OXFORD JOURNAL
OF STUDENT
SCHOLARSHIP

The Forefront of Warfare: Governing Cyberwarfare through International Organizations

Daniel Son
daniel0929son@gmail.com

ABSTRACT

Cyberwarfare is increasingly enabling state and non-state actors to inflict civilian, political, economic, and infrastructural harm without the traditional thresholds of armed conflict. This paper examines the evolving nature of this development and evaluates the capacity of existing international organizations to regulate cyber operations that rival or exceed the effects of conventional warfare. By comparing the United Nations, NATO, and the Organization for Security and Co-operation in Europe (OSCE) across multiple categories of cyber conflict the study assesses their legal authority, operational capability, neutrality, and effectiveness. The analysis finds that while the UN excels in norm creation and NATO in deterrence within alliance structures, both face significant political and structural constraints in incident-level engagement. Ultimately, OSCE, with targeted institutional expansion and enhanced rapid-response capabilities, is best positioned to lead practical cyberwarfare governance by prioritizing civilian protection, escalation management, and cooperative security.

INTRODUCTION

On a brisk winter evening, power suddenly vanished across multiple regions in Ukraine. Nearly 225,000 people lost electricity for hours on end. In the middle of a military confrontation, this was a nightmare, but the more terrifying fact that this was done on purpose. The 2015 Ukraine power grid attack would have required detailed maps of transmission lines, special force units trained in infrastructure sabotage, cross-border infiltration, and meticulous planning for simultaneous attacks from the Russian government. This is an impossible amount of effort for a short outage that mostly affects civilians over military personnel. What makes this incident unique is that none of these measures were needed. Instead, the operation was carried out entirely through cyber means, with no personnel required to cross borders. This demonstrates how attacks in cyberspace can replicate and outperform the effects of traditional warfare while bypassing its costs, logistics, and legal thresholds.

In the era of national security unshielded easily and self-destructive warfare doomed, regulating such a type of warfare is critical for the upholding of global peace and stability, which would lead all international entities win-win in the long run. The purpose of this paper is to explore types of

cyberwarfare and its effects, explore international organizations that may be able to regulate cyberwarfare, and determine the best way suited to lead the regulation of cyberwarfare globally. This series of prospecting points pose the central question: when cyber operations can surpass the effects of conventional military action, who should be the central, international authority to regulate this new type of war in order to minimize political instability and civilian harm, given the existing international system?

BACKGROUND

The scope of cyberwarfare is difficult to define, both in what qualifies as an attack and at what point attacks cross the line of international law. One thing clear is that cyberwarfare can produce effects comparable to conventional military force.[1] For the purpose of this paper, inspection of cyberwarfare will be limited to "actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks."[2]

Cyberwarfare Igniting International Attention

A prime example of cyber warfare is the 2007 attack on the Estonian government. A barrage of Distributed Denial of Service (DDoS) attacks crippled the country's digital infrastructure over three weeks. This incident introduced to the world the need for formal intervention from international organizations – in this case, NATO.[3] The DDoS attack targeted political, financial, and other e-services, impacting online banking systems and news outlets for the citizens. Targeting the Estonian government as a whole, the attack significantly disrupted the private sector. The attackers were identified as a Russian private sector with possible connections to the Russian government. Only one person had been convicted of the incident: a 20-year-old student, Dmitri Galuškevitš, establishing the availability of such technologies. In future incidents, many attackers, although state-sponsored, would often be independent groups or political organizations, known as "hacktivists."[4]

Following the Russian attack, NATO and private-sector infrastructure providers launched initiatives to protect against, neutralize, and prevent cyberattacks. Specifically in 2008, NATO established the Cooperative Cyber Defence Centre of Excellence in Estonia. Over the years, many international organizations and independent nations, such as the UN and the United States, have developed advanced cyber defence technologies and infrastructure. Examples of these include the Global Counter Terrorism Programme on Cybersecurity and New Technologies and the United States Cyber Command.

Because cyberwarfare possesses capabilities similar to conventional warfare, international law has been a critical tool for regulating it. Professor Harold Koh has affirmed that "international law principles do apply in cyberspace", the problem lies in how "existing rules will apply to such innovation."[5] Specifically, Jus in bello (Justice in war) has been identified as crucial in determining the boundary between peacetime operations and acts of war. In fact, some states, such as Singapore, have argued that malicious cyber activities can constitute an armed attack under Jus ad bellum, even without any physical harm.[6]

Cyberwarfare has far exceeded the era of the "ILOVEYOU" worm, known for stealing internet login credentials through email phishing.[7]

With sophisticated, state-sponsored cyberattacks that integrate artificial intelligence and machine learning technologies, individuals and governments are constantly under threat. Power grids, health services, and military digital infrastructure are common targets of these threats. In 2017, for example, a ransomware attack known as WannaCry restricted access to patient records, delayed surgeries, and redirected patients to other hospitals.[8] In fact, healthcare services had more cyber threats than any other critical US infrastructure in 2024.[9]

The real distinction between traditional warfare and cyberwarfare lies in the ambiguity of the latter. The "scope of the definition of what constitutes a civilian object versus military objective" is unclear.[10] Additionally, the effects on systems used by both state and private actors, the anonymity of the attacker, and indirect effects of the attack make it almost impossible to enforce principles of proportionality and distinction. Finding an agreed-upon answer to this question is imperative for future legislation on cyberwar.

Potential Solutions

Potential organizations that can regulate cyberwarfare can be sorted into three broad categories: alliance coalitions, international organizations, and individual states. Examples of alliance coalitions include the European Union (EU), the North Atlantic Treaty Organization (NATO), the African Union (AU), and the Association of Southeast Asian Nations (ASEAN). These organizations generally have greater authority over member states than international organizations do, but they have difficulty setting precedent for the rest of the world. NATO, for example, has undertaken efforts to strengthen its cyber defence, establishing the Cooperative Cyber Defence Centre of Excellence (CCDCOE) and other organizations to benefit its member states. The nature of such organizations has led to a limited effect on non-member states. For example, the CCDCOE has had a significant hand in aiding Ukraine during Russia's invasion of Ukraine.[11] Due to organizational responsibilities, countries such as Malaysia, which have been the victim of over 1500 attacks in a single quarter, have not received such assistance.[12]

International organizations include entities such as the United Nations (UN) and affiliate bodies, including the International Criminal Court (ICC) and the International Court of Justice (ICJ). These bodies have a larger reach, spanning many more states than alliance coalitions, but often have limited authority over them. For example, the UN has had trouble getting the agreement of member states for the UN Open-Ended Working Group (OEWG) on Information and Communication Technologies (ICTs).[13] In this process, Russia, China, the United States, and their allies argued for solutions that each served their own self-interest. These disagreements delayed the establishment of said rules and impeded any real progress in securing cyberspace for member states.

Many individual states have developed their own cyber commands and national cybersecurity laws, managing both defensive and offensive operations. These efforts are more actionable and have

reinforcement mechanisms that are often lacking in international entities, but they often lead to conflicting standards that create geopolitical competition and tension. Russia and the United States, for example, are both states with advanced cyber capabilities and cyber defense protocols, and their conflicting philosophies on cyberwarfare complicate the centralization of control. For example, the United States upholds the value of international law in cyberspace, but Russia focuses on protecting the nation-state, its information, and its infrastructure, without invoking international legal norms.[14]

METHODS

Framework of Categories

This paper divides cyberwarfare into five categories: political, economic, infrastructure, terrorism, and espionage. Each type has different motivations, actors, and victims, which allows evaluation of how each organization will react to different situations. Still the ability to apply precedent across these categories is an important factor in choosing which organization should lead regulation.

Political cyberwarfare is the interference with another state's political stability, institutions, leadership, or public opinion.[16] It often influences state leaders, undermines the state's legitimacy, or manipulates political processes. An example of this would be the alleged Russian interference in the 2016 United States Presidential Election. Although direct harm is not done to the state, the political instability and change in political opinion, which can benefit other states, call into question the principle of sovereignty that is expressed in "multiple declarations by the UN, the African Union, the European Union, NATO, OSCE, and individual states".[15] Specifically, this type of cyberwarfare calls into question the sovereignty of states and the actor's domaine reservé, which describes the exclusive domestic jurisdiction where other states or international bodies are prohibited from intervening.[16] Controlling this type of cyberwarfare is difficult because of its discreteness and unclear effects.

Economic cyberwarfare is the interference with another state's financial systems, whether in the form of banks, markets, or specific industries. This type of cyberwarfare seeks to weaken economic capability, disrupt commerce, or temporarily halt economic activity. For example, Estonia's major banks, small businesses, and governmental portals were attacked in 2007.[17] For over 3 weeks, financial services were limited, making the country's regular operations almost impossible. Especially during wartime, economic instability and interference can bring significant harm not only to the political sphere but also to the civilian population, hence being able to evaluate what constitutes proportionality and necessity in responses.

Infrastructure cyberwarfare is that which focuses on both cyber and physical infrastructure, such as water systems, medical facilities, and power grids. This kind of cyberwarfare does not directly target civilians but often harms facilities that are essential to civilians. The 2020 Israeli water facilities attack by Iran is an example. The attack targeted 6 Israeli water supplies by hacking valves and logic controllers, the goal

of which was contamination or a shortage of water. If successful, the attack led to substantial damage to the civilian population.[18]

Cyberterrorism is a rare type of cyberwarfare in which civilians are directly targeted as victims. Although commonly seen in attacks by individual actors, most states do not participate in terrorism through cyberwarfare. As the most severe form of cyberwarfare, it is crucial that organizations have a strong basis for their response despite the limited precedents. An example of cyberterrorism is the hypothetical "Cyber Pearl Harbor" that has been prominent in the U.S. cybersecurity debate.[19] Even though this specific example of a city-wide attack is largely a worst-case scenario that has been described as "unhelpful and dangerous",[20] a similar action at a smaller scale, like the 2020 Düsseldorf University Hospital Ransomware Attack, is important to mention.[21] A ransomware attack on the hospital was attributed as the cause of death for a 78-year-old woman whose surgery was delayed. A direct death caused by a cyberattack may be considered use of force under international law, even if no physical threats were made, allowing the victim state to exercise its right of self-defense.[22] The consequences and complexity of such an outcome pose a significant dilemma to global politics and should be navigated carefully.

Cyberespionage, although not considered an act of war under international law, must be regulated. An organization's ability to define cyberespionage and what constitutes an act of war is essential to this classification of cyberwarfare. The extent to which sensitive, confidential information is stored on the Internet calls into question what constitutes lawful surveillance and what constitutes a breach of rights to privacy and freedom established by international law, such as the International Covenant on Civil and Political Rights (ICCPR). For example, Ethiopia's extensive surveillance efforts in the 2010s have been widely criticized for their widespread nature. Cynthia Wong, a senior internet researcher at Human Rights Watch, has mentioned concern that these surveillance methods may threaten the freedom of expression and privacy of the people targeted.[23] The ability to distinguish lawful from unlawful uses of cyber espionage is therefore a significant factor in determining whether an organization is capable of regulating cyberwarfare.

Potential Candidates for Regulation of Cyberwarfare

Detecting cyberwarfare, determining appropriate responses, and preventing future attacks are all deeply challenging. A variety of organizations have attempted to create an international norm for such regulations, but it is difficult to determine the optimal option. The three options this paper focuses on are: the United Nations, the North Atlantic Treaty Organization, and the Organization for Security and Co-operation in Europe. These three were chosen for their political leverage, expertise, or extensive history with Cyberwarfare. By analyzing their potential, historical record, and individual strengths and weaknesses across different types of cyber warfare, it will be established which organization is best suited for the task.

The UN has established the UN Counter-Terrorism Centre (UNCCT), aiming to provide leadership on the counter-terrorism mandates across the United Nations system, including those concerning Cyber Warfare,

in tandem with the UN Security Council.[24] In general, the UN has two benefits over other organizations: its extensive member list and considerable history and experience in cyberspace. First, its near-universal membership grants it unparalleled legitimacy. Any norm, framework, or standard developed under UN auspices carries global representativeness, making it the most inclusive forum for addressing cyber warfare, which by nature transcends borders. For example, the UN Law of the Sea (UNCLOS) has seen widespread use and has been honored by most of its signatories, which include key players such as the United Kingdom, Russia, and China.[25] This has provided a legal framework for conflicts happening overseas. Most significantly, UNCLOS was recently invoked by China to frame its legal position on the South China Sea.[26] The analogy has limits — maritime boundaries are physically defined in ways cyberspace is not, and state interests in sea lanes are more legible than those in network infrastructure — but UNCLOS demonstrates that UN-backed frameworks can shape state behavior even among major powers with competing strategic interests.

The UN has extensive institutional experience in dealing with cyberspace. The Cybersecurity and New Technologies programme by the UNCCT provides support to member states in creating infrastructure that deters cyberattacks by terrorists and other malicious actors.[27] On the other hand, the UN's capability is called into question by historical efforts to set norms for the international community. Most significantly, the Universal Declaration of Human Rights (UDHR) is widely endorsed but non-binding. Many states violate it without legal consequence. UDHR Article 19 outlines "the right to freedom of opinion and expression," a right commonly violated in many countries.[28] Can Dündar, a Turkish journalist and editor-in-chief of the Turkish newspaper Cumhuriyet, was arrested by the state, being accused of being a member of a terror organization.[29] The UN's inability to respond to these situations reveals critical limitations in its power, but its scale provides a strong argument for UN's leadership in cyberwarfare regulation.

NATO has created comprehensive resources and norms related to cybersecurity for its member nations. Since the recognition of cyberspace as a domain of operation in 2016, NATO has integrated cyber defense into its security strategy.[30] Specifically, institutions such as the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) focus on technology, strategy, operations, and law of cyber defense. Interestingly, the CCDCOE was created in response to the 2007 cyberattacks against Estonia.[31]

Organizationally, NATO differs from the UN in that Article 5 of the North Atlantic Treaty states that a sufficiently severe cyberattack may trigger collective defense obligations.[34] This is a major deterrent factor that an international organization like the UN does not have. The smaller scale of NATO also allows frequent cyber exercises, intelligence sharing, and capability development, which allow for rapid detection and response to cyber threats. However, this limited membership also constrains its effectiveness. As Western states dominate the creation of policies from NATO, their geopolitical situation slows the adaptation of norms by a large portion of the globe. This raises conflict and noncooperation and reduces their legitimacy in the eyes of several major cyber powers such as Iran, China, and Russia. However, their ability to respond to threats in real time and implement solutions makes NATO a strong contender to enforce cyberwarfare.

The OSCE is the most specialized organization for combating cyber threats. As a security-oriented organization, its protocols and framework, such as the confidence and security building measures (CSBMs), specifically look to reduce the risks of misperception, escalation, and conflict in cyberspace.[32] These measures promote transparency, information sharing, and communication between participating states regarding national cyber policies and incidents.

Similar to the UN, the OSCE's member list is also global. With 57 member states spanning North America, Europe, and Central Asia, its reach and authority are respectable. However, like the UN, the lack of enforcement authority and operational capabilities makes it questionable. Its frameworks are voluntary and depend entirely on political goodwill, limiting their effectiveness against deliberate or large-scale cyber aggression. Additionally, much of its efforts are focused on the prevention of aggression between states, not the response to them.[33] As a result, while the OSCE contributes meaningfully to stability and communication in cyberspace, it is poorly equipped to deter or respond to high-intensity cyber warfare. Their ability to set global norms has not been fully explored and must be evaluated, but its organizational expertise and specialization makes it a strong candidate.

DISCUSSION

Political Cyberwarfare

Each of the three organizations is evaluated across four dimensions: legal and normative authority, speed of response, scope of engagement, and enforcement mechanisms.

As an international peace organization, the United Nations has long advocated for the proliferation of democratic governance and free governments.[28] This includes the promotion of fair elections, one of the first targets of political warfare due to their central role in legitimizing state authority. Rather than retroactively acting on instances of election interference, the UN focuses on the prevention of such interference in the future through the creation of norms and fostering discussion between states. These normative frameworks are often non-binding and slow, especially when member states disagree on definitions and enforcement.[34] This framework includes a specific, actionable list of state behaviors, which include protection of critical infrastructure and reporting of ICT vulnerabilities, which are critical in the prevention of political cyberwarfare.[35] This gives the UN an extreme amount of legal/normative authority, even when they are non-binding, as a large number of states and entities have participated in the creation of this document. This is extremely useful for creating a safe digital space; the weaknesses of the UN are apparent in what happens after such norms are created and published.

As mentioned, these norms have a strong ethos that the states are incentivized to follow, but they are not forced to do so. This is because of the aforementioned lack of enforcement by the UN. Unenforced laws created by state governments have been criticized as "undermining public respect for the law and

violating the separation of powers".[36] In this case, it is unenforced not by lack of will or corruption in the system but by design. This highlights a critical flaw in the international law framework. Powerful states frequently disregard international law when it conflicts with their strategic interests, leading to recurring breaches and non-enforcement, a pattern across all types of cyberwarfare for the UN.

Even though it is unknown many political warfare incidents have been prevented by the UN, it is clear that attacks have not stopped. Right after the resolution adopted by the general assembly in Dec 2015, often cited as a major step in preventing political cyberwarfare, a major hack by Russian GRU intelligence led to the US Democratic National Committee's emails being leaked and being used to disrupt the campaign of Hillary Clinton in the 2016 US election.[37] The lack of post-incident action other than occasional trials by the ICC suggests that the UN alone may not be well-suited to organize a system that extends beyond the creation of resolutions. The pattern did not end in 2016. French intelligence documented a coordinated leak operation targeting Emmanuel Macron's presidential campaign in 2017, and the German Bundestag suffered a sustained intrusion in 2015 attributed to Russian military intelligence, compromising data from dozens of parliamentary offices. Each incident was acknowledged in UN forums and then absorbed into the same normative cycle: documentation, reaffirmation of existing principles, no enforcement action.

The North Atlantic Treaty Organization approaches political cyberwarfare from a fundamentally different position than the United Nations. As a collective defense alliance rather than a normative or human-rights body, NATO views election interference not primarily as a legal or democratic issue, but as a security threat capable of undermining the political stability of its member states. Cyber-enabled interference in elections is therefore framed within NATO's broader concern over hybrid warfare, where cyber operations, disinformation, and political manipulation are used to weaken states below the threshold of armed conflict.

Rather than developing universal norms, NATO's response centers on deterrence, resilience, and signaling of collective defense. In 2016, NATO formally recognized cyberspace as an operational domain, following the UN's 2015 declaration.[38] This marked a shift from viewing election interference as an internal political error to an organizational security issue. This prompted the creation of NATO's Cyber Coalition, an annual cyber defense exercise conducted by Allied Command Transformation.[39] This has allowed for participation from more than 200 participants and 1,300 cyber defenders, who are not just NATO's Allies but Partners that extend across six continents.

Institutionally, NATO's response capacity is reinforced by specialized bodies such as the NATO Cooperative Cyber Defence Centre of Excellence, which has produced legal and strategic analyses on state responsibility in cyberspace. One notable output is the Tallinn Manual process, an independent academic project hosted at the CCDCOE that has shaped how member states legally interpret cyber operations interfering with political sovereignty, including elections. Though non-binding and produced by scholars rather than NATO itself, it has contributed to a shared understanding of when election

interference may constitute a security threat — demonstrating that NATO institutions can influence the normative environment without formally setting policy.

Other than deterrent policies, NATO has shown capabilities for post-incident coordination as well. Although NATO has rarely made public statements confirming alliance-level responses to specific cases, it possesses mechanisms for intelligence sharing and defense cooperation among its members. NATO policy recognizes that a "serious cyberattack" against a member could trigger Article 5 of the North Atlantic Treaty, treating such an attack as an attack on all members.[40] Some may argue that the lack of precedent undermines its validity, but the sheer military capability of the alliance is an extremely strong deterrence.

The Organization for Security and Co-operation in Europe approaches political cyberwarfare, specifically elections, through individual election integrity, rather than a militaristic or normative approach. It considers election interference a threat to democratic legitimacy and takes an operational role in individual elections. In Ukraine's 2019 presidential and parliamentary elections, OSCE documented attacks against election infrastructure in an "ODIHR Needs Assessment Mission Report."[41] This document included not just a summary of events but a detailed list of recommendations for increasing defense structures and changes in political systems to refine equality in the state.

OSCE also specializes in internal threats against election integrity. Moldova's 2016 presidential election report discusses media manipulation within the state and gives recommendations to better facilitate fair and free elections.[42] OSCE framed them as systemic threats to electoral fairness. Similarly, in Albania's 2021 parliamentary elections, OSCE reports highlighted the misuse of personal data, digital voter profiling, and vulnerabilities in campaign-related digital systems, underscoring how data exploitation has become a central tool of modern political cyberwarfare.[43]

Their case-study approach gives OSCE several distinct strengths. Its compilation allows for detailed, incident-specific reporting that few other international organizations can match. This unique intervention in electoral systems, when needed, offers technical guidance and procedural recommendations that are immediately relevant to national authorities. As a result, it is particularly effective at protecting and exposing elections for the development of more resilient electoral infrastructure.

In comparison to the UN and NATO, OSCE offers the most evidence-driven response to election interference, offering actual prevention of political cyberwarfare in practice. Even as it lacks the legal authority of the UN or the deterrent power of NATO, the OSCE remains a strong contender in addressing political cyberwarfare.

Economic Cyberwarfare

The lack of sufficient precedent for international organizations engaged in economic cyberwarfare makes the analysis of their capabilities challenging. Hence, the potential capabilities of each organization using

the limited evidence and existing defense measures, will be used in the following areas: pre-incident direct prevention, pre-incident indirect prevention, and post-incident measures. Direct actions refer to measures that address a specific cyber incident by name, including actions taken in response to an identifiable attack on economic or financial infrastructure. Indirect actions encompass general cybersecurity efforts that are not tied to a single incident, such as capacity building, resilience frameworks, information sharing, and normative guidance aimed at strengthening economic cyber defenses overall. Post-incident measures look to deter similar attacks, punish the actor, or aid in recovery efforts.

As previously established, all three organizations have significant infrastructure supporting pre-incident indirect prevention. This comes in the form of norm development, information sharing, capacity building, and resilience enhancement. The UN, for example, has put in place policy frameworks, such as those proposed by the Group of Governmental Experts (GGE), thereby making the protection of financial systems the norm.

Pre-incident direct prevention requires rapid detection capabilities, real-time information sharing, and sufficient political leverage, which allows for direct prevention or alarming of the state. This is the least developed category across all three organizations. Specifically, the lack of a 24/7 response team means that attribution is slow, and the role of international organizations as a collection of delegates from each country means it generally lacks the authority to directly monitor or intervene in national financial systems. However, among the three organizations, NATO is structurally the most capable of approaching pre-incident direct prevention. This is due to its limited membership and military alliance status. Specifically, the NATO Cyber Rapid Reaction Teams (CRRT) are available 24/7, allowing for assistance to allies when approved by the North Atlantic Council. OSCE has a similar response mechanism, but it is slower and not focused on ICTs. The Cyber Confidence-Building Measures enable rapid information sharing and provide points of contact. However, they are much more limited than CRRTs as they are more focused on helping states to defend themselves than providing defense capabilities.

Post-incident measures define an organization's focus and priorities, as they allow time for the organization to weigh options and develop a plan. For the UN, the priorities continue the pattern of norm-setting and preventative measures. Specifically, GGE and Open-ended Working Group (OEWG) sessions reaffirm and clarify existing norms, particularly those on critical infrastructure protection and state responsibility. ICT is one of the main focuses of the OEWG, with the General Assembly mandating quarterly meetings that discuss the development of rules, norms, and principles for the responsible behavior of States in 2020. Documents such as the OEWG on ICT's final report show that the UN not only created new norms but a system for "additional norms... to be developed over time[44] concerning cyberattacks that cause damage to economic infrastructure.

NATO, too, continues its pattern of selective and security-driven service to cyberwarfare. The scope of potential NATO engagement in economic cyberwarfare is illustrated by two distinct cases. In 2016, attackers believed to be linked to North Korea compromised the SWIFT interbank messaging system and

stole $81 million from Bangladesh Bank by sending fraudulent transfer orders — an operation that exploited trusted financial infrastructure rather than destroying it. A year later, the NotPetya malware, attributed to Russian military intelligence, caused an estimated $10 billion in commercial losses globally, crippling Maersk's shipping operations, disrupting Merck's pharmaceutical production, and halting FedEx's logistics. NotPetya is particularly important for NATO's analysis: it began as a cyberattack on Ukrainian financial software but spread uncontrollably across global supply chains, demonstrating that economic cyberwarfare can produce casualties well beyond the intended target state. In both cases, NATO had no formal mechanism to respond. The Bangladesh heist fell below any threshold of collective defense, and NotPetya, while devastating to several NATO member economies, did not produce a formal invocation of Article 5 consultations. Separately, in April 2007, Estonia was subjected to prolonged DDoS attacks by Russian state-sponsored actors that targeted Estonia's digital economy.[45] It disrupted online banking services, financial transactions, and access to private property. Under such circumstances, the incident had the potential to be considered under Article 5 of the North Atlantic Treaty, which frames an attack on one member as an attack on all. Despite these concerns, Article 5 was not invoked as there was insufficient evidence to conclusively attribute the attacks to the Russian state at the time.[46] Nevertheless, the episode served as a critical turning point for the alliance and eventually led to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn the next year. This is one of the clearest examples of post-incident measures, and it has been a critical part of deterring cyberattacks in Europe, with no attack as major as Estonia's since.

OSCE works closely with states to prevent future incidents and aid reconstruction through its Confidence-Building Measures. The Transnational Threats Department has committed to assist participating States in implementing these CBMs and developing new ones as threats evolve.[47] Unlike NATO's security-driven post-incident posture or the UN's norm-reaffirmation cycle, OSCE's recovery-oriented model is less concerned with attribution or deterrence than with stabilizing economic systems and helping targeted states restore functionality. This is a narrower role, but in cases where geopolitical dynamics make attribution politically toxic, it may be the only role available to an international institution.

The UN, NATO, and OSCE demonstrate their greatest effectiveness in indirect and post-incident measures, while direct pre-incident prevention remains largely underdeveloped due to sovereignty constraints, attribution challenges, and limited enforcement authority. The potential for such measures will be necessary in choosing the contender for the best fit organization to lead cyberwarfare prevention. Together, these organizations highlight the need for simulated practice, the establishment of specific committees for deterrence, and authority for direct intervention.

Infrastructure Cyberwarfare

Attacks on critical infrastructure such as hospitals, power grids, and water systems are some of the most detrimental to a country, as they can affect local civilian populations and undermine the stability of the entire state. As a result, studying infrastructure cyberwarfare is crucial for evaluating how an organization

acts when faced with a threat to civilian populations. Examining these responses provides insight into whether international institutions are equipped to prevent and manage operations that threaten civilian welfare and societal stability.

The United Nations addresses infrastructure cyberwarfare primarily through norm development and international security discourse, rather than operational response. High-impact incidents such as the 2015 and 2016 cyberattacks on Ukraine's power grid, which caused civilian electricity outages, and the 2022 Viasat satellite network attack, which disrupted civilian communications across Ukraine and parts of Europe, have been repeatedly referenced in UN discussions as real-world consequences of cyber operations targeting critical infrastructure. These cases have informed the work of the Group of Governmental Experts and the Open-Ended Working Group, reinforcing norms that call on states to refrain from cyber operations that damage critical infrastructure and threaten civilian populations. While the UN does not respond directly to these incidents, it uses them to justify the application of international law in cyberspace and to strengthen expectations of responsible state behavior. A complicating precedent is Stuxnet, the 2010 operation attributed to the United States and Israel that destroyed centrifuges at Iran's Natanz nuclear facility. Unlike the Ukraine or Viasat cases, Stuxnet targeted explicit military infrastructure and caused physical destruction — raising the question of whether the UN's norms apply differently to military versus civilian targets, a distinction the GGE has been reluctant to resolve clearly.

NATO approaches infrastructure warfare by maximizing collective resilience and minimizing civilian risk. Infrastructural operations such as the 2015 attack on Ukraine's power grid have reinforced NATO's assessments that cyberattacks can generate civilian disruption without immediate targets. Especially interesting is the 2022 attack on the Viasat satellite network. This attack, although it did not disrupt the primary needs of citizens such as water and energy, caused significant difficulties for citizens and imposed a threat on the national security of Ukraine.[48] These incidents have been treated as indicators of the evolving threat environment facing NATO members, demonstrating how cyber operations against infrastructure can undermine essential services and economic activity without crossing the traditional threshold of armed conflict.

In response, NATO has emphasized defensive preparedness and institutional adaptation rather than direct retaliation. Infrastructure attack scenarios are now routinely incorporated into alliance cyber exercises and resilience planning, strengthening coordination among members and improving protection of shared systems. NATO's post-incident posture prioritizes situational awareness, support to affected allies, and the development of collective defensive capabilities, reflecting a deliberate effort to deter future attacks by increasing the cost and complexity of targeting civilian infrastructure. However, this approach also reveals NATO's limitations: responses remain contingent on political consensus, escalation thresholds are intentionally ambiguous, and the alliance avoids public enforcement actions in infrastructure cyber cases. As a result, NATO's effectiveness in this domain lies more in preventing future harm through preparedness than in punishing past attacks.

The OSCE approaches infrastructure cyberwarfare primarily as a threat to civilian welfare and regional security. Rather than a military challenge requiring deterrence or retaliation, OSCE focuses on rebuilding and preventing future incidents. This perspective is reflected in OSCE discussions following the Ukraine power grid cyberattack, which demonstrated how cyber operations against electrical infrastructure could cause direct civilian harm and disrupt essential services.[49] The incident has been repeatedly referenced in OSCE cybersecurity discourse as an example of why infrastructure cyberattacks pose risks not only to state security but also to societal resilience and public trust.

Rather than responding through enforcement, OSCE has focused on confidence-building, transparency, and post-incident stabilization. The adoption of OSCE CBMs under Permanent Council Decision No. 1106 in 2013 and their subsequent expansion[50] in Decision No. 1202 in 2016 reflect lessons drawn from major cyber incidents such as the Ukraine power grid attacks.[51] These CBMs establish mechanisms such as national points of contact, voluntary information sharing, and crisis communication channels that can be activated following cyber incidents affecting critical infrastructure. By facilitating rapid communication and cooperative risk reduction after infrastructure disruptions, the OSCE seeks to prevent escalation and support recovery rather than impose punishment. While this approach lacks the deterrent capacity of NATO or the normative reach of the UN, it enables the OSCE to function effectively in politically sensitive environments, positioning it as a de-escalatory and recovery-oriented actor in infrastructure cyberwarfare.

Cyberterrorism

Cyberterrorism is analytically difficult to evaluate because truly threatening cases (non-state actors using cyber means to cause mass physical harm or sustained disruption comparable to state cyber operations) remain relatively uncommon. That rarity should not be treated as evidence that cyberterrorism is insignificant. Instead, it reflects a persistent capability gap: sophisticated cyber operations typically require sustained access, resources, and operational security that most terrorist groups struggle to maintain. For this reason, the most consequential current threat is often not terrorist malware that destroys a power plant, but rather terrorist exploitation of ICTs as an enabling layer for terrorism: online recruitment and propaganda, secure communications, operational planning, intimidation, and financing. This is also how international organizations generally frame the problem: cyberterrorism is addressed through counterterrorism (CT) policy and institutions, with cyber treated as a cross-cutting accelerator of terrorist capability rather than as a separate warfighting domain.

Because pure cyberterrorism incidents are relatively rare, evaluating each organization's response requires a consistent analytical framework. In this paper, four attributes structure the comparison below: detection and information sharing, disruption of terrorist cyber-enabling activity, protection of likely targets and reduction of vulnerability, and post-incident recovery and learning. This reflects how these organizations actually operate in practice: the UN as a global convening and capacity-building system, NATO as a collective security alliance with defensive cyber support options,[52] and the OSCE as a regional security organization focused on confidence-building, resilience, and practical assistance. [53]

The United Nations approaches cyberterrorism primarily through its broader CT architecture and the logic of prevention: strengthening member states' ability to identify, investigate, and prosecute terrorist activity that is facilitated by digital tools. A key signal of this approach is the UN Office of Counter-Terrorism's programming on "Cybersecurity and New Technologies," which is explicitly designed to help member states raise awareness of terrorist cyber threats and enhance technical capacity to prevent and respond to terrorist misuse of digital technologies.[54] Rather than offering operational cyber response teams, the UN's comparative advantage is institutional: it can standardize understanding, diffuse best practices, and provide a legitimacy framework that helps states cooperate across borders.

Analytically, the UN's strongest contributions fall under indirect prevention and post-incident learning. First, UN CT bodies treat terrorist exploitation of the internet as a persistent strategic problem and encourage member states to align domestic approaches with international obligations and human-rights considerations. The UN Security Council Counter-Terrorism Committee Executive Directorate has emphasized how terrorists exploit online platforms and digital ecosystems to facilitate a wide range of terrorist purposes.[55] This framing matters because it keeps cyberterrorism within CT's legal-operational toolkit rather than pushing it toward uncertain "cyber war" thresholds. Second, the UN ecosystem increasingly connects cyberterrorism to the broader market of cybercrime services: a 2024 UNICRI/UNOCT-linked report highlighted terrorist and violent extremist use of the dark web and "cybercrime-as-a-service," which explains how terrorist actors can outsource capability even when they lack internal expertise.[56]

NATO's counter-terrorism work is explicitly policy-driven and structured around three pillars: awareness, capabilities, and engagement, which informs the analysis of their cyberterrorism response.[57] NATO's approach differs from the UN in two important ways. First, it treats terrorism as a direct security threat to Allies and integrates CT work across deterrence/defence, crisis management, and cooperative security. Second, NATO is able to support defensive cyber operations through alliance mechanisms that can respond faster than UN deliberative processes, though still constrained by political approval.

NATO's most relevant cyber capability for cyberterrorism is its defensive support and assistance capacity. NATO publicly states that its Cyber Rapid Reaction Teams are on standby 24/7 to assist Allies if requested and approved by the North Atlantic Council.[58] This matters for cyberterrorism because the most plausible terrorist cyber scenarios, ransomware against emergency services, disruption of transport or communications, or opportunistic attacks on critical infrastructure, require rapid containment and recovery more than long-term norm setting. In other words, NATO's contribution is strongest in protect/recover functions: helping member states manage incidents that could cause civilian harm or strategic disruption, even if the actor is non-state.

The OSCE frames cyberterrorism through regional security, governance, and stability, emphasizing practical cooperation rather than coercion. Its counter-terrorism work explicitly recognizes terrorism and violent extremism as threats to citizens and to broader stability in the OSCE region.[59] OSCE explicitly

connects its cyber/ICT work to counter-terrorism objectives, including "the use of the internet for terrorist purposes."[60] This makes the OSCE a strong example of how cyberterrorism is operationalized as a CT governance problem: building the processes that allow states to cooperate, share information, and reduce misperception during incidents, especially in politically sensitive environments.

OSCE's cyber capability is less about technical intervention and more about confidence-building and resilience. Its Transnational Threats Department is explicitly structured to address terrorism alongside cyber/ICT security, reflecting an organizational design meant to treat cyber-enabled threats as transnational security challenges.[61] The OSCE's cyber/ICT security materials emphasize concrete activities such as exercises and capacity-building to help participating states respond to cyberattacks on critical infrastructure and to counter terrorist use of the internet. This is a different kind of "cyber capability" than NATO's CRRT model: OSCE increases state readiness and coordination, but it does not function as a deployable cyber defense force.

The OSCE's most important cyber instrument for cyberterrorism-adjacent risk is its set of CBMs to reduce the risks of conflict stemming from ICT use. These CBMs are not anti-terror raids in cyberspace. They are institutional mechanisms, points of contact, information exchange, and consultative procedures that reduce escalation risk and improve crisis communication when incidents occur, including incidents that may involve non-state actors or ambiguous attribution. Subsequent OSCE documents also stress implementation and further development of these CBMs, highlighting rapid technical/policy communication and procedures to reduce misperception and tensions, features that matter in cyberterrorism contexts where uncertainty is high.[62] OSCE also runs practical activities (e.g., national table-top exercises) explicitly focused on addressing terrorist use of the internet, which supports the claim that OSCE's approach is prevention and preparedness oriented.

Genuine cyberterrorism incidents are rare because sustained, damaging cyber operations require resources and operational security most terrorist groups lack, so international organizations mainly treat cyber as an enabling layer for terrorism. Evaluated across detection, disruption, protection, and post-incident recovery, the UN's strength lies in institutional capacity-building and norm-setting, NATO's in rapid defensive response through mechanisms like its Cyber Rapid Reaction Teams, and the OSCE's in confidence-building and regional coordination rather than deployable defense. The three organizations end up playing complementary rather than competing roles, with the OSCE distinguished by its focus on reducing misperception and escalation risk in politically sensitive, low-attribution incidents.

Cyber Espionage

Cyber espionage occupies a unique position in international security. Unlike cyberterrorism, espionage, conducted through traditional human intelligence or digital means, is not explicitly illegal under international law. States have long accepted espionage as an enduring feature of international relations, tolerated in practice even if condemned politically. The rise of cyber capabilities has not altered this legal reality, but it has dramatically expanded the scale, speed, and intrusiveness of espionage activities. As a

result, international organizations face the challenge not of outlawing cyber espionage altogether, but of defining when espionage crosses into unlawful or destabilizing behavior and determining how such boundary violations should affect international relations.

The absence of a clear prohibition on espionage means that the ability to draw normative red lines, particularly over activities that cause significant harm, is a key metric of an organization's ability. In other words, the key question is not whether cyber espionage should be illegal, but where organizations believe restraint is needed to maintain international stability and peace.

The UN approaches cyber espionage through efforts to clarify how existing international law applies in cyberspace rather than through attempts to ban espionage itself. UN bodies such as the Group of Governmental Experts and the Open-Ended Working Group consistently affirm that principles of sovereignty, non-intervention, and due diligence govern state conduct in cyberspace while avoiding claims that espionage violates international law directly. As a result, the UN frames its guidance around the effects of individual cases instead of their intent which is harder to quantify.[63] The UN states cyber operations, regardless of their classification, should not damage critical infrastructure or interfere with critical civilian services.

This approach naturally constrains certain forms of cyber espionage: large-scale data extraction campaigns, persistent access operations that threaten economic stability, and political campaigns that pose a threat to national security to name a few. Through this effects-based framing, the UN seeks to preserve strategic realism while discouraging destabilizing practices. The 2020 SolarWinds operation illustrates both the promise and the limits of this approach. Russian state actors compromised a software update trusted by approximately 18,000 organizations, including the US Treasury Department, the Department of Homeland Security, and parts of the Pentagon, gaining access to sensitive networks for months before detection. The operation was conducted through espionage tradecraft but the persistent access it achieved over critical government infrastructure falls squarely within what the GGE's effects-based framework would identify as destabilizing. Yet no UN body took formal action. The normative logic identified the violation; the institutional architecture could not respond to it.

NATO's focus on ally security means it treats espionage primarily as a counterintelligence and security challenge rather than a legal problem. NATO policy acknowledges that espionage is a persistent feature of state competition and cyber threat forefronts.[64] However, when such espionage threatens military readiness, civilian infrastructure, or alliance cohesion, alliance doctrine draws sharper, firmer boundaries. Similar to the UN, NATO emphasizes that the consequences of a cyber operation matter more than its label as an espionage operation. Certain cyber activities may therefore increase escalation risks even when they fall below the threshold of an armed attack under Article 5.

A central concern for NATO involves persistent access that adversaries could later exploit, known as pre-positioning.[67] This concern has driven NATO to integrate cyber defense into its core security posture and to recognize cyberspace as an operational domain. Although espionage alone does not trigger

collective defense obligations under Article 5, NATO policy acknowledges that severe cyber effects could, in principle, meet that threshold. In response, NATO prioritizes resilience, intelligence sharing, and defensive preparedness over public retaliation.

NATO's capacity to assist member states includes mechanisms such as Cyber Rapid Reaction Teams, which remain on standby around the clock to provide defensive cyber assistance upon request and approval by the North Atlantic Council. These mechanisms do not criminalize espionage, but they reduce its strategic value by limiting adversary access and constraining potential harm. In practice, this approach reinforces bloc-based security dynamics: cyber espionage deepens mistrust among geopolitical rivals even when it remains legally permissible, and NATO's defensive posture does more to contain that mistrust than to resolve it.[68]

The OSCE addresses cyber espionage through a framework centered on risk reduction, transparency, and confidence-building. OSCE policymakers recognize that espionage-related cyber incidents can escalate rapidly when states misinterpret intent or capability. Rather than seeking prohibition, the OSCE focuses on managing the destabilizing consequences of cyber espionage through institutionalized cooperation. It emphasizes the dangers that arise when cyber intrusions generate uncertainty about intent or escalate political tensions. In this context, the OSCE's contribution lies not in attempting to draw hard legal prohibitions around espionage, but in structuring communication, transparency, and procedural restraint so that espionage-related cyber incidents do not spiral into broader crises.

Two illustrative examples highlight this approach. First, following repeated cyber incidents affecting Ukrainian government and energy-sector networks after 2014, OSCE forums increasingly emphasized the need for clarity, communication, and restraint in state cyber behavior, even where incidents fell short of destructive cyberattacks.[65] Rather than focusing on attribution or condemnation, OSCE discussions centered on preventing misinterpretation of cyber intrusions that could exacerbate an already volatile security environment. Second, OSCE cybersecurity dialogues have repeatedly addressed concerns arising from large-scale cyber intrusions against governmental and diplomatic systems across the OSCE region, including incidents widely understood as intelligence collection.[66] In response, the OSCE promoted enhanced transparency regarding national cyber policies and encouraged participating States to maintain open channels for consultation following significant cyber events, recognizing that unmanaged espionage-related incidents could escalate political tensions even without physical damage.

Rather than prioritizing punishment or deterrence, the OSCE's approach emphasizes predictability and escalation control. By encouraging states to clarify doctrine, sustain communication, and contextualize cyber incidents within cooperative security mechanisms, the OSCE seeks to contain the destabilizing effects of cyber espionage without attempting to eliminate the practice itself. This strategy reflects a pragmatic institutional choice: espionage persists as a structural reality of international relations, but its most dangerous consequences arise from misunderstanding rather than from intelligence collection alone. In this way, the OSCE complements NATO's security-focused posture and the UN's normative efforts by concentrating on risk containment and crisis management, rather than on legal prohibition.

ANALYSIS

The previous sections demonstrate that no existing international organization currently possesses the authority, technical capacity, and political freedom to comprehensively prevent or deter cyberwarfare. However, there is an organization that seems best fit to organize efforts that regulate cyberwarfare. The Organization for Security and Co-operation in Europe has the potential to become a leader in securing and regulating cyberspace with the assistance of other organizations. This final analysis will take into account four clear evaluation criteria: (1) ability to directly engage with cyber incidents, (2) the breadth of membership across the globe, (3) ability to stay politically neutral and prevent escalation, and (4) ability to set precedent for future incidents and policy. Although some criteria are not filled by the OSCE as well as comparable organizations, taking into account future potential and current trade-offs, the OSCE is better positioned than the UN and NATO to fulfill that role.

The OSCE has a significant advantage over the UN and NATO when evaluating its ability to directly engage with cyber incidents, big or small. A central pattern across the body of evidence shows that direct pre-incident prevention remains underdeveloped across all organizations. The United Nations lacks enforcement mechanisms and relies on non-binding norms, and NATO's direct intervention capabilities remain politically constrained and alliance-specific. Hence, effectiveness in cyberwarfare depends less on legal force or deterrence and more on incident-level engagement, escalation management, and resilience building. Although the OSCE does not possess coercive authority, it does have more experience in preventing and aiding states in a cyber incident in non-obligatory situations. The OSCE consistently operates closest to the point of impact, particularly in cases involving elections, infrastructure disruption, and regional instability.

Where this advantage is clearest is in politically sensitive situations. The UN waits for post-incident consensus; NATO acts only when alliance-wide approval is secured. The OSCE's election monitoring presence in Ukraine and Moldova, its post-incident infrastructure dialogue, and its confidence-building mechanisms all demonstrate an organization that engages before other institutions have agreed on whether to respond at all.

The breadth of membership and political neutrality play a critical role in determining how effectively an organization can address cyberwarfare, particularly when incidents cross borders and involve multiple political systems. It prevents escalation and allows for diplomatic solutions. Cyber operations frequently exploit regional interdependence, shared infrastructure, and jurisdictional gaps, which makes inclusive participation an operational advantage rather than a symbolic one. When comparing the OSCE, NATO, and the UN, differences in membership structure significantly shape each organization's practical capacity to engage with cyber incidents.

NATO's membership structure presents clear limitations in this regard. While its cohesion strengthens collective defense, it also frames cyber incidents through a strategic competition lens that discourages

participation from non-member states. This dynamic constrains NATO's ability to engage in cyber incidents that require cooperation beyond the alliance, especially when attribution remains uncertain or when incidents involve civilian infrastructure. The United Nations, by contrast, benefits from universal membership, which in theory allows for the most inclusive form of cyber governance. In practice, however, decision-making power remains heavily concentrated within the Security Council, where the permanent five members hold veto authority. This structure complicates meaningful inclusion, particularly when cyber incidents implicate major cyber powers. Political rivalry among permanent members frequently slows or blocks collective action, limiting the UN's ability to respond to cyber incidents in a timely or coordinated manner. As a result, the UN's broad membership often translates into legitimacy without operational agility.

The OSCE occupies a middle ground that enhances its practical potential. With 57 participating States spanning North America, Europe, Central Asia, and parts of the post-Soviet space, the OSCE includes both frequent cyber targets and suspected sources of cyber activity within a single institutional framework. This breadth allows the OSCE to address cyber incidents without defaulting to alliance politics or global power rivalries. Its regional focus enables deeper engagement and sustained cooperation, while its inclusive membership preserves legitimacy among participating States. In the context of cyberwarfare, where cooperation and communication matter more than enforcement, the OSCE's balanced membership structure provides a significant operational advantage.

This advantage carries a structural tension that must be acknowledged directly. Russia is an OSCE participating State and has been since the organization's founding. It is also the state most frequently attributed as the actor behind the major cyberattacks examined in this paper — the 2007 Estonia DDoS, the 2015–2016 Ukraine power grid attacks, the 2016 US and 2017 French election interference operations, and NotPetya. Russia's participation enables the dialogue and confidence-building that give the OSCE its comparative value, but it also means the primary threat actor in European cyber conflict sits at the same table as its targets. This is not grounds for dismissing the OSCE as a governing institution — the same tension exists in UN Security Council dynamics, where veto-holding permanent members regularly block action against themselves and their allies. It does, however, mean that the OSCE's political neutrality is less a structural feature than a deliberate and fragile posture that depends on Russia's continued willingness to participate in good faith. The organization's effectiveness in managing cyberwarfare may be most reliable precisely in contexts where Russian interests are not directly implicated.

The main critique of the OSCE centers on its limited ability to set binding precedent or shape future cyber policy at a global level. Unlike the United Nations, which operates as the primary forum for international norm development, or NATO, which influences state behavior through deterrence and security doctrine, the OSCE lacks formal mechanisms to codify binding rules or enforce compliance. This limitation, however, does not undermine the OSCE's practical potential in cyberwarfare. Instead, it highlights a functional division of labor in international cyber governance, where precedent-setting and operational engagement need not reside within the same institution.

The United Nations already occupies the role of normative authority in cyberspace. Through processes such as the Group of Governmental Experts and the Open-Ended Working Group, the UN develops global frameworks that articulate how international law applies to cyber activity and establish expectations for responsible state behavior. These norms shape long-term precedent and influence state conduct at a conceptual level, but they rarely translate into immediate operational impact during active cyber incidents. The OSCE does not compete with this function. Rather, it benefits from it by operating within an established normative environment that provides legal and ethical boundaries for its engagement. In this sense, the UN supplies the rules of the road, while the OSCE applies them in practice.

CONCLUSION

Crucially, cyberwarfare does not require every organization to perform every function. Attempting to centralize enforcement, deterrence, and norm creation within a single institution would likely reduce effectiveness rather than enhance it. Cyber conflict unfolds across legal, political, and technical domains, each of which demands different tools. The OSCE's inability to set a binding precedent, therefore, reflects not a weakness but a specialization. Its strength lies in managing incidents, facilitating dialogue, and preventing escalation within the boundaries already defined by broader international policy frameworks.

By relying on the UN for normative guidance, the OSCE avoids mandate overreach and preserves its legitimacy as a neutral, cooperative actor. This institutional complementarity allows the OSCE to focus on what it does best: translating abstract norms and security principles into practical engagement during cyber incidents. In doing so, the OSCE demonstrates that effective cyber governance depends less on centralized authority and more on coordinated specialization, where each organization contributes according to its comparative advantage.

Although the OSCE currently lacks the institutional capacity to assume full responsibility for managing cyberwarfare, it remains the organization best positioned to evolve into such a role. This conclusion does not imply that the OSCE should transform into a coercive cyber authority or a military cyber force. Rather, it reflects the organization's structural compatibility with the realities of cyber conflict, which favor flexibility, legitimacy, and sustained engagement over enforcement or deterrence. The practical question, therefore, concerns what incremental developments would allow the OSCE to translate its comparative advantages into greater operational effectiveness.

One necessary development involves the creation of rapid deployment teams tailored to cyber incidents. These teams would function as defensive cyber units similar to NATO's CRRTs, working as groups capable of engaging states during or immediately after cyber incidents. Their role would include incident assessment, verification support, coordination with national authorities, and stabilization efforts in politically sensitive environments. This model aligns with the OSCE's existing approach in election observation and post-conflict monitoring, where early engagement and neutral reporting reduce escalation

and support institutional recovery. Rapid deployment teams would strengthen the OSCE's ability to operate at the point of impact without undermining its cooperative security mandate.

A second critical step involves expanding the OSCE's geographic inclusion, particularly to African and South American states. Cyberwarfare increasingly affects regions beyond the OSCE's traditional Euro-Atlantic focus, with infrastructure interdependence and digital supply chains linking global systems. Limiting OSCE participation to its current regional scope risks reinforcing fragmented cyber governance and excluding states that experience growing cyber vulnerability but lack institutional support. Carefully structured expansion would enhance the OSCE's legitimacy and relevance while preserving its neutral posture. Importantly, this expansion would not require universal membership but strategic inclusion of regions currently underrepresented in cyber governance frameworks.

These reforms would not eliminate the need for the UN or NATO. Instead, they would reinforce a division of labor in which the UN continues to develop global norms, NATO maintains deterrence and defense within alliance boundaries, and the OSCE operates as the primary institution for incident-level engagement, stabilization, and cooperative management. By avoiding mandate overreach and focusing on incremental, mandate-consistent expansion, the OSCE could strengthen its practical role without sacrificing neutrality or legitimacy.

The SolarWinds operation and the failure of any international institution to formally respond to it captures the central problem this paper has traced. The operation was identifiable, attributable with reasonable confidence, and fell within the effects-based prohibitions that the UN's own frameworks articulate. Yet no body acted. The UN lacked enforcement authority. NATO lacked jurisdiction over a non-kinetic operation affecting non-member systems. The OSCE lacked the technical capacity to intervene. What that gap reveals is not that international institutions are useless in cyberspace, but that they are currently organized around functions — norm-setting, collective defense, confidence-building — that were not designed to converge on a single incident. The case for the OSCE is not that it alone can fill this gap, but that it is structurally positioned to become the institution where those functions begin to connect: present at the incident level, inclusive enough to convene adversaries, and neutral enough to act without triggering escalation. Whether it develops the capacity to do so remains an open question, and one that the pace of state-sponsored cyber activity makes increasingly urgent.

This study has notable limitations. The evaluation of the UN, NATO, and OSCE relies heavily on incidents that each organization has itself documented, referenced, or responded to, which means the comparison likely understates cases these institutions overlooked, declined to publicize, or never engaged with in the first place. Relatedly, the incidents examined skew toward moderate and mid-range cyberwarfare; because truly extreme cases, such as attacks producing mass civilian casualties or the sustained collapse of national infrastructure, remain rare or largely hypothetical, this paper's framework could not be tested against the upper bound of what cyberwarfare is capable of, leaving uncertain whether these organizations' comparative strengths and weaknesses would hold under far more severe conditions. Future research should draw on a wider set of documented incidents, including those handled outside

major international institutions, and should revisit this comparison as more extreme cyberwarfare scenarios materialize and as the UN, NATO, and OSCE continue to adapt their capabilities.

NOTES

1. "International Law in Cyberspace," U.S. Department of State, September 18, 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.
2. Rand Corporation, "Cyber Warfare," Rand.org, 2019, https://www.rand.org/topics/cyber-warfare.html.
3. "Hybrid Threats: 2007 Cyber Attacks on Estonia," NATO Strategic Communications Centre of Excellence, June 6, 2019, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.
4. Tim Maurer, "When States Pretend to Be Terrorists or Hacktivists in Cyberspace," Carnegie Endowment for International Peace (Cipher Brief, 2017), https://carnegieendowment.org/posts/2017/04/when-states-pretend-to-be-terrorists-or-hacktivists-in-cyberspace?lang=en.
5. S. Boyko, "UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," International Affairs 62, no. 005 (October 31, 2016): 242–54, https://doi.org/10.21557/iaf.47559235.
6. "The ILOVEYOU Worm, a Global Crisis," cyberTAP (Purdue University, 2024), https://cyber.tap.purdue.edu/blog/articles/the-iloveyou-worm-a-global-crisis/.
7. Roger Collier, "NHS Ransomware Attack Spreads Worldwide," Canadian Medical Association Journal 189, no. 22 (June 5, 2017): E786–87, https://doi.org/10.1503/cmaj.1095434.
8. Federal Bureau of Investigation, "2024 Internet Crime Report," Internet Crime Complaint Center (IC3), April 23, 2025, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
9. CDR Peter Pascucci, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution," Minnesota Journal of International Law 1, no. 26 (2017), https://scholarship.law.umn.edu/cgi/viewcontent.cgi?params=/context/mjil/article/1256/&path_info=auto_convert.pdf.
10. Nataliya Tkachuk, "Ukraine as the Frontline of European Cyber Defence: Building Resilience in the Face of Russian Cyber Aggression" (Tallinn Paper No. 15, 2025), https://ccdcoe.org/uploads/2025/07/Tkachuk_N_Tallinn_Paper_15_Ukraine-as-the-Frontline-of-European-Cyber-Defence.pdf.
11. "SR-029.022025: MyCERT Report - Cyber Incident Quarterly Summary Report - Q4 2024," MyCERT, February 27, 2025, https://www.mycert.org.my/portal/advisory?id=SR-029.022025.
12. Arindrajit Basu, Irene Poetranto, and Justin Lau, "The UN Struggles to Make Progress on Securing Cyberspace," Carnegie Endowment for International Peace, May 19, 2021, https://carnegieendowment.org/research/2021/05/the-un-struggles-to-make-progress-on-securing-cyberspace?lang=en.
13. U.S. Department of State, "International Law in Cyberspace."

14. "Doctrine of Information Security of the Russian Federation," Security Council of the Russian Federation, December 5, 2016, http://www.scrf.gov.ru/security/information/DIB_engl/.
15. "Sovereignty," International Cyber Law Toolkit, May 5, 2022, https://cyberlaw.ccdcoe.org/wiki/Sovereignty.
16. Katja S. Ziegler, "Domaine Réservé," Oxford Public International Law, 2023, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1398.
17. NATO, "Hybrid Threats."
18. Joby Warrick and Ellen Nakashima, "Foreign Intelligence Officials Say Attempted Cyberattack on Israeli Water Utilities Linked to Iran," Washington Post, May 10, 2020, https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html.
19. David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," Security Dialogue 44, no. 2 (April 2013): 147–64, https://doi.org/10.1177/0967010613478323.
20. Betz and Stevens, "Analogical Reasoning."
21. William Ralston, "The Untold Story of a Cyberattack, a Hospital and a Dying Woman," Wired, November 11, 2020, https://www.wired.com/story/ransomware-hospital-death-germany/.
22. "UN Charter," United Nations, 1945, https://www.un.org/en/about-us/un-charter.
23. "Ethiopia: New Spate of Abusive Surveillance," Human Rights Watch, December 6, 2017, https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance.
24. United Nations, "About Us," Office of Counter-Terrorism, 2024, https://www.un.org/counterterrorism/en/about.
25. UN Press, "General Assembly Lauds Success of Law of Sea Convention, but Deplores Sea-Level Rise, Lack of Support for Small Island Nations, Increased Maritime Risks," United Nations, December 8, 2022, https://press.un.org/en/2022/ga12479.doc.htm.
26. Center for Preventive Action, "Territorial Disputes in the South China Sea," Global Conflict Tracker (Council on Foreign Relations, September 17, 2024), https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea.
27. Office of Counter-Terrorism, "Cybersecurity and New Technologies," United Nations, 2024, https://www.un.org/counterterrorism/en/cybersecurity.
28. "Universal Declaration of Human Rights," United Nations, December 10, 1948, https://www.un.org/en/about-us/universal-declaration-of-human-rights.
29. "Can Dündar, Turkey," Committee to Protect Journalists, January 3, 2023, https://cpj.org/awards/can-dundar-turkey/.
30. "Cyber Defence," North Atlantic Treaty Organization, 2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence.
31. "About Us," NATO Cooperative Cyber Defence Centre of Excellence, accessed October 22, 2025, https://ccdcoe.org/about-us/.
32. "Confidence and Security Building Measures," Organization for Security and Co-operation in Europe, accessed October 24, 2025, https://www.osce.org/secretariat/107484.
33. "Cyber/ICT Security," Organization for Security and Co-operation in Europe, December 9, 2016, https://www.osce.org/field-of-work/Cyber-ICT-security.

34. Dennis Broeders, "The (Im)Possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG: A Mid-Process Assessment," Journal of Cyber Policy 6, no. 3 (April 26, 2021): 277–97, https://doi.org/10.1080/23738871.2021.1916976.
35. Bart Hogeveen, "The UN Norms of Responsible State Behaviour in Cyberspace" (The Australian Strategic Policy Institute, March 2022), https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.
36. Ben Depoorter and Stephan Tontrup, "The Costs of Unenforced Laws: A Field Experiment," Social Science Research Network, March 17, 2016, https://doi.org/10.2139.
37. Zack Beauchamp, "The Key Findings from the US Intelligence Report on the Russia Hack, Decoded," Vox, January 6, 2017, https://www.vox.com/world/2017/1/6/14194986/russia-hack-intelligence-report-election-trump.
38. "Cyber Defence Pledge," North Atlantic Treaty Organization, July 8, 2016, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/cyber-defence-pledge?.
39. "Cyber Coalition: NATO's Flagship Cyber Exercise," NATO Allied Command Transformation, accessed November 30, 2025, https://www.act.nato.int/activities/cyber-coalition.
40. North Atlantic Treaty Organization, "Collective Defence."
41. "Ukraine, Presidential Election, 31 March 2019: Needs Assessment Mission Report," OSCE Office for Democratic Institutions and Human Rights (Organization for Security and Co-operation in Europe, December 21, 2018), https://odihr.osce.org/odihr/elections/ukraine/407657?download=true.
42. "Moldova, Presidential Election, 30 October 2016: Statement of Preliminary Findings and Conclusions," OSCE Office for Democratic Institutions and Human Rights (Organization for Security and Co-operation in Europe, August 31, 2016), https://odihr.osce.org/odihr/elections/moldova/278191.
43. "Albania, Parliamentary Elections, 25 April 2021: Final Report," OSCE Office for Democratic Institutions and Human Rights (Organization for Security and Co-operation in Europe, July 26, 2021), https://odihr.osce.org/odihr/elections/albania/493687.
44. "Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations, August 8, 2022, https://docs.un.org/en/A/77/275.
45. Häly Laasme, "Estonia: Cyber Window into the Future of NATO," Joint Force Quarterly, no. 63 (2011): 58–63, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_58-63_Laasme.pdf?ver=Gmp2P_MaR_5WUw4ETKCnXA%3D%3D.
46. Emily Benson and Pau Alvarez-Aragones, "NATO and Economic Security: A Political Oxymoron or Inevitability?," Center for Strategic International Studies, May 15, 2024, https://www.csis.org/analysis/nato-and-economic-security-political-oxymoron-or-inevitability.
47. "OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," Organization for Security and Co-Operation in Europe (Organization for Security and Co-operation in Europe, March 10, 2016), https://www.osce.org/sites/default/files/f/documents/d/a/227281.pdf.

48. Jonathan Greig, "NSA, Viasat Say 2022 Hack Was Two Incidents; Russian Sanctions Resulted from Investigation," The Record from Recorded Future News, August 11, 2023, https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions.
49. "Ransomware Attacks on Healthcare Sector 'Pose a Direct and Systemic Risk to Global Public Health and Security', Executive Tells Security Council | Meetings Coverage and Press Releases," United Nations, November 8, 2024, https://press.un.org/en/2024/sc15891.doc.htm.
50. "Permanent Council Decision No. 1106," Organization for Security and Co-Operation in Europe (Organization for Security and Co-operation in Europe, December 3, 2013), https://www.osce.org/pc/109168.
51. "Permanent Council Decision No. 1202," Organization for Security and Co-Operation in Europe (Organization for Security and Co-operation in Europe, March 10, 2016), https://www.osce.org/pc/227281.
52. "Countering Terrorism," North Atlantic Treaty Organization, August 6, 2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism.
53. "Countering Terrorism," Organization for Security and Co-operation in Europe, accessed November 30, 2025, https://www.osce.org/field-of-work/countering-terrorism.
54. Office of Counter-Terrorism, "Cybersecurity and New Technologies."
55. "Counter-Terrorism in Cyberspace," United Nations, October 2021, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ct_in_cyberspace_oct_2021.pdf.
56. "NEW Report! Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-As-a-Service for Cyber-Attacks | UNICRI :: United Nations Interregional Crime and Justice Research Institute," United Nations Interregional Crime and Justice Research Institute, June 28, 2024, https://unicri.org/news/new-report-beneath-surface-terrorist-and-violent-extremist-use-dark-web-and-cybercrime-service-cyber-attacks.
57. North Atlantic Treaty Organization, "Countering Terrorism."
58. "Cyber Defence," NATO Allied Command Transformation, accessed November 30, 2025, https://www.act.nato.int/activities/cyber/.
59. Organization for Security and Co-operation in Europe, "Countering Terrorism."
60. Organization for Security and Co-operation in Europe, "Cyber/ICT Security."
61. "OSCE Transnational Threats Department," Organization for Security and Co-operation in Europe, accessed November 29, 2025, https://tntd.osce.org/?.
62. "Decision No. 5/16: OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies ," Organization for Security and Co-Operation in Europe (Organization for Security and Co-operation in Europe, December 9, 2016), https://www.osce.org/sites/default/files/f/documents/2/8/288086.pdf.
63. "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," NATO Cooperative Cyber Defence Centre of Excellence, 2015, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

64. NATO Allied Command Transformation, "Strengthening Cyber Resilience: NATO's Cyber Coalition and Collective Defence," NATO Allied Command Transformation, November 29, 2024, https://www.act.nato.int/article/cyber-coalition-collective-defence/.
65. Organization for Security and Co-operation in Europe, "Status Report as of 25 February 2019," Organization for Security and Co-Operation in Europe, March 1, 2019, https://www.osce.org/special-monitoring-mission-to-ukraine/412862.
66. Organization for Security and Co-operation in Europe, "Transnational Threats Department, Cyber/ICT Security," Organization for Security and Co-Operation in Europe, accessed November 25, 2025, https://www.osce.org/sites/default/files/f/documents/c/c/256071.pdf.
67. IBM, "Are attackers already embedded in U.S. critical infrastructure networks?", IBM, accessed Jul 10, 2026, https://www.ibm.com/think/insights/are-attackers-already-embedded-in-us-critical-infrastructure-networks
68. Sophie Arts, "Offense as the New Defense: New Life for NATO's Cyber Policy", GMF, accessed Jul 10, 2026, https://www.gmfus.org/news/offense-new-defense-new-life-natos-cyber-policy

BIBLIOGRAPHY

"Albania, Parliamentary Elections, 25 April 2021: Final Report." OSCE Office for Democratic Institutions and Human Rights. Organization for Security and Co-operation in Europe, July 26, 2021. https://odihr.osce.org/odihr/elections/albania/493687.
Basu, Arindrajit, Irene Poetranto, and Justin Lau. "The UN Struggles to Make Progress on Securing Cyberspace." Carnegie Endowment for International Peace, May 19, 2021. https://carnegieendowment.org/research/2021/05/the-un-struggles-to-make-progress-on-securing-cyberspace?lang=en.
Beauchamp, Zack. "The Key Findings from the US Intelligence Report on the Russia Hack, Decoded." Vox, January 6, 2017. https://www.vox.com/world/2017/1/6/14194986/russia-hack-intelligence-report-election-trump.
Benson, Emily, and Pau Alvarez-Aragones. "NATO and Economic Security: A Political Oxymoron or Inevitability?" Center for Strategic International Studies, May 15, 2024. https://www.csis.org/analysis/nato-and-economic-security-political-oxymoron-or-inevitability.
Betz, David J., and Tim Stevens. "Analogical Reasoning and Cyber Security." Security Dialogue 44, no. 2 (April 2013): 147–64. https://doi.org/10.1177/0967010613478323.
Broeders, Dennis. "The (Im)Possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG: A Mid-Process Assessment." Journal of Cyber Policy 6, no. 3 (April 26, 2021): 277–97. https://doi.org/10.1080/23738871.2021.1916976.
Center for Preventive Action. "Territorial Disputes in the South China Sea." Global Conflict Tracker. Council on Foreign Relations, September 17, 2024. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea.
Collier, Roger. "NHS Ransomware Attack Spreads Worldwide." Canadian Medical Association Journal 189, no. 22 (June 5, 2017): E786–87. https://doi.org/10.1503/cmaj.1095434.

Committee to Protect Journalists. “Can Dündar, Turkey,” January 3, 2023.
https://cpj.org/awards/can-dundar-turkey/.
“Counter-Terrorism in Cyberspace.” United Nations, October 2021.
https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ct_in_cyberspace_oct_2021.pdf.
cyberTAP. “The ILOVEYOU Worm, a Global Crisis.” Purdue University, 2024.
https://cyber.tap.purdue.edu/blog/articles/the-iloveyou-worm-a-global-crisis/.
“Decision No. 5/16: OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies .” Organization for Security and Co-Operation in Europe. Organization for Security and Co-operation in Europe, December 9, 2016.
https://www.osce.org/sites/default/files/f/documents/2/8/288086.pdf.
Depoorter, Ben, and Stephan Tontrup. “The Costs of Unenforced Laws: A Field Experiment.” Social Science Research Network, March 17, 2016. https://doi.org/10.2139.
Federal Bureau of Investigation. “2024 Internet Crime Report.” Internet Crime Complaint Center (IC3), April 23, 2025. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
Greig, Jonathan. “NSA, Viasat Say 2022 Hack Was Two Incidents; Russian Sanctions Resulted from Investigation.” The Record from Recorded Future News, August 11, 2023.
https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions.
Hogeveen, Bart . “The UN Norms of Responsible State Behaviour in Cyberspace.” The Australian Strategic Policy Institute, March 2022.
https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.
Human Rights Watch. “Ethiopia: New Spate of Abusive Surveillance,” December 6, 2017.
https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance.
IBM, “Are attackers already embedded in U.S. critical infrastructure networks?”, IBM, accessed Jul 10, 2026,
https://www.ibm.com/think/insights/are-attackers-already-embedded-in-us-critical-infrastructure-networks
International Cyber Law Toolkit. “Sovereignty,” May 5, 2022.
https://cyberlaw.ccdcoe.org/wiki/Sovereignty.
Laasme, Häly. “Estonia: Cyber Window into the Future of NATO.” Joint Force Quarterly, no. 63 (2011): 58–63.
https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_58-63_Laasme.pdf?ver=Gmp2P_MaR_5WUw4ETKCnXA%3D%3D.
Maurer, Tim. “When States Pretend to Be Terrorists or Hacktivists in Cyberspace.” Carnegie Endowment for International Peace. Cipher Brief, 2017.
https://carnegieendowment.org/posts/2017/04/when-states-pretend-to-be-terrorists-or-hacktivists-in-cyberspace?lang=en
“Moldova, Presidential Election, 30 October 2016: Statement of Preliminary Findings and Conclusions.” OSCE Office for Democratic Institutions and Human Rights. Organization for Security and Co-operation in Europe, August 31, 2016. https://odihr.osce.org/odihr/elections/moldova/278191.

MyCERT. “SR-029.022025: MyCERT Report - Cyber Incident Quarterly Summary Report - Q4 2024,” February 27, 2025. https://www.mycert.org.my/portal/advisory?id=SR-029.022025.
NATO Allied Command Transformation. “Cyber Coalition: NATO’s Flagship Cyber Exercise.” NATO Allied Command Transformation. Accessed November 30, 2025. https://www.act.nato.int/activities/cyber-coalition.
———. “Cyber Defence.” NATO Allied Command Transformation. Accessed November 30, 2025. https://www.act.nato.int/activities/cyber/.
———. “Strengthening Cyber Resilience: NATO’s Cyber Coalition and Collective Defence.” NATO Allied Command Transformation, November 29, 2024. https://www.act.nato.int/article/cyber-coalition-collective-defence/.
NATO Cooperative Cyber Defence Centre of Excellence. “2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law.” NATO Cooperative Cyber Defence Centre of Excellence, 2015. https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.
———. “About Us.” NATO Cooperative Cyber Defence Centre of Excellence. Accessed October 22, 2025. https://ccdcoe.org/about-us/.
———. “Hybrid Threats: 2007 Cyber Attacks on Estonia.” NATO Strategic Communications Centre of Excellence, June 6, 2019. https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.
North Atlantic Treaty Organization. “Collective Defence and Article 5.” North Atlantic Treaty Organization, November 12, 2025. https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5.
———. “Countering Terrorism.” North Atlantic Treaty Organization, August 6, 2025. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism.
———. “Cyber Defence.” North Atlantic Treaty Organization, 2025. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence.
———. “Cyber Defence Pledge.” North Atlantic Treaty Organization, July 8, 2016. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/cyber-defence-pledge?.
Office of Counter-Terrorism. “Cybersecurity and New Technologies.” United Nations, 2024. https://www.un.org/counterterrorism/en/cybersecurity.
Organization for Security and Co-operation in Europe. “Confidence and Security Building Measures.” Organization for Security and Co-operation in Europe. Accessed October 24, 2025. https://www.osce.org/secretariat/107484.
———. “Countering Terrorism.” Organization for Security and Co-operation in Europe. Accessed November 30, 2025. https://www.osce.org/field-of-work/countering-terrorism.
———. “Cyber/ICT Security.” Organization for Security and Co-operation in Europe, December 9, 2016. https://www.osce.org/field-of-work/Cyber-ICT-security.
———. “OSCE Transnational Threats Department.” Organization for Security and Co-operation in Europe. Accessed November 29, 2025. https://tntd.osce.org/?.

———. “Status Report as of 25 February 2019.” Organization for Security and Co-Operation in Europe, March 1, 2019. https://www.osce.org/special-monitoring-mission-to-ukraine/412862.
———. “Transnational Threats Department, Cyber/ICT Security.” Organization for Security and Co-Operation in Europe. Accessed November 25, 2025. https://www.osce.org/sites/default/files/f/documents/c/c/256071.pdf.
“OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.” Organization for Security and Co-Operation in Europe. Organization for Security and Co-operation in Europe, March 10, 2016. https://www.osce.org/sites/default/files/f/documents/d/a/227281.pdf.
Pascucci, CDR Peter. “Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution.” Minnesota Journal of International Law 1, no. 26 (2017). https://scholarship.law.umn.edu/cgi/viewcontent.cgi?params=/context/mjil/article/1256/&path_info=auto_convert.pdf.
“Permanent Council Decision No. 1106.” Organization for Security and Co-Operation in Europe. Organization for Security and Co-operation in Europe, December 3, 2013. https://www.osce.org/pc/109168.
“Permanent Council Decision No. 1202.” Organization for Security and Co-Operation in Europe. Organization for Security and Co-operation in Europe, March 10, 2016. https://www.osce.org/pc/227281.
Ralston, William. “The Untold Story of a Cyberattack, a Hospital and a Dying Woman.” Wired, November 11, 2020. https://www.wired.com/story/ransomware-hospital-death-germany/.
Rand Corporation. “Cyber Warfare.” Rand.org, 2019. https://www.rand.org/topics/cyber-warfare.html.
S. Boyko. “UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” International Affairs 62, no. 005 (October 31, 2016): 242–54. https://doi.org/10.21557/iaf.47559235.
Sophie Arts, “Offense as the New Defense: New Life for NATO’s Cyber Policy”, GMF, accessed Jul 10, 2026, https://www.gmfus.org/news/offense-new-defense-new-life-natos-cyber-policy
Security Council of the Russian Federation. “Doctrine of Information Security of the Russian Federation,” December 5, 2016. http://www.scrf.gov.ru/security/information/DIB_engl/.
Tkachuk, Nataliya. “Ukraine as the Frontline of European Cyber Defence: Building Resilience in the Face of Russian Cyber Aggression.” Tallinn Paper No. 15, 2025. https://ccdcoe.org/uploads/2025/07/Tkachuk_N_Tallinn_Paper_15_Ukraine-as-the-Frontline-of-European-Cyber-Defence.pdf.
U.S. Department of State. “International Law in Cyberspace,” September 18, 2012. https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.
“Ukraine, Presidential Election, 31 March 2019: Needs Assessment Mission Report.” OSCE Office for Democratic Institutions and Human Rights. Organization for Security and Co-operation in Europe, December 21, 2018. https://odihr.osce.org/odihr/elections/ukraine/407657?download=true.
UN Press. “General Assembly Lauds Success of Law of Sea Convention, but Deplores Sea-Level Rise, Lack of Support for Small Island Nations, Increased Maritime Risks.” United Nations, December 8, 2022. https://press.un.org/en/2022/ga12479.doc.htm.

United Nations. “About Us.” Office of Counter-Terrorism, 2024. https://www.un.org/counterterrorism/en/about.
———. “Developments in the Field of Information and Telecommunications in the Context of International Security.” United Nations, August 8, 2022. https://docs.un.org/en/A/77/275.
———. “Ransomware Attacks on Healthcare Sector ‘Pose a Direct and Systemic Risk to Global Public Health and Security’, Executive Tells Security Council | Meetings Coverage and Press Releases.” United Nations, November 8, 2024. https://press.un.org/en/2024/sc15891.doc.htm.
———. “UN Charter.” United Nations, 1945. https://www.un.org/en/about-us/un-charter.
———. “Universal Declaration of Human Rights.” United Nations, December 10, 1948. https://www.un.org/en/about-us/universal-declaration-of-human-rights.
United Nations Interregional Crime and Justice Research Institute. “NEW Report! Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-As-a-Service for Cyber-Attacks | UNICRI :: United Nations Interregional Crime and Justice Research Institute,” June 28, 2024. https://unicri.org/news/new-report-beneath-surface-terrorist-and-violent-extremist-use-dark-web-and-cybercrime-service-cyber-attacks.
Warrick, Joby, and Ellen Nakashima. “Foreign Intelligence Officials Say Attempted Cyberattack on Israeli Water Utilities Linked to Iran.” Washington Post, May 10, 2020. https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html.
Ziegler, Katja S. “Domaine Réservé.” Oxford Public International Law, 2023. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1398.