackers had breached into the Electoral Commission's systems, accessing the personal information of 40 million people between 2021 and 2022. While there was no evidence that the leaked data had been used to interfere with the elections themselves, the breach raised considerable public concerns about the security of the UK's electoral processes and institutions (Uddin, 2024). Such incidents could damage voter confidence by giving the impression that elections can be easily subverted. In some cases, cyber operations and disinformation campaigns have even been used jointly to deliberately sow

doubts about the safety and integrity of elections. During the 2020 U.S. presidential election cycle, for instance, the U.S. Justice Department also found that Iranian hackers had breached into voter registration databases and used the stolen data to fabricate and disseminate a video containing disinformation designed to leave the impression that ballots could be fraudulently submitted (Tulp, 2022).

III- CYBER THREAT ACTORS, MOTIVATIONS, AND TECHNIQUES

A. MOST COMMON CYBER THREAT ACTORS

13. Just like the number of targeted institutions has grown, the election cybersecurity threat actor landscape has expanded in the last decade. Such actors now range from foreign to domestic actors, and from criminal groups to independent hackers. Today, **authoritarian foreign state actors** represent the most serious threat to elections**.** From 2015 to 2020, 76% of malicious cyber activities targeting democratic processes for which there has been attribution were conducted by state-sponsored actors (Canadian CSE, 2021). This includes entities working directly within state agencies (usually security services) or acting on their behalf. Because of their greater operational capacities, state coordinated campaigns are generally more disruptive to electoral processes. Foreign state attacks are often geopolitically motivated: they target countries of strategic significance to them to advance core interests. They may try to get candidates with views or policies favourable to their regime's interests elected, seek retribution for another country's foreign policies choices, and/or delegitimise democracy as a political model to further their own ideological views and autocratic models. Since 2021, groups with links to Russia and China have conducted the majority of attributed cyber threat activities against foreign elections (Canadian CSE, 2023). So far, there is no clear evidence that authoritarian states have closely collaborated to leverage their interference campaigns against foreign elections. However, collaboration is already thriving in other domains, including in the information sphere, indicating that this risk cannot be ignored.

14. The **Russian Federation** is by far the state most actively involved in cyberattacks against elections. It has a well-documented history of interfering in elections in NATO and partner democracies, including most recently in the U.S., UK, France, and Ukraine. Its goals are both political and disruptive in nature. Russia is intent on undermining trust in democracy and fuelling instability, while promoting parties and candidates that it sees as favourable to its interests. Cyberattacks are thus part of Moscow's hybrid warfare toolbox to destabilise democratic countries, undermine the international rules-based order, and pursue its deleterious geopolitical goals. Russian threat actors are usually connected to state security services and involved in a wide variety of other cyber-enabled activities, including disinformation campaigns. The hacker groups "Fancy Bear" and "Cozy Bear", also respectively known as APT28 and APT29, to name only two, are Russian threat actors that have been linked to the Kremlin's Military Intelligence Directorate (GRU) and Foreign Intelligence Service (SVR) (USAID, 2022). They have been operating since the mid-2000s and are responsible for the most high-profile cyber operations against elections in the past years (Vanderlee and Collier, 2024). In 2025, French authorities attributed to the "Fancy Bear" group the cyberattacks on President Emmanuel Macron's 2017 election campaign, which resulted in the disclosure of thousands of confidential campaign documents (see paragraph 23) (Caulcutt, 2025).

15. **The People's Republic of China** (PRC) is another major cyber threat actor. In its neighbourhood, especially in Taiwan, China has deployed offensive cyber capabilities to disrupt elections. There, the use of cyber interference operations aligns with its broader foreign policy goals: to promote pro-China narratives and push prominent individuals to advocate for its interests. During the 2024 Taiwanese presidential election, for instance, PRC cyber actors unleashed an unprecedented number of cyberattacks against critical infrastructure and government agencies in the weeks leading up to and following the election (Vanderlee and Collier, 2024). This was done in combination with large-scale disinformation campaigns targeting candidates. China's actions illustrate the potential of cyber operations to cause disruption during elections by targeting a country's broader national critical infrastructure. In Allied states, China's efforts to interfere in

elections appear to be less aggressive and more targeted, primarily relying on cyber espionage and data theft. As China focuses on expanding its cyber capabilities, including within its armed forces, its disruptive cyber potential is, however, likely to increase (Garriaud-Maylam, 2022; Rajagopalan, 2024).

16. **Iran** is another emerging cyber threat state actor. Historically, Iran's cyber campaigns have been aimed at countries involved in nuclear negotiations and/or offering support to Israel (Vanderlee and Collier, 2024). In the West, its efforts so far have primarily focused on targeting U.S. election infrastructure and disseminating election-related disinformation during the last three election cycles. According to U.S. officials, the most significant cyber incidents from the past years can be traced back to an Iranian company called Emennet Pasargad, which was contracted by the Iranian government (FBI, 2022). During the 2020 U.S. presidential elections, it engaged in cyber intrusion activities, data theft, information operations, and attempts at voter intimidation. Most recently, U.S. intelligence agencies denounced Iran's attempts to hack into the campaigns of the Democrat and the Republican Parties in the runup to the 2024 presidential elections (FBI, 2024).

17. Finally, **North Korea** has also proven its disruptive potential in electoral contexts. The country has a track record of conducting cyber operations and other disruptive activities during South Korean election cycles aiming at inciting voters to elect candidates with a more moderate approach to North Korea (Choi, 2022). During the 2020, 2022, and 2024 election cycles, Google reported an increase in malicious cyber activities attributed to North Korea targeting South Korean security, defence, and diplomacy experts, as well as South Korea-based media organisations and NGOs (Vanderlee and Collier, 2024). North Korea also has a history of increasing provocative military actions and information operations around South Korean elections.

18. Authoritarian governments also deploy **cyber operations to target electoral stakeholders within their own countries**, including opposition leaders, independent journalists, and civil society organisations. These actions are designed to suppress political dissent and ensure the survival of the regime. More broadly, these states exploit the cyber space to maintain tight control over their societies, curbing the potential for opposition by exerting dominance over digital infrastructure.

19. **Domestic non-state actors** represent a growing threat as well. The main threat usually comes from ill-intentioned and/or politically motivated groups and individuals, such as campaign workers and political activists. In some cases, the cyber threat has been fuelled by misinformation and conspiracy theories (Bay, 2024). In addition, domestic and foreign actors are increasingly becoming *de facto* partners when it comes to spreading election-related falsehoods. For instance, French far-right groups inadvertently helped disseminate and fuel Russian disinformation during the Russian-sponsored "hack and leak" operation that targeted the 2017 French election (see paragraph 23) (Tenove et al., 2018).

20. Finally, **criminal organisations** are involved in election-related cyber operations. Between 2015 and 2020, 8% of malicious cyber interventions against democratic processes and institutions were attributed to criminally motivated actors (Canadian CSE, 2021). With no specific interest in the electoral processes themselves, they are involved in cybercrime primarily for financial gain, using tactics like ransomware attacks to extort money from victims. The rise of cybercrime "as a service" is further complexifying the cyber threat landscape as criminal groups increasingly sell their resources, usually malware, access to an infected computer, or compromised data, to actors seeking to interfere in elections (ENISA, 2023). Not only can cybercrime "as a service" help malicious actors lacking resources or experience conduct more effective cyber operations against elections, it can also help them mitigate the risk of retaliation and escalation by making attribution more complex.

B. MOST FREQUENTLY USED TACTICS AND TECHNIQUES

21. The **modus operandi** of cyberattacks on elections varies. Using vulnerabilities in software, hardware and/or human behaviour, cyberattacks usually aim to breach the confidentiality, integrity

and availability of data and systems. In election contexts, this includes accessing and leaking private or confidential information relating to voters, political parties or candidates; tampering with the accuracy of the information being processed by electoral systems either by deleting or manipulating data; and disrupting the availability of essential systems like online voter registration platforms or result websites by encrypting data or making networks inaccessible to users. Below is a summary of the most common cyberattacks targeting electoral processes.

Most common cyberattacks	
Hacking	Attackers gain unauthorised access to and control of digital devices or digital systems.
Zero-day attack	Attackers take advantage of a security flaw in software or hardware unknown to vendors or manufacturers to break into a system and launch a cyberattack.
Phishing	Attackers trick users into disclosing sensitive information, such as usernames and passwords, to gain access to accounts or networks. Alternatively, attackers may seek to trick users into clicking on links to deploy a malware and compromise their systems. This is usually done via email, phone calls or text messages.
Social engineering	Similar to phishing, attackers exploit human psychology by posing as a trusted source to trick users into disclosing sensitive information that can be used to compromise electronic systems.
Ransomware	After gaining access to a network, attackers deploy software that encrypts the data. Attackers then contact the victim and offer to decrypt the data in exchange for money. Before file encryption, the data is often exfiltrated to be sold or used to exert further pressure.
Wiperware	After gaining access to a network, attackers deploy malware that erases or "wipes" data from a system's hard drive.
Distributed denial of service (DDoS)	Attackers deploy multiple connected online devices (botnets) to overwhelm a target website or service with fake traffic, causing it to become unavailable. This is often done during critical and visible phases.
Defacement	After gaining access to a network, attackers manipulate the appearance of a public website to create confusion, spread disinformation or cause reputational damage.

22. **Advanced Persistent Threats** (APT) are the most destructive cyber threats and rely on a combination of these techniques. These are well-planned, multi-phased attacks conducted by well-resourced actors over a long period of time. They are usually carried out or sponsored by states (van der Staak and Wolf, 2019). APTs require substantial research and experimentation to identify potential vulnerabilities in target systems. They also use state intelligence to engineer sophisticated operations targeting high value individuals or entities. The 2014 Russian-backed attack on Ukraine's Central Electoral Commission (CEC) is a notorious example of such an attack. Four days before the national vote, the CEC's servers were breached, with critical data and systems destroyed using wiperware, rendering the vote-tallying system temporarily inoperable. On election day, the CEC's website faced a DDoS attack which momentarily shut it down. A Russian TV station broadcasted false election results showing a minor candidate as the winner. Ukrainian cybersecurity personnel discovered an image containing the same fake results on the CEC servers. If this image had not been found, it would have been displayed instead of the real results when the polls had closed, thus presumably creating confusion and undermining trust in the process and the real results (CCDCOE, 2021).

23. Cyber intrusion activities are also **increasingly combined with information operations**. Because this issue has been thoroughly covered in past reports, the Rapporteur has chosen to focus primarily on cyber interferences in the present draft report, while still acknowledging the strong synergies between both threats. “Hack and leak” operations typically rely on both. For instance, Russian intelligence services hacked into an email account belonging to the British trade minister and leaked confidential UK-U.S. trade documents in an attempt to influence voters ahead of the 2019 British General Election (Sabbagh, 2020). In some cases, forged documents and altered data may be released alongside authentic data – these are known as “tainted leaks” (Tenove et al., 2018). This was the strategy used by Russian-backed hackers during the 2017 French presidential campaign. After hacking into Emmanuel Macron’s campaign team’s email accounts, attackers released the stolen data online alongside false documents containing allegedly compromising information about offshore accounts, tax evasion and other fabricated wrongdoings by Emmanuel Macron and his campaign. “Hack and post” operations are another strategy which typically relies on gaining control over websites to publish misleading, false, and/or confusing information. During the 2024 European Parliament elections, for example, after gaining unauthorised access to the website of the Polish state news agency, hackers published a false article about military mobilisation on it, in an attempt to influence voters. According to the Polish government, the attack is likely to have emanated from Russia (Gregory, 2024). In 2018, a similar incident was reported on the popular Latvian social network Draugiem.lv with pro-Russian messages published on its front page on election day (CEPA, 2018).

24. The election cyberthreat landscape is evolving rapidly as a result of technological innovations. **Developments in artificial intelligence** (AI) are amplifying cyber risks by allowing for greater sophistication in cyberattacks. AI is trained to analyse vast amounts of data and mimic human behaviour and may thus be misused to scale up and deploy more effective phishing or social engineering attacks (Arctic Wolf, 2024). Threat actors with less technical expertise may also use AI to generate malware that is harder to detect or to optimise the use of botnets for DDoS attacks (Easterly et al., 2024). In February 2024, for instance, OpenAI announced that state-affiliated cyber threat accounts had used its services to gather open-source information, assist with coding, and generate content likely used for phishing campaigns (OpenAI, 2024). Since 2021, AI-generated content relating to elections has increased and is likely to continue growing as this technology evolves (Canadian CSE, 2023). However, while the risk of misuse by cyber threat actors is real, AI may also be leveraged by cybersecurity professionals to uncover vulnerabilities in electronic systems and help protect them from attackers.

25. Lastly, cyber threat actors may increasingly try to harness the power of **social media algorithms** to meddle in elections. In December 2024, Romania’s Constitutional Court annulled the country’s presidential elections after finding that a covert influence operation on TikTok played a decisive role in the victory of a far-right independent candidate in the first round. According to Romanian intelligence services, TikTok’s algorithm was successfully manipulated to massively promote the candidate’s content, thereby swaying voting intentions. They also flagged other irregularities, including TikTok’s failure to label the candidate’s content as election campaign material, as required by Romanian law (Haeck et al., 2024). Although the attack has yet to be attributed, Romania’s intelligence service said the attack was likely state-sponsored, mirroring influence operations conducted by Moscow on social media during the 2019 Ukrainian and 2024 Moldovan elections (Romanian Presidency, 2024). This incident could create a dangerous precedent for malicious cyber actors seeking to exploit regulatory and transparency gaps on social media platforms.

IV- CHALLENGES TO ENHANCING ELECTORAL CYBERSECURITY

A. THE DIFFICULT RESPONSE TO CYBERATTACKS

26. Responding to cyberattacks is arduous, not least because of the **difficulty to attribute** them to specific threat actors. Governments often struggle to obtain proof of the perpetrators' identity. Attacks can be launched from anywhere and may involve multiple actors. Foreign state actors often use third-party proxies to prevent their activities from being traced back to them and avoid attribution. The growth of cyberattacks "as a service" makes their attribution to specific actors all the more difficult. In 2022, 85% of cyber threat activities targeting elections were unattributed (Canadian CSE, 2023). This makes deterring cyberattacks and holding their perpetrators accountable complex.

27. **Institutional fragmentation** is another obstacle to building effective responses to cyberattacks. Cybersecurity bodies often have limited electoral expertise. Because election infrastructure has yet be recognised as critical by most countries, election-related cyber threats may be given less priority than threats to military, health, or energy infrastructure. Often, electoral cybersecurity falls under the responsibility of multiple entities, or there is a lack of clarity about whose jurisdiction it falls under altogether. Having a network of different jurisdictions, competences, and responsibilities can result in fragmented electoral cyber defence strategies. Difficulties relating to interagency collaboration may also hamper response efforts when incidents do occur.

28. Another challenge is the **absence of adequate national laws and international norms** to prosecute those responsible for cyberattacks. Domestically, states may find it difficult to initiate criminal prosecution because they lack a coherent legal framework for cybersecurity. Relevant provisions are often scattered in multiple pieces of legislation, some of which may be outdated. Even when appropriate legal frameworks do exist, meaningful enforcement is usually lacking. As a result, arrests for cyberattacks remain very rare. There are many challenges to investigating and prosecuting election-related cybercrimes, including difficulties with attribution and the location of attackers abroad in a different national jurisdiction. Despite the need for international legal cooperation, most states still have different policies and approaches to cyber criminality (Garriaud-Maylam, 2022). The Russian Federation, for instance, refuses to extradite its citizens on cybercrime charges and has not signed the Council of Europe's 2001 Budapest Convention. Apart from this partly outdated convention, there are no binding international legal instruments to hold cyber attackers accountable. Since 2017, efforts to come up with a UN cybercrime treaty have been somewhat controversial, which illustrate the difficulties of adopting common laws and standards in this field (Hartmann, 2024). While a text was finally adopted by the United Nations Ad Hoc Committee on Cybercrime in August 2024, it is widely opposed by democratic nations, human rights organisations, and a coalition of technology companies. It thus remains to be seen whether enough states will ratify the new Treaty for it to enter into force.

B. HURDLES TO ENHANCING CYBER SECURITY CAPACITIES

29. The **periodic nature of electoral cycles** constitutes a challenge for electoral bodies seeking to improve their cybersecurity capacities. Election technology is usually only activated for a few days or a few hours every few years. As a result, electoral actors often struggle to find adequate time, funding and human resources to develop long-term cybersecurity strategies. Cybersecurity is not incorporated into IT infrastructure and election infrastructure closely monitored early enough. Staff may be onboarded without sufficient cyber training. Yet, to prevent and mitigate cyber risks, electoral cybersecurity must be a comprehensive, long-standing, and continuous commitment. Indeed, the most disruptive cyber operations often start several months before election day.

30. **Poor digital literacy and cybersecurity awareness** are other enduring challenges. Studies report that 98% of cyberattacks can be avoided by following basic cyber-hygiene practices (Microsoft, 2022). Poor digital literacy levels in election stakeholders and individuals administering

election technology makes them less likely to identify and mitigate threat vectors such as malicious email attachments. Limited understanding of their roles in ensuring the cybersecurity of the electoral process may also lead to mismanagement when incidents do occur (Klein, 2021). Citizens' poor understanding of how election technology works can facilitate misrepresentations about its security and lay the groundwork for effective disinformation campaigns. Malicious cyber actors are aware of these vulnerabilities and actively exploit them to interfere in elections.

31. Ensuring the security of election infrastructure **supply chains** is another challenge for electoral authorities. Their reliance on externally sourced components and services creates vulnerabilities at all levels. Cyber attackers may target election infrastructure suppliers during the design, production, or distribution phases to identify or introduce vulnerabilities before the technology is even delivered to election management bodies. Limited understanding, visibility, and control over the risks pertaining to their supply chain makes the comprehensive management of cyber risks more difficult for election management bodies.

C. CHALLENGES TO BOLSTERING THE CYBER SECURITY OF THE DEMOCRATIC ECOSYSTEM

32. Democratic states must be **transparent** about the risks they face, despite the incentives they may find in certain cases to remain silent about cyberattacks targeting their electoral processes. Keeping information about failed or minor cyberattacks confidential may be tempting to avoid spreading confusion and undermining public confidence in the elections. Some agencies may refuse to divulge information about breaches to the public to avoid disclosing how they obtained that information. Yet, transparency is key to strengthening public confidence in election technology, as well as in democratic institutions' ability to protect elections from attacks. High public trust in democratic institutions also makes it more difficult for malicious cyber actors to successfully disrupt elections.

33. **Political polarisation** may increase the risk of cyber interference in elections. High levels of political polarisation may generate distrust in political institutions, including electoral management bodies. This, in turn, may raise the number of domestic cyber threats. As already seen in some countries, hyper-partisanship can create incentives to tamper with election infrastructure and spread disinformation if believed to benefit the interests of one's political group. Political polarisation can also lay the groundwork for foreign interference in elections, with malicious state actors actively exploiting this vulnerability to conduct more effective cyber campaigns.

34. More broadly, **state intervention** in election cybersecurity remains a grey area. State intervention, if perceived as excessive, can provoke suspicion, and rapidly become counterproductive. To address domestic cyber threats effectively, for instance, states must find a balance between using intelligence and gathering sensitive and personal data to identify and mitigate potential threats and addressing populations' legitimate reluctance to be subjected to increased surveillance. Election management bodies also often have restrictions on engaging with political and democratic actors on cybersecurity issues for reasons of impartiality. Finding the appropriate level of cyber support for political parties and candidates, as well as the media and relevant civil society organisations without compromising their independence remains a challenge.

V- NATIONAL AND COLLECTIVE EFFORTS TO ENHANCE ALLIED ELECTORAL CYBERSECURITY

A. NATIONAL LEVEL ENDEAVOURS TO PROTECT DEMOCRACIES AGAINST CYBER THREATS

35. At the national level, faced with growing cyber threats to their democracy and elections, most Allied states have strengthened their cybersecurity capabilities in recent years. Many have undertaken efforts to improve the cybersecurity of their electoral processes and democratic actors. **At the strategic level**, Allied states have started adopting more comprehensive national cyber security strategies. Italy's 2022-2026 National Cybersecurity Strategy, for instance, acknowledges the menace posed by hybrid threats to democratic systems (ACN, 2022). More explicitly, Latvia's 2023-2026 Cyber Security Strategy recognises the importance of ensuring the security of information and communication technology systems used in electoral processes to preserve the integrity of elections (Latvian MOD, 2023). These strategies are important as they promote public awareness and often provide a roadmap to increase democratic cyber resilience. Some Allies have taken the step to define election infrastructure as "critical infrastructure", further raising the profile of the issue. In 2017, the U.S. Department of Homeland Security officially designated election infrastructure as a sub-sector of the broader Government Services and Facilities critical infrastructure sector. Congress subsequently provided increased federal funding to help states better safeguard their election systems against cyberthreats, while election officials at all levels adopted cybersecurity best practices in their daily operations. As a result, public officials assess that the U.S. election system has become far more resilient to cyberattacks (Tisler and Norden, 2023).

36. **At the institutional level**, Allied countries have established national cyber security agencies responsible for strengthening their cyber defence. These agencies are increasingly involved in election cybersecurity and play an important role in raising awareness of the issue. Many of them also have emergency response teams that are increasingly deployed during elections to protect critical infrastructure and manage incidents that may occur. For example, Spain's National Cybersecurity Institute and its computer emergency response team are part of a network of state organisations responsible for election security that has been deployed for every election since 2019 (INCIBE, 2024). In 2024, they set up a helpline for citizens and digital service providers to quickly report and manage cyber incidents during the European Parliament elections. Other Allied nations have set up units specifically dedicated to election cybersecurity within their administration. In 2022, for instance, the British government established a Defending Democracy Task Force reporting to the National Security Council to protect, *inter alia*, the integrity of British elections from foreign interference. Its Joint Election Security Preparedness Unit is responsible for the overall coordination of electoral security and the protection of core electoral infrastructure (NCSC, 2023).

37. **At the regulatory level**, some Allied parliaments have updated and strengthened national legislation to better address electoral cybersecurity and foreign interference in democratic processes. In 2018, for instance, the Secure Elections Act was introduced in the U.S. Senate to help the federal administration protect American elections against cybersecurity threats by granting the Department of Homeland Security responsibility for sharing cybersecurity information with other federal entities and election agencies and expanding the role of the Election Assistance Commission in cybersecurity (CRS, 2018). In Canada, Bill C-70, *An Act Respecting Countering Foreign Interference*, was adopted by the Canadian Parliament in June 2024. The purpose of this act is to deter foreign actors from attempting to covertly influence political or governmental processes in Canada and raise public awareness on this issue to strengthen national security (Parliament of Canada, 2024). Nevertheless, **the fragmentation of legislation and regulations covering election cybersecurity remains an issue**. Relevant regulatory frameworks often come from multiple legislative texts covering different components, such as national critical infrastructure or personal data.

38. In many Allied countries, national agencies have started **providing assistance to election stakeholders and democratic actors to help them build the technical capacity to prevent and react to cyber threats**. During the Czech Republic's 2017 and 2018 parliamentary and presidential election cycles, for instance, the National Cyber and Information Security Agency provided training to the Czech Statistical Office, whose employees were involved in securing electoral processes. Both organisations continue to collaborate to this day (NIS Cooperation Group, 2024). Canada's Cyber Center, the UK's National Cyber Security Centre and the U.S. Cybersecurity and Infrastructure Security Agency have all also produced cyber security guides, training courses, and other free online tools that can be used by election management bodies, national and local government officials, as well as political parties and candidates. Romania's Permanent Election Commission issues cyber hygiene training programs for political parties to protect parties' internal information and election-related data (van der Staak and Wolf, 2019).

39. Fully aware that cyber threats know no borders, NATO members have also been actively involved in **international efforts to raise awareness on election cybersecurity and promote the development of international standards**. All Allies are parties to the Council of Europe's 2001 Budapest Convention on Cybercrime which sets out norms and procedures for responding to cybercrime. Some have been actively engaged in cyber diplomacy efforts. In 2018, for instance, France launched the Paris Call for Trust and Security in Cyberspace, building on UN norms of responsible state behaviour in cyberspace. "Defend electoral processes" is one of the Call's nine principles and involves strengthening countries' ability to prevent foreign actors from interfering in their electoral processes through malicious cyber activities (Paris Call, 2018). A number of Allied countries also participated in the 2018 annual Copenhagen Democracy Summit which helped set up the Transatlantic Commission on Election Integrity. The Commission serves as a forum to raise public awareness and share best practices between decision-makers and institutions (Alliance of Democracies, 2024). Many Allies have also contributed to strengthening regional norms through their European Union membership. The EU has issued two cybersecurity compendiums on elections in 2018 and 2024, which provide guidelines and best practices for election management bodies. Since 2015, Allied states have been pushing at the UN level for the international community to recognise the unlawfulness of cyber operations targeting cyber infrastructure, including electoral infrastructure (Garriaud-Maylam, 2022). Despite these efforts, **international standards and norms regulating cyberspace remain fragmented and insufficiently implemented**.

B. NATO'S CYBER RESILIENCE ROLE

40. While the electoral cybersecurity is a national prerogative, **NATO has a role to play in helping Allies enhance their electoral cyber-resilience** as part of its **cyber defence policy**. NATO protects its own networks but also helps Allies strengthen their national cyber resilience by serving as a platform for consultation and information sharing. In 2014, the Allies recognised cyber defence as a core part of collective defence, declaring that a cyber-attack against one or more Allies could lead to the invocation of Article 5 of the North Atlantic Treaty. Two years later, Allies agreed to implement a Cyber Defence Pledge to strengthen national networks and infrastructure. In 2021, Allies endorsed a Comprehensive Cyber Defence Policy to support NATO's three core tasks, acknowledging that these efforts must be carried out at the political, military, and technical levels. At the 2024 Washington Summit, NATO leaders agreed to establish a NATO Integrated Cyber Defence Centre to further enhance the protection of NATO and Allied networks, improve situational awareness, and enhance collective resilience and defence.

41. NATO recognises the need for a **comprehensive approach to cyber security that includes civilian networks and infrastructure**. The 2022 Strategic Concept mentions that malign actors are using cyberspace to "degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities" (NATO, 2022). In 2023, Allied leaders also adopted an Enhanced Cyber Defence Pledge, restating their commitment to enhance their national cyber defence while further strengthening civil-military cooperation and engaging with the private sector. In the declaration adopted at the Hague Summit

in June 2025, Allied heads of state and government reaffirmed their commitment to "safeguard […] freedom and democracy" across the Euro-Atlantic area. Tackling cyber-interference in elections must be a component of that commitment. At the Summit, Allies also agreed to raise defence spending to 5% of GDP by 2035, with 3.5% allocated to core defence and 1.5% to strategic investments aimed, among other objectives, at reinforcing resilience (NATO, 2025). It is essential that a share of these investments be directed toward countering electoral cyber-interference, particularly from authoritarian regimes seeking to erode our democratic institutions and fragment our social cohesion.

42. Protecting Allies against cyber threats to their electoral processes also falls under NATO's role in **supporting Allies in defending themselves collectively against hybrid threats**. Since 2015, NATO has developed a dedicated strategy for countering hybrid warfare. Allied Ministers of Defence updated the Strategy in June 2025, ahead of the Hague Summit. In 2016, Allied leaders agreed on seven baseline requirements for national resilience to bolster their resilience against all types of threats, including hybrid ones (NATO, 2024). Most recently, in its 2022 Strategic Concept, the Alliance recognised that strategic competitors are increasingly seeking to interfere in Allied democratic processes through hybrid tactics: "Authoritarian actors challenge our interests, values and democratic way of life. […] They interfere in our democratic processes and institutions and target the security of our citizens through hybrid tactics, both directly and through proxies" (NATO, 2022). Elevating resilient democratic systems as one of NATO's baseline requirements for national resilience could help enhance Allies' posture against cyber interferences in elections.

43. NATO has a number of **practical tools** at its disposal to help bolster Allies national cyber resilience. The Alliance supports Allies' efforts to identify national vulnerabilities and detect threats by contributing to their **situational awareness and facilitating information exchange**. For instance, NATO's Computer Incident Response Capability, while primarily responsible for the protection of the Alliance's own networks, shares its analysis of cyber threats with the Allies. NATO's Joint Intelligence and Security Division also has a hybrid analysis branch that helps improve situational awareness. In addition, NATO has a number of **emergency and incident support tools** that can be deployed upon request to help Allies defend civilian networks and infrastructure against cyberattacks, including in electoral contexts. In 2018, in particular, NATO leaders agreed to set up Counter-Hybrid Support Teams to provide tailored assistance to Allies. In 2023, for instance, NATO sent a team to North Macedonia to help the country cope with the consequences of a series of hybrid attacks, including cyberattacks (NATO, 2023). In 2023, Allies also agreed to launch the Virtual Cyber Incident Support Capability to assist national response efforts to malicious cyber activities. Although these initiatives should be lauded, they remain fragmented. For this reason, **establishing a Centre for Democratic Resilience within NATO headquarters is necessary**, among other tasks, to better coordinate and support the deployment of these tools to protect Allied democratic societies.

44. Finally, **NATO cooperates with like-minded partners** grappling with the same threats to democratic processes. For instance, the Alliance has been working with partner states in its eastern neighbourhood on cyber resilience and defence, as well as countering hybrid threats. It especially cooperates with Ukraine, including via the NATO-Ukraine Platform on Countering Hybrid Warfare. Institutional partners include the European Union, the United Nations and the OSCE. NATO and the EU have been working particularly closely in recent years, sharing information and best practices between their cyber response teams. In 2016, they signed a joint declaration to strengthen EU-NATO cooperation on hybrid threats and resilience, including cyber security and defence (NATO, 2016). The Alliance also cooperates with industry partners and academia, particularly through the NATO Industry Cyber Partnership. Engaging with tech service providers is especially important to respond effectively to ever-evolving cyber threats driven by technological innovation.

45. In addition, NATO-accredited centres of excellence – such as the European Centre for Excellence for Countering Hybrid Threats and the Cooperative Cyber Defence Centre of Excellence – are building knowledge and expertise in these fields.

VI- CASE STUDIES

A. ESTONIA: INVESTING IN ROBUST CYBER INFRASTRUCTURE AND VOTER TRUST

46. Estonia is one of the most digitalised societies in the world. This has helped enhance the quality of Estonian public services but also increased the need for cybersecurity measures. In 2007, an unprecedentedly disruptive series of cyberattacks – amidst disagreement with Russia about the relocation of a Soviet statue in Tallinn – prompted the country to reinforce its cyber resilience efforts. With the implementation of e-voting, election cybersecurity has become a key priority for Estonian authorities. In the 2023 elections, the majority of votes were cast online rather than on paper for the first time. E-voting has been credited with facilitating citizens' participation in elections, increasing the transparency and integrity of the voting process, and enhancing voter trust (e-Estonia, 2023).To achieve these results, Estonia has worked to strike a balance **between accessibility, transparency and security**.

47. Estonia has built a **robust, integrated cybersecurity framework** to accompany the increasing digitalisation of its election processes. The cybersecurity of the Election Information System (VIS), Estonia's digital system for organising elections used by the State Electoral Office, is assured by the Information System Authority (RIA). The VIS is hosted and administered by RIA, which is responsible for protecting digital state services, raising public awareness on cyber threats and handling security incidents in Estonian computer networks (RIA, 2023). RIA cooperates with electoral authorities throughout the entire electoral process to secure information systems. RIA also provides hardware and software required for the collection of e-votes through a different system, the Electronic Voting System (EHS).

48. Concurrently, Estonia has made significant efforts to **invest in voter trust**. To strengthen public trust in the digitalisation of electoral processes, election management bodies communicate throughout the process on how the information and communication systems have been made safe and secure (Heinmaa, 2022). The e-voting process also provides citizens with tools to verify that their ballot has been well received and taken into consideration.

B. FRANCE: REINFORCING OPERATIONAL CAPACITIES AND INTER-INSTITUTIONAL COORDINATION

49. The 2017 "Macron leaks" raised awareness on the risk posed by foreign digital interference to French democratic processes and highlighted the need for a more robust protective framework for elections. Building on a ruling from its Constitutional Council, France subsequently created its **first legal definition of foreign digital interference** to update its legal code for internal security and strengthen the overall legal framework around such attacks (French National Assembly, 2025b).

50. Since then, France has worked to **enhance its operational capacities to detect and address digital threats to elections, with an emphasis on prevention and anticipation**. In 2022, France created a vast election protection system under the authority of its Secretariat-General for National Defence and Security (SGDSN). This involves VIGINUM, an agency created in 2021 to monitor, detect, and investigate foreign digital interference, with the goal of enhancing France's understanding of key tactics and malicious networks. During election processes, VIGINUM forwards any information of interest to national regulators and election authorities (French National Assembly, 2025b).

51. At the same time, France has set up a **multi-stakeholder coordination network to help prevent and respond to digital incidents**, which has been successfully deployed during four election cycles since 2022 (French National Assembly, 2025b). Within this network, the French National Agency for the Security of Information Systems (ANSSI) is the main institutional

actor responsible for the cybersecurity of elections. ANSSI provides recommendations and technical assistance to preserve the cybersecurity of systems used during elections, especially for e-voting by French citizens living abroad (French National Assembly, 2025a). In addition, ANSSI offers technical assistance to political parties and campaign teams upon request to enhance the security of their digital infrastructure. It also monitors cyber threats and reports any cyber incident which may impact the voting process to the relevant institutions.

C. NORWAY: A MULTI-LEVEL APPROACH TO CYBER RESILIENCE AND PREPAREDNESS

52. Norway has one of the highest levels of digitalisation of public services in the Euro-Atlantic region. As part of its National Digitalisation Strategy for 2024-2030, it is implementing a comprehensive approach to protect its highly digitalised election processes from interference. In 2024, the Norwegian government established an inter-ministerial working group to strengthen electoral resilience. Ahead of each election, the working group now presents an action plan to prevent interference (Norwegian Ministry of Digitalisation and Public Governance, 2024).

53. Norway also ensures that **appropriate resources and expertise are disseminated** to sub-national election authorities (Expert Group, 2025). The Ministry of Local Government and Regional Development, Norway's main election management body, plays a crucial role in strengthening the resilience of stakeholders at all levels. In 2023, for example, the Ministry sent out information brochures to all candidates running for municipal and county councils, informing them about how foreign states and other malicious actors may attempt to get access to sensitive information and giving advice on how to prevent such interference.

54. As part of its 2024-2030 strategy, Norway has also created a robust framework to **strengthen and preserve trust in democratic processes**. The Norwegian government has started working on building an open and informed public discourse around the risks posed by disinformation and influence operations (Norwegian Ministry of Digitalisation and Public Governance, 2024). During the Committee on Democracy and Security's visit to Norway in May 2025, officials from the Norwegian Ministry of Local Government and Regional Development also insisted on the importance of explaining to citizens how their votes are protected to build public trust in democratic processes.

55. In addition, Norway is building societal resilience through domestic preparedness by **anticipating the risks posed by new technologies**. In 2024, the Norwegian government established an Expert Group on Artificial Intelligence and Elections to look into how AI may both strengthen and challenge democratic elections. The Group published its report in February 2025, with measures to ensure that electoral processes remain secure and trusted despite rapid developments in AI (Expert Group, 2025).

VII- RECOMMENDATIONS

A. UNDERSTAND, PREVENT, AND MITIGATE CYBER THREATS TO CORE ELECTION INFRASTRUCTURE

56. **Assess cyber risks to election infrastructure**: Given the diversity of election processes across NATO countries, each Ally must perform comprehensive cybersecurity assessments regularly to identify potential vulnerabilities in their election infrastructure that could be exploited by malevolent actors and come up with appropriate mitigation measures. National cybersecurity actors may consider using AI tools to help them better identify and address such vulnerabilities.

57. **Strengthen national crisis response capacities**: To react swiftly to large-scale cyber crises and mitigate their impact on elections, Allied states must devise robust emergency procedures, including crisis management and contingency plans. Allied states should also regularly conduct exercises and simulations with all relevant stakeholders to test these procedures, identify remaining vulnerabilities, and enhance response capabilities in the long-term.

58. **Strengthen national legal and regulatory frameworks on cybersecurity**: Allied states must adopt a robust and coherent framework that clearly defines the powers and duties of actors involved in the cybersecurity of elections and the cybersecurity standards required for election technology. Allied legislators may also need to update existing laws on cybersecurity, data protection and telecoms regulations more broadly to adapt to the evolving nature of cyber threats, while always ensuring that these updates do not compromise fundamental freedoms.

59. **Designate election infrastructure as critical**: Allies should consider whether designating electoral technology as critical infrastructure can improve the overall safety of their elections. This may help unlock long-term government assistance and additional resources to enhance the cybersecurity of elections. Allies, where necessary, should also update their national cybersecurity strategies to cover democratic processes and elections as part of national critical infrastructure.

60. **Incorporate cybersecurity into election technology procurement:** To reduce supply chain risks, Allied election authorities should select trusted vendors that comply with high cybersecurity requirements. In addition, election management bodies must ensure that new technology is sufficiently tested before being introduced to prevent technical challenges from occurring during elections. To ensure that the technology remains secure throughout its life cycle, they should conduct regular reviews, audits, and updates independently from election cycles.

61. **Invest in human resources through capacity-building measures**: Poorly trained technology users represent easy targets for cyber attackers. Allied states must therefore help election officials and other staff involved in administering elections comply with high security standards by providing them with comprehensive cyber security training. Strengthening their technical capacity to detect, mitigate risks, and respond swiftly to incidents will help reinforce the overall resilience of election systems in the long term.

62. **Adding resilient democratic systems to NATO's baseline requirements for national resilience**: Allied leaders should consider updating NATO's seven baseline requirements to include resilient democratic systems. This would prompt Allies to improve their individual ability to react quickly to crises and safeguard the integrity of democratic systems from cyber threats. NATO could support these national efforts by providing expertise and coordination.

63. **Allocate a portion of the 1.5% of GDP in defence-related investments to countering cyber interference in elections:** Allies should ensure that part of this funding is dedicated to protecting democratic processes from cyber threats. Electoral interference not only undermines trust in democratic institutions but also poses a serious risk to the social cohesion and political stability of our societies.

B. ENHANCE THE RESILIENCE OF THE BROADER ALLIED DEMOCRATIC ECOSYSTEM TO CYBER THREATS

64. **Raise awareness on the need for a whole-of-society approach**: The democratic ecosystem is made up of a diverse and interconnected group of actors, including political parties, candidates, the media, and civil society organisations. Because these actors are closely intertwined, a cybersecurity breach affecting one can have wide-ranging consequences for the entire electoral system. NATO states must raise awareness to help these actors understand the cyber security risks related to their activities, as well as their roles and responsibilities in keeping elections secure.

This will help improve the resilience of election systems and democratic processes over the long term.

65. **Provide targeted cyber security assistance to democratic stakeholders**: Democratic stakeholders often lack the resources to implement robust cybersecurity measures or provide comprehensive training for their staff, making them prime targets for cyberattacks. Allied states should offer them support that includes guidance on protective measures and practical assistance to strengthen their cybersecurity posture. This support could involve developing and promoting accessible resources, such as free online toolkits and basic cyber hygiene training. At the same time, Allied countries must ensure that such assistance remains – and is viewed as – nonpartisan and does not compromise the independence of these democratic actors.

66. **Bolster efforts to counter disinformation campaigns combined with cyberattacks**: Because disinformation campaigns can exacerbate the effects of cyberattacks, NATO Allies must safeguard their election processes against those as well. To pre-emptively dismantle disinformation narratives, Allied states should engage the public by explaining how election technology operates and how its integrity is maintained throughout the election cycle.

67. **Enhance public communication to build trust**: Managing perceptions of cyberthreats to electoral processes is just as important as defending them against actual threats. Ultimately, electoral integrity depends on the trust and confidence of the public, making consistent and transparent communication essential. Allied states should be transparent about the cyber risks their election systems face, the measures they have taken to mitigate those risks, and the mechanisms in place to respond to incidents.

C. DEVELOP EFFECTIVE COUNTER MEASURES TO RESPOND TO CYBERATTACKS ON ALLIED DEMOCRACIES

68. **Double-down on attribution efforts**: The Allies should significantly enhance both their individual and collective capabilities to attribute malicious cyber activities targeting electoral infrastructure and democratic systems with accuracy and confidence. By investing in advanced cyber intelligence and forensic technologies, Allies can improve their ability to trace cyber incidents to specific actors or states.

69. **Strengthen accountability measures for cybercrime**: At the national level, Allied states should criminalise cyber interferences in elections, empower law enforcement agencies to investigate cybercrimes, and systematically prosecute offenders within their jurisdiction. At the international level, Allies should engage in judicial cooperation with other states and international law enforcement organisations to effectively investigate and prosecute transborder cybercrimes. Allies should also display their collective resolve to apply joint sanctions or other retaliatory measures against states tolerating the presence of criminal groups responsible for malicious cyberattacks originating from their territory.

70. **Engage in effective dissuasion efforts to deter future cyberattacks**: Allied should regularly reiterate that cyberattacks targeting the critical infrastructure of one or more Allies may be considered an armed attack and warrant a collective response under Article 5 of the Washington Treaty. The Allies should also continue to reflect on possible joint responses to cyberattacks falling below the threshold of Article 5.

71. **Continue supporting the development of international standards and norms**: The Allies should continue leveraging their diplomatic influence to clarify, update, and expand international provisions relating to cybersecurity and cybercrime, while strongly advocating for the protection of democratic values, freedom of speech, and other human rights within these frameworks.

D. STRENGTHEN MULTI-STAKEHOLDER COOPERATION AND COORDINATION EFFORTS AT ALL LEVELS

72. **Facilitate multistakeholder collaboration at the national level**: Protecting elections from cyber threats requires a coordinated effort involving diverse stakeholders. Allied states should consider establishing a national electoral network that includes election management bodies, relevant ministries, law enforcement agencies, national cyber agencies, computer emergency response teams, and private service providers. By collaborating before and during elections, these actors can accurately assess cyber threats, share relevant information, help election management bodies implement robust cybersecurity standards, and effectively manage incidents.

73. **Establish a Centre for Democratic Resilience to strengthen the sharing of information and best practices at the collective level**: NATO should strengthen mechanisms for sharing information, experience, and best practices to help Allies enhance their situational awareness, build up their capacity to detect cyber threats to elections processes early, and devise common solutions. Setting up a Centre for Democratic Resilience within NATO HQ, among other benefits, would centralise resources and coordinate information-sharing efforts among Allies and with partners, strengthening collective resilience against cyber threats to elections.

74. **Increase practical assistance to Allied and partner countries**: At the national level, Allies with electoral cybersecurity expertise and experience should pool some of their resources to support Allied and partner countries in need of cyber assistance. At the NATO level, the role of the NATO's Counter-Hybrid Support Teams should be expanded, and efforts to assist partner countries in developing long-term cyber defence capabilities should continue.

75. **Bolster collaboration with like-minded countries and organisations:** NATO should maintain close cooperation on cybersecurity issues with organisations that have election-related expertise, such as the European Union and the Organization for Security and Co-operation in Europe. Similarly, NATO should enhance its exchanges with partner countries in this area to strengthen collective efforts and share valuable insights. These expanded collaborations would help enhance the collective Allied and partner ability to address cybersecurity threats to democratic processes.

76. **Deepen cooperation with the private sector and academia**: Cooperating with reputable technology providers is essential for building cyber security expertise and sharing information on potential threats and best practices. NATO can serve as a forum for reflection, discussion, and cooperation with major industry actors. Allied governments should also consider funding further research into current and emerging risks that new technologies bring to democratic processes and elections.

BIBLIOGRAPHY

ACN (Agenzia Per la Cybersicurezza Nazionale), "National Cybersecurity Strategy 2022-2026", 2022.

Alliance of Democracies, "Transatlantic Commission on Election Integrity", 2024.

Artic Wolf, "Behind the Ballot: Insights from Arctic Wolf's 2024 Election Security Survey", 9 January 2024.

Bay, Sebastian, "Countering hybrid threats to elections: From updating legislation to establishing collaboration networks", The European Centre of Excellence for Countering Hybrid Threats, Research Report 12, March 2024.

Blackburn, Gavin, "Poland's PM Donald Tusk says his party's computer systems targeted in cyberattack", Euronews, 2 April 2025.

Canadian CSE (Communications Security Establishment):

- (2021), "Cyber threats to Canada's democratic process – July 2021 Update";
- (2023), "Cyber threats to Canada's democratic process – 2023 Update".

Caulcutt, Clea, "Notorious Russian hackers behind 2017 'Macron leaks,' France says", POLITICO, 29 April 2025.

CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence), "Ukrainian parliamentary election interference (2014)", 6 July 2021.

CEPA (Center for European Policy Analysis), "Exploring Latvia's Election Day Hack", 9 October 2018.

Cerulus, Laurens and Klingert, Liv, "Russia's 'Ghostwriter' hacker group takes aim at German election", *POLITICO*, 21 September 2021.

Choi, Seong, "North Korea's Provocative and Secret Interventions in South Korean Elections", Center for Strategic & International Studies, 7 March 2022.

Commonwealth Secretariat, "Cybersecurity for Elections: A Commonwealth Guide on Best Practice", 2020.

CRS (Congressional Research Service), "S.2593 - Secure Elections Act", U.S. Congress, 22 March 2018.

Easterly, Jen, et al., "How to Safeguard U.S. Elections From AI-Powered Misinformation and Cyberattacks", *Foreign Affairs*, 3 January 2024.

e-Estonia, "How did Estonia carry out the world's first mostly online national elections", 7 March 2023.

ENISA (European Union Agency for Cybersecurity), "ENISA Threat Landscape 2023", 19 October 2023.

European Parliament, "Combating gender-based violence: cyberviolence", 14 December 2021.

Expert Group, "Artificial Intelligence and Democratic Elections – International Experiences and National Recommendations - Report by the Expert Group on Artificial Intelligence and Elections", Norwegian Government, February 2025.

FBI (Federal Bureau of Investigation):

- "Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad", 26 January 2022;
- "Joint ODNI, FBI, and CISA Statement on Iranian Election Influence Efforts", 19 August 2024.

French National Assembly:

- (2025a), « Organisation des élections en France : Anciens représentants des personnels de la société Milee ; M. Vincent Strubel, directeur général de l'ANSSI », 5 March.
- (2025b), « Organisation des élections en France : M. Marc-Antoine Brillant, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) »18 March.

Garriaud-Maylam, Joëlle, "Strengthening the protection of critical infrastructure against cyber threats", NATO Parliamentary Assembly, Report by the Committee on Democracy and Security, 19 November 2022.

Government of Canada, "Cyber threats to elections", 2023.

Gregory, Jennifer, "Poland spending $760 million on cybersecurity after attack", *Security Intelligence*, 24 June 2024.

Haeck, Pieter, Paun, Carmen, Cerulus, Laurens and Starcevic, Seb, "TikTok's Romanian reckoning", *POLITICO*, 29 November 2024.
Hartmann, Théophane, "UN approves landmark controversial cybercrime treaty", Euractiv, 12 August 2024.
Hartog, Eva, "Dutch party websites attacked as EU vote kicks off", *POLITICO*, 6 June 2024.
Heinmaa, Thomas, "Cybersecurity in Elections: Recent Developments in Europe – Online Discussion", International IDEA, 14 February 2022.
INCIBE (Instituto Nacional de Ciberseguridad), "El dispositivo especial de vigilancia de ciberseguridad en las elecciones europeas contará con la colaboración de INCIBE", 14 May 2024.
Klein, David, "Report: Minorities and Women are More Likely Victims of Cyber Crime", Organized Crime and Corruption Reporting Project, 19 October 2021.
Latvian MOD (Ministry of Defense), "The Cybersecurity Strategy of Latvia 2023-2026", 2023.
Microsoft, "Microsoft Digital Defense Report 2022", 2022.
Microsoft, "Iran steps into U.S. election 2024 with cyber-enabled influence operations", 9 August 2024.
NATO (North Atlantic Treaty Organization):
– (2016), "Joint declaration", 8 July;
– (2022), "NATO 2022 Strategic Concept", 29 June;
– (2023), "NATO team in North Macedonia to help against hybrid attacks", 14 March;
– (2024), "Resilience, civil preparedness and Article 3";
– (2025), "The Hague Summit Declaration", 25 June.
NCSC (National Cyber Security Centre), "Annual Review 2023", 2023.
NIS Cooperation Group, "Compendium on Elections Cybersecurity and Resilience", Updated version, 2024.
Norwegian Ministry of Digitalisation and Public Governance, "The Digital Norway of the Future – National Digitalisation Strategy 2024-2030", 2024.
OpenAI, "Disrupting malicious uses of AI by state-affiliated threat actors", 14 February 2024.
OSET Institute (Open Source Election Technology Institute), "Critical Democracy Infrastructure: Protecting American Elections in the Digital Age: Threats, Vulnerabilities, and Countermeasures as a National Security Agenda", 2nd edition, May 2020.
Paris Call, "The 9 principles", 2018.
Parliament of Canada, "BILL C-70 - An Act respecting countering foreign interference", 6 May 2024.
Pohjanpalo, Kati, "Finland Detects Cyber Attack on Online Election-Results Service", *Bloomberg*, 10 April 2019.
Rajagopalan, Rajeswari, "U.S. Official Warns of China's Growing Offensive Cyber Power", *The Diplomat*, 12 February 2024.
Reuters:
– (2017), "Czech election websites hacked, vote unaffected - Statistics Office", 22 October;
– (2024), "Germany's Christian Democratic party hit by 'serious' cyberattack", 1 June.
RIA (Estonian Information System Authority), "Election information system and i-voting", Republic of Estonia, 17 December 2023.
Romanian Presidency, "Comunicat de presă", 4 December 2024.
Sabbagh, Dan, "Russians hacked Liam Fox's personal email to get U.S.-UK trade dossier", *The Guardian*, 3 August 2020.
Sabin, Sam, "One-third of top U.S. cyber force has left since Trump took office", Axios, 3 June 2025.
Sanger, David and Barnes, Julian, "United States Indicts Iranian Hackers in Voter Intimidation Effort", *The New York Times*, 18 November 2021.
Tenove, Chris et al., "Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy", Centre for the Study of Democratic Institutions, 16 January 2018.
Tisler, Derek and Norden, Lawrence, "Securing the 2024 Election: Recommendations for Federal, State, and Local Officials", Brennan Center for Justice, 27 April 2023.
Tomé, Joao and Woolbright, Jocelyn, "Exploring Internet traffic shifts and cyber attacks during the 2024 U.S. election", Cloudflare Blog, 11 June 2024.

Tulp, Sophia, "Iranian 'hacking' video fabricated to push election disinfo", *AP News,* 7 November 2022.
Uddin, Rafe, "UK election body failed to protect voter data before Chinese cyber attack, says watchdog", *Financial Times*, 30 July 2024.
USAID (United States Agency for International Development), "Primer: Cybersecurity and Elections", July 2022.
U.S. Department of Justice:
- "Report on the investigation into Russian interference in the 2016 Presidential election", Special Counsel Robert S. Mueller, III, March 2019;
- "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election", Office of Public Affairs, 18 November 2021.

Vanderlee, Kelli and Collier, Jamie, "Poll Vaulting: Cyber Threats to Global Elections", Mandiant, 25 April 2024.
Van der Staak, Sam and Wolf, Peter, "Cybersecurity in Elections: Models of Interagency Collaboration", International Institute for Democracy and Electoral Assistance, 2019.