

Forum: Disarmament Commission

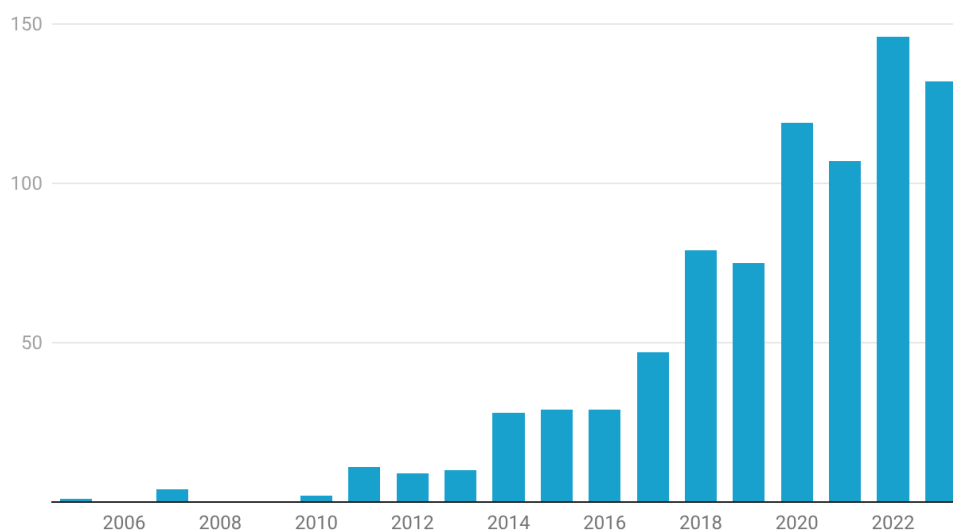
Issue: Preventing the Militarization of Cyberspace and the Escalation of Cyber Conflict

Student Officer: Dehao Zhao

Position: Deputy President

Introduction

Number of State-Sponsored Cyberattacks



Source: Council on Foreign Relations • Created with Datawrapper

Figure 1: A chart showing the number of state-sponsored cyberattacks per year (Council on Foreign Relations)

As global reliance upon digital and online systems increases, cybersecurity and cyberattacks have become among the most pressing concerns globally, for both military and civilian purposes alike. As a result, around 161 nations have designated cybersecurity agencies or divisions, with 132 nations possessing national cybersecurity strategies, reflecting the widespread nature of cyber conflict. However, most of these programs either lack real military capacity in cyberspace or heavily rely upon shared services and alliances to effectively defend against sophisticated threats from state-sponsored attacks or prominent terrorist organizations, thus reducing overall efficacy and reliability. Consequently, publicly acknowledged state-sponsored cyberattacks have increased in volume by 45% between 2023 to 2025, whilst intensifying their focus away from intelligence-gathering and towards the disruption of critical infrastructure and physically destructive activities.

Furthermore, various technologies, both future and present, threaten to disrupt global cyberspace and cybersecurity in enormous proportions. Artificial Intelligence (AI), particularly generative AI, has dramatically

altered the current cybersecurity landscape by reducing decision-making time, automating vulnerability detection and exploitation, and allowing non-state actors to conduct increasingly sophisticated cyber operations. Therefore, AI-powered cyberattacks have experienced an 89% year-on-year increase, endangering global cybersecurity. Moreover, quantum computing risks fundamentally undermining the security structure of cyberspace, due to its ability to bypass almost all commonly used types of data encryption. The lack of adoption of quantum-resistant cryptography furthers this issue, as governments do not host mechanisms to protect information from quantum attacks.

As technology has progressed, cyberwarfare has also dramatically expanded in scope and severity, shifting from espionage on militaries and government infrastructure to direct cyberattacks against key civilian service industries, with the EU reporting that 38% of all 2025 cyberattacks targeted public administration. These increased disruptions of civilian life, along with the current geopolitical situation, link both conventional and cyber warfare, elevating the conflict beyond a traditional battlefield.

Definition of Key Terms

Advanced Persistent Threat (APT)

An APT is a form of sophisticated, sustained cyberattack, generally performed by nation-states or nation-state sponsored hacker groups. It involves an intruder maintaining a prolonged, undetected presence within a computer system or network (up to years) to steal sensitive or classified information and gain strategic advantages, primarily targeting governments, high value firms, or key industries. These attacks require a high degree of customization compared to other cyberattacks, and are tailored specifically against individual organizations, evading specific security measures and avoiding detection. Due to their highly specific nature, APTs often take long periods of time to develop, and are thus generally employed by well-funded, highly skilled groups of cybercriminals. APTs may also refer to well-established state-sponsored hacker groups.

Artificial Intelligence (AI)

Artificial Intelligence refers to a computer system that possesses the ability to perform tasks generally associated with human intelligence, such as reasoning, learning, problem-solving, and decision-making. In the context of cyberattacks and cyberwarfare, AI acts to decrease decision-making time, automate certain cyberattacks through autonomous vulnerability detection and exploitation. AI systems are further divided into certain subcategories, in which AI can be “generative” when it aims to create new content from an input prompt of outputting audio, text, or images, and “agentic” when it has some level of autonomy and focuses on achieving a set, defined goal, determining what steps are needed, selecting from possible actions, and working for a task over time.

Cyberspace

Unlike the internet, cyberspace is commonly defined as the online, virtual world created by the connections between various digital systems, such as computers, servers, routers, and certain Internet-enabled devices. The term is often described in terms of layers. This includes a physical layer, consisting of computer hardware and its location, serves as the base layer of the model and acts as the medium for data transfer. It also includes a logical layer of geographically separate systems operating upon the first layer, forming the platform-like nature of cyberspace (i.e., a website that exists on several servers, but is represented by a single URL). Lastly, a cyber-persona layer exists upon the logical layer, consisting of the actual people on the network, represented through data such as email or IP addresses, phone numbers, or digital accounts. As cyber-personas may represent a group of people, and as a single person may have multiple cyber-personas, attributing blame or responsibility to an individual in cyberspace is extremely difficult. It should be noted that there is no singular, fully internationally recognized definition of cyberspace.

Cyberwarfare

Cyberwarfare refers to the actions taken within cyberspace by a state or state-sponsored actor which aims to achieve strategic, military, or political objectives against another nation. Although not currently subject to International Humanitarian Law unless accompanied by physical armed conflict, these actions may still cause significant harm or damage, such as the disruption of vital computer systems or networks, and possibly leading to loss of human life. Such damage is comparable with the harm caused by physical strikes, with cyberwarfare potentially inducing a military response. Additionally, the term cyber conflict and cyberwarfare are different as cyber conflict may only include lower-level disruption or espionage.

Information and Communication Technologies (ICT)

An ICT refers to the tools, platforms, or websites used to facilitate and coordinate the exchange of information between individuals or groups of people. Due to their convenience, ICTs have become extremely widespread among governments, corporations, organizations, and individuals alike, transforming into a cornerstone of modern cyberspace. As a result, various individual governments have issued domestic laws and regulations regarding ICTs, covering a broad range of topics, such as 5G networks, standard encryption practices, and cybercrime response networks. These discrepancies result in difficulty when harmonizing regulations or definitions internationally, with conflicting standards and regulations challenging negotiation.

Quantum Computing

A quantum computer is an emergent type of computer that uses qubits (quantum bits) to perform calculations rather than traditional bits used in normal computers. Through unique qubits, quantum computers solve problems that would otherwise be nearly impossible for traditional computers to solve, such as those used in data encryption. Quantum computing effectively bypasses almost all commonly used forms of encryption, threatening global data security.

Current quantum computers pose little threat to cybersecurity, as they lack neither the necessary number of qubits nor a sufficiently low error rate to effectively run the algorithms needed to bypass current data encryption. Thus, while quantum-resistant cryptography (QRC) exists, it is not widely adopted by any nation on a large scale within government.

Background

Historical Roots

Modern cyberattacks and, by extension, cyberwarfare, began as simple, harmless programs created by individual programmers. The first computer worm (a self-replicating, self-propagating program), known as “Creeper”, was developed in 1971 by programmers Bob Thomas and Ray Tomlinson, which, whilst created with harmless intentions, would display a simple message on affected computers. This eventually evolved into modern computer viruses, malware, and cyberattacks.

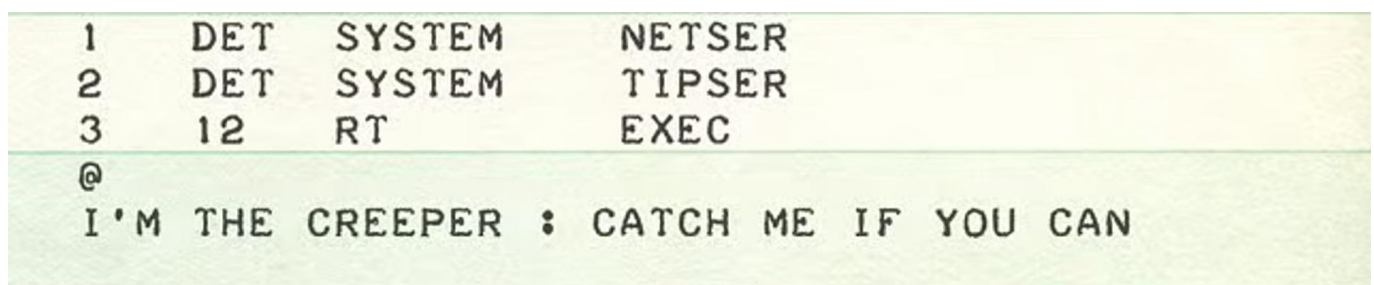


Figure 2: A photo illustrating the effects of the “Creeper” Worm (SentinelOne)

State-sponsored and politically motivated cyberattacks became a reality in 1986 when West German hackers gained access to around 400 military computers, including mainframes at the Pentagon, with the intention of selling military secrets to the KGB. Although unsuccessful, the attack represented the first publicly recorded instance of a major cyberattack against a government. However, due to the limited network size and rudimentary technology of the time, cyberattacks were limited in scale, and primarily focused on intelligence gathering. By the 1990s, with the introduction of the internet and easy to use, pre-written code, hacking became a widespread activity, often focusing on simple vandalism or destruction, rather than malicious cyberattacks, scams, or APTs that are often associated with hacker groups and state-sponsored cyberwarfare. This unintentionally promoted the growth of the anti-malware industry, with firewalls, intrusion detection systems, and advanced antivirus software being developed during this time, while businesses and governments alike began recognizing cybersecurity as a more serious matter.

This period also saw the rise of state-sponsored cyber activities, with technological development allowing for more advanced forms of cyberwarfare. For example, an APT cyberattack that targeted US universities and government systems, including the Pentagon, Department of Energy, and NASA, was discovered in 1998, and found to have been functional since 1996. Codenamed “Moonlight Maze”, the operation was widely considered

one of the first prolonged, state-sponsored cyberattacks. It successfully gained access to thousands of documents detailing maps of military installations, troop configurations, and military hardware designs. Investigators attributed the attack to Russia, though only limited evidence supported this claim.

Cyberwarfare gained further heightened within geopolitical events during the 2000s and 2010s, with advancing technology playing a major role in facilitating such cyberattacks. These issues were first highlighted through the “Titan Rain” cyberattack. The “Titan Rain” cyberattack was a large-scale, international cyberattack that began in 2003 and was publicly revealed in 2005. It was reported to have continued up to 2007. It triumphed in targeting US and UK government agencies, breaching the US’s Departments of Defense, Energy, State, and Homeland Security, while the UK’s Ministry of Defense, House of Commons (parliament), and Foreign Office were heavily affected. Additionally, major government-tied institutions such as Lockheed Martin and NASA were impacted by the cyberattack, which represented one of the most impactful cyberattacks to date. Both the UK and US attributed the attack to China, specifically PLA Unit 61398, claims which China has rejected.

The 2010s marked a change of emphasis for cyberattacks, transforming from espionage and intelligence gathering to physical damage, akin to kinetic strikes. This was best exemplified by the “Stuxnet” computer worm, developed in 2005 but revealed in 2009/2010. It was a joint US-Israeli operation which targeted Iran’s Natanz nuclear facility, causing 20% of all enrichment centrifuges to spin irregularly and burn out. Stuxnet not only marked the first cyberattack to cause lasting physical damage but was also the first to effectively bypass a digital air-gap system (a computer system removed from the outside world completely) using infected USB drives, a system previously thought to be digitally impenetrable. The worm infected over 200,000 computers, caused around 1,000 to physically degrade, and exploited four zero-day vulnerabilities (vulnerabilities in a computer system unknown to its developers), a scale unheard of at the time and still uncommon in the modern day. Whilst it is currently inoperational, Stuxnet’s method of operation and effects have been developed into other forms of computer worms and malware, such as Duqu and Flame.

The Current Situation

Through rapid technological development, cyberwarfare and cybersecurity have undergone significant advancements since their early inception. In 2018, around 61 countries had dedicated military cyber forces, many of which integrated cyber command units or multinational forces under international agreements and treaties, such as the North Atlantic Treaty Organization (NATO) or the Collective Security Treaty Organization (CSTO). This represents a major shift in military strategy, with cyberspace now being widely considered a fifth domain of warfare, alongside land, sea, air, and space.

Cybersecurity incidents have also increased in severity and volume in recent times, achieving effects previously only attainable by kinetic strikes and military force while being cheaper and more accessible. This is primarily illustrated through cyberattacks on critical infrastructure, particularly energy grids and power plants. In 2016, a cyberattack attributed to Russian APT “Sandworm” was launched on Kyiv, Ukraine, directly causing power outages amounting to 20% of the city’s power consumption at that time of night, affecting over 220,000 residents. This initiated a trend of cyberattacks on civilian infrastructure, with similar attacks being attempted on

Ukraine in 2022 and Poland in December 2025, the latter of which likely used a generative AI large language model (LLM) to assist in automation.

These events also show a correlation between the launching of cyberattacks and direct kinetic strikes, with cyberwarfare and physical operations becoming increasingly intertwined. The 2026 Iran War serves as a prime example of this tactic, with each Iranian strike on the UAE being accompanied by a cyberattack on the same target. Cyberattacks have also been used to overcome geographic distance, with Iran-linked cyberattacks retaliatorily affecting up to 30 US water systems and a UK-based power plant. Iran has also leveraged the opposite effect, using physical strikes to disrupt critical cyber infrastructure, through the targeting of nearby data centers in the UAE and Bahrain, likely damaging certain US or Israeli military capabilities and disturbing civilian life. While data centers have both civilian and military uses, they exist in an international legal grey area, as while strikes on dual use infrastructure are allowed under certain criteria, militaries cannot effectively assess whether such targets are being actively used by the enemy.

AI in Cyberwarfare

AI plays a rapidly evolving and important role in both cybersecurity and cyberwarfare, capable of compressing decision-making times, autonomous threat detection and analysis, and long-term, agentic coding. These properties make AI appealing in both cybersecurity and cyber-operations, with AI already receiving widespread usage across both fields. While few concrete statistics exist on AI in cybersecurity, analysts have pointed towards a steady trend of increasingly agentic AI cyberattacks, with agentic AI autonomously carrying out cyberattacks within defined parameters. Furthermore, generative AI can serve as a collaborator in the creation of cyberattacks through code writing and debugging, accelerating the process while maintaining human control.

These AI-powered cyberattacks have already been employed by various state-sponsored groups against governments across the world. One such example, instigated by a suspected Russian-linked group, used a version of Claude (a generative LLM trained by Anthropic) that had had its security features bypassed to automate a series of cyberattacks that primarily targeted Ukrainian and European governments. Claude was used to autonomously develop and edit malware, evading detection, and changing the code of malware to bypass cybersecurity measures. Additionally, current frontier models already pose significant risks to global cybersecurity and cyberspace, with models such as GPT-6 Astra achieving a 100% score on ExploitBench, which is a benchmark test designed to evaluate an AI's ability to detect and exploit known vulnerabilities in computer systems. Furthermore, groups of AI agents working together toward a common objective (referred to as swarms) can also allow for vast increases in cyber capabilities compared to individual agents, enabling fully autonomous cyberattacks.

Quantum Computing–Related Cybersecurity Threats

Quantum computing serves as one of the key future challenges for cybersecurity and data security on a global scale. A 2026 study found that around 51% of current internet domains/connections remain vulnerable to quantum attacks, while a survey of 32,011 internet domains found 0% use of QRC in digital certificates, effectively allowing a quantum computer to facilitate the impersonation of any individual on the internet.

Similarly, as mentioned in the “Definition of Key Terms” section, quantum computers primarily threaten current cybersecurity through HNDL strategies employed by nation-states and state-sponsored actors alike. HNDL is primarily threatening due to its passive nature, with no existing countermeasures outside of preventing data from being harvested in the first place. Therefore, few statistics exist on HNDL actors, outside of the recognition of such a threat by international governments, making it not only impossible to judge the severity of HNDL tactics but also highly difficult to regulate or appoint responsibility for HNDL actors.

Currently, the EU, China, the US, and the UK lead in quantum computing, with each country/bloc pledging billions on quantum computing in hopes of achieving a sufficiently powerful quantum computer to bypass traditional encryption – an accomplishment which would likely completely upend the balance of power in cyberspace and cyberwarfare. International efforts have also been introduced to mitigate the impact of quantum computers, with most of the above nations aiming to fully switch all systems to QRC by 2035.

Cybersecurity in Hybrid Warfare

Hybrid warfare is a form of conflict encompassing various non-traditional tactics, including covert means such as disinformation, economic coercion, deployment of paramilitary armed forces, cyberwarfare, and alternative military force, such as drone warfare. Hybrid warfare is best exemplified through the recent Russo-Ukrainian War, particularly following 2022, with Russia exerting pressure on Europe through the manipulation of energy markets, disinformation and propaganda campaigns, broad-reaching cyberattacks on various European countries, and reported election interference throughout the EU, and reported election interference throughout the EU. In another instance outside of the Russo-Ukrainian war, a reportedly Russia-backed cyberattack was detected in Norway, targeting a government agency, disrupting government services for three days while leaking details of the Norwegian state budget. These events highlight the rapid development of the issue, alongside the expansion of military force into newer domains.

Cyberspace acts as a critical aspect of such strategies, complementing major operations through synchronized cyber-kinetic strikes, disrupting enemy communications, or interfering with critical public infrastructure to expand the civilian impact of conflict, degrading public morale. Cyberwarfare also allows state actors to maintain plausible deniability, a key asset in navigating the grey area between peace and open conflict.

Major Parties Involved

Hacktivist Organizations

Hacktivism refers to the use of cyberattacks or computer hacking to pursue an ideological, political, or societal goal, primarily focusing on government or corporate targets. Hacktivism proves a critical aspect of geopolitics and cyberwarfare, with certain self-declared hacktivist organizations acting similarly to state-sponsored APTs or with actions taken by various nation-states, whilst claiming to be independent. In recent times, hacktivist activity has increased in both severity and frequency following geopolitical events such as the Russo-Ukrainian War (2022) and Israel-Palestine conflict (2023), expanding into cyberattacks on nation-states and critical infrastructure, blurring the line between hacktivism and state-sponsored cyberwarfare.

This has led to hacktivism playing a tangible role in global conflicts and live conflicts between states. In April 2026, a Ukraine-based hacktivist group, “BlackJack”, claimed to have carried out an attack against Moscollector, a Moscow-based company responsible for the construction and monitoring of underground water, sewage, and communications infrastructure. Believed to be affiliated to Ukrainian intelligence agencies, BlackJack, amongst other state-linked hacktivist groups, allow governments high degrees of plausible deniability in cyberwarfare and cyberattacks, allowing nations to act within cyberspace without fear of diplomatic or retaliatory backlash. This strategy is sometimes brought even further by other nations, with hacktivist organizations acting as fronts for government agencies.

People’s Republic of China

China acts as one of the largest employers of state-sponsored cyberattacks, with a survey of 60 verified APT attacks between 2024 and 2025 attributing 16 campaigns to China, or around 26.67%. These cyberattacks appear to focus globally upon long-term pre-positioning in various sectors, encompassing finance, energy, defense, and government agencies. Centering on zero-day exploits and living-off-the-land tactics (a fileless tactic using software already installed on target systems), these intrusions aim to minimize detection and notice, suggesting long-term exploitation and APT cyberattacks. This suggests a strategy of layered pressure and disruption during active warfare, resembling a cyberspace version of military buildup.

China also operates one of the world’s most extensive internal APT networks, with not only alleged government support, but also suspected participation and backing from various cybersecurity and technological firms. These firms could have provided certain hardware, intelligence, and cyber-related services to such state-sponsored actors. Extensive use of China’s strong domestic AI industry has also been reported. Such systems could explain how China-based APTs, such as Salt Typhoon, Volt Typhoon, Mustang Panda, and Flax Typhoon, have conducted large-scale, high-profile cyberattacks on a variety of targets. Institutions such as the US Army National Guard, the UK and New Zealand National Cyber Security Centres have reported compromise by such APTs, in total affecting over 80 countries in total. Currently, China does not officially recognize the existence of either Volt Typhoon or Salt Typhoon, and no comments have been made on other similar groups.

Russian Federation

Russia is another major player in cyberwarfare and state-sponsored cyberattacks, accounting for approximately 28.3% of cyberattacks globally, as seen from a sample of 60 cyberattacks – the largest share by any nation in the report. Russian cyberwarfare primarily acts against Ukraine and the EU, with around 47% of Russian-targeted systems being government affiliated. These attacks have also been increasingly focused on critical infrastructure, such as energy systems, suggesting activities associated with hybrid warfare. Russia has also exhibited strong alignment between cyberoperations and physical warfare, particularly in Ukraine, implying the expansion and coordination of conflict between various domains.

Russia has also effectively employed cyberattacks in conjunction with information warfare to spread disinformation and manipulate media, often on an unprecedented scale. In 2024, Russian influence allegedly played a role in the Romanian Presidential Election, with Russia utilizing cyberattacks and online disinformation to sway the result of the election. A similar case occurred in Moldova, where Russia used a combination of vote buying, cyberattacks on electoral commissions, and paid pro-Russian influencers to influence the result of the election.

United States of America

The US plays a large role in cybersecurity primarily through its particularly strong cybersecurity capabilities, as exemplified through its collaboration in the Stuxnet cyberattack and its strong domestic AI industry. Furthermore, the US has also been the primary target of multiple cyberattacks, such as the 2019 Russian-linked cyberattack on the SolarWinds – a piece of IT management software, which caused 18,000 customers to install updates containing malicious code which granted backdoor remote access to these hackers. This cyberattack was significant primarily due to SolarWinds' widespread use in the US Federal Government's computer systems, possibly allowing malicious actors to conduct espionage on confidential US systems.

The US also operates an extensive national cybersecurity or cyberwarfare department, with the US Cyber Command being among the most developed and complex governmental cyber-agencies globally. Whilst intrusions have extensively tested the defensive capabilities of the US's Cyber Command and Cyber Forces, its offensive capabilities remain to be seen. Furthermore, the US also serves as a major cybersecurity partner for multiple nations through international treaties, such as the NATO alliance and various bilateral alliances. The efficacy of these organizational alliances is also exacerbated by the inherent strength of the US's allies in cybersecurity, serving as a cyberspace force-amplifier through collaboration and intelligence-sharing.

Previous Attempts to Resolve the Issue

Open Ended Working Group (OEWG)

The OEWG was first founded in 2019 under UN General Assembly (UNGA) resolution A/RES/73/27, adopted in 2018, to develop and improve international cyberwarfare regulations, study threats to cyberspace, and build trust through discussion and clarification of international law. The OEWG operated by consensus, and was open to all UN member states, aiming to make negotiation processes more “democratic, inclusive, and transparent”. Although no outcomes of the OEWG were legally binding, it produced a Final Substantive Report on the topic, in which the OEWG affirmed that cyberspace is subject to international law, recognized the potentially destabilizing and far-reaching threats of state-sponsored cyberwarfare, and urged for greater global awareness on the topic as a whole.

The OEWG was further continued in 2021, under UNGA resolution A/RES/75/240, with a mandate up to 2025. This iteration of the OEWG primarily focused on the same issues as the previous OEWG, though it successfully implemented certain concrete steps towards addressing the issue. In its 2025 Final Report, the OEWG successfully introduced a single-track, permanent UN mechanism known as the “Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behavior in the use of ICTs”, or the Global Mechanism on ICTs – a subsidiary body of the UNGA First Committee (relating to disarmament affairs). It held its inaugural organizational session in March 2026 and will hold two meetings each year – one on general substantive issues, and one on capacity-building measures. Due to its recent nature and consensus-based conception, its effectiveness remains yet to be determined.

UN Group of Governmental Experts (GGE)

The UN GGE on cybersecurity was a UN process parallel to the OEWG, which produced substantive reports in 2010, 2013, and 2015. The GGE had a smaller membership than the OEWG, comprising experts from 25 countries, which aimed to provide legal and normative methods for the prevention and management of cyberwarfare. The 2010 report represented the first time experts agreed on the threat nature of cyberspace, while the 2013 report confirmed the extension of international law, particularly the UN Charter and International Humanitarian Law, to cyberspace, suggesting that no new treaty on cyberspace is needed. This was further clarified in the 2015 report, where a set of 11 non-binding, voluntary guiding principles on responsible state behavior in cyberspace were proposed, encompassing international support regarding cyberattacks on critical infrastructure, respect for human rights in cyberspace, and global cooperation regarding the safe use and development of cyberspace. These concepts were then solidified into UNGA Resolution A/RES/70/237, adopted by the GA in December 2015.

The GGE on cybersecurity, however, encountered several difficulties during its tenure. During the 2016-2017 sessions, the GGE was unable to reach a consensus, devolving into diplomatic “finger-pointing”. This resulted in both the American and Cuban delegations issuing public statements on why the negotiations had failed – in their view – a highly irregular action under standard diplomatic traditions. Cuba accused Western experts of

attempting to militarize cyberspace, while the US accused certain experts of backtracking on previous agreements, with arguments primarily emerging over the applicability of international law (particularly humanitarian law) in cyberspace. Furthermore, the GGE was disrupted by the COVID-19 pandemic, resulting in a prolonged period of diplomatic silence on the topic, during which the parallel OEWG functioned as the primary UN mechanism for cyberspace discussions.

Regional Efforts

Regional blocs, agreements, and supranational organizations also play a major role in cybersecurity regulation. Certain blocs, such as the EU or Association of Southeast Asian Nations (ASEAN) have already moved forwards, pushing regional agreements or legislation regarding state responsibilities and behavior in cyberspace. In the case of ASEAN, the 11 GGE guiding principles were adopted into a comprehensive checklist, with each norm divided into policy, operational, technical, legal, and diplomatic sections, providing practical actions towards the implementation of the GGE principles. Whilst non-mandatory in its nature, the checklist facilitated the development of various ASEAN member states' national cyber policies, such as Thailand's National Policy and Action Plan on Cybersecurity, which integrated aspects of the checklist.

The EU has also implemented regional legislation regarding national cybersecurity and cyberwarfare regulations through various initiatives, such as the 2022 Strategic Compass, which developed the Cyber Diplomacy Toolbox to strengthen EU cyber defense and resilience, monitored and raised awareness of foreign information manipulation and interference, and used Rapid Response Teams to better address then-emerging hybrid threats. The EU has also previously created a Cyber Defense Policy Framework (2018), which aimed to promote real-time cyber threat sharing between member states, enhance cooperation between civil and military sectors in cybersecurity, and foster research and technological advancement in cyberspace.

Possible Solutions

Legally Binding Treaties/Agreements on Cyberspace

One possible solution would be a set of legally binding international agreements or treaties that would act to define the boundaries of international law within cyberspace and introduce new norms or regulations as necessary. Such agreements could build on the previous work of the GGE and OEWGs on cyberwarfare or adapt regional regulations from relevant supranational organizations to better suit the international community. The agreements could also further consolidate methods for international dialogue on cyberwarfare, which could help facilitate the building of future norms or foster international collaboration on the safe development and use of relevant technology.

This agreement could help bridge the conflicting viewpoints on the topic and build upon global consensus – crucial for swift international action in the constantly evolving field. It could also serve as a beneficial platform for future regulations regarding cyberspace or relevant technologies, or act as a basis for new treaties/agreements

regarding recent or emergent technologies, helping to coordinate a unified international response. However, this agreement may face challenges during its implementation due to the divergent opinions of various opposing blocs and nations, which may complicate the finding of common ground.

International Enhancement of Cybersecurity Capabilities

Due to the rapid proliferation of APTs and state-sponsored cyberwarfare throughout the world, an internationally coordinated increase in cybersecurity capabilities could prove to be useful as a defense against hostile actors in cyberspace, such as by state-sponsored groups or well-equipped non-state actors, such as terrorist organizations. This coordinated development of cybersecurity capabilities could also aid less economically developed countries, or countries with less experience in cyberspace technologies, with their digital transition and technological development through technology-sharing programs or cooperation with further digitalized nations.

International collaboration and coordination would be vital to this solution to avoid false signaling of a rapid buildup in cyber-capabilities, which may lead to global mistrust and further competition between nations. This strategy would therefore need both widespread global cooperation and concrete international monitoring mechanisms, to prevent a downwards spiral into a “cyber race”. Definitive outcomes and actual, unambiguous steps could help with these issues, with internationally agreed upon, specific, and well-chosen targets on national cybersecurity capabilities being of critical importance towards the risk-free development of these capabilities, promoting common understanding and mutual trust.

Comprehensive International Dialogue and Collaboration on Cybersecurity

Comprehensive international dialogue and collaboration on cybersecurity could serve as an essential stepping stone towards the formation of global norms and regulations. This is due to the importance of finding common ground between significantly different global viewpoints, which acts as a foundational layer for further development and evolution, helping to build upon the previous momentum from the OEWGs and GGE. Such a comprehensive multilateral agreement would be crucial to fostering mutual trust and understanding, ensuring the equitable effect of regulations, and furthering global compliance and adherence to such rules. These dialogues could be held within the context of the UN, or through other relevant international organizations, which would act as neutral, mediatory bodies to facilitate conversation and constructive diplomacy.

Collaboration on cybersecurity between nations could also help reduce the prevalence of cyberattacks and cyberwarfare. Such collaboration could take place as technology-sharing in or regarding cyberspace, acting as a trust-building mechanism on cybersecurity. In such exercises, academia and experts in cybersecurity from civil society would play a major role, both possibly helping further technological development in cybersecurity, while ensuring common conformity to global regulations. Thus, multinational collaboration could not only bring tangible benefits towards global cyberspace development but could also promote mutual trust and further international confidence on international cybersecurity as a whole.

Bibliography

- ‘(4th Meeting) Plenary Session, Global Mechanism on ICTs in the Context of International Security (20-24 July)’. UN Transcripts, [object Object], <https://transcripts.un.org/en/asset/k14/k14hvbhuvvt>.
- Agentic AI on the Attack: How Human-AI Teaming Is Realigning Cyber Defense.
<https://www.infoguard.ch/en/blog/human-ai-teaming-against-ai-agents>. Accessed 14 Sept. 2026.
- ASEAN, et al. ‘ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace’. ASEAN, https://asean.org/wp-content/uploads/2025/02/ASEAN_checklist_print.pdf.
- Bajarūnas, Eitvydas. ‘The Hybrid Threat Imperative: Deterring Russia Before It Is Too Late’. CEPA, 2 Dec. 2025, <https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/>.
- 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*, vol. 6, no. 3, Sept. 2021, pp. 277–97. DOI.org (Crossref), <https://doi.org/10.1080/23738871.2021.1916976>.**
- Bussel, Jennifer. Cyberspace. Britannica, <https://www.britannica.com/topic/cyberspace>.
- Center, Cyber Defense. ‘Cyber Defense Center’. Cyber Defense Center, <https://cyberdefensecenter.org/fifth-domain-of-warfare>. Accessed 22 Sept. 2026.
- ‘China Hacks U.S. Wiretapped Systems in Bold Cyber Attack’. Hide.Me, <https://hide.me/en/blog/china-hacks-u-s-wiretapped-systems-in-bold-cyber-attack/>. Accessed 30 Sept. 2026.
- Computer Security Division, Information Technology Laboratory. ‘Post-Quantum Cryptography | CSRC | CSRC’. CSRC | NIST, 3 Jan. 2017, <https://csrc.nist.gov/projects/post-quantum-cryptography>.
- ‘Countering Hybrid Threats’. Countering Hybrid Threats, <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>. Accessed 28 Sept. 2026.
- Countering Misuse of AI: September 2026 / Anthropic. <https://www.anthropic.com/threat-intelligence-report-september-2026>. Accessed 25 Sept. 2026.

global-threat-report. Accessed 14 Sept. 2026.

paper/2021/06/cyber-capabilities-national-power/. Accessed 16 Oct. 2026.

Operations Tracker. <https://www.cfr.org/cyber-operations/>. Accessed 14 Sept. 2026.

Warfare?afd_azwaf_tok=eyJraWQiOiJBTQTFBOUFGMTM1QUU0NDI0RDgyN0I1M0MwOUYyR
DA4N0JCRTQxMjRENDE4MDNFMzY5NkYwMUUYwQjk2NUU4RTUzZlwiYWxnIjoilMyNTYifQ.
eyJhdWQiOiJjYXNlYm9vay5pY3JjLm9yZyIsImV4cCI6MTc4OTU1MjYyMCwiaWF0IjoxNzg5N
TUyNjEwLCJpc3MiOiJ0aWVyMS03Njk2NDQ4NTRiLTlya3diliwic3ViIjoilOTJhOmM1YmE6ZDF
mOjFlMjg6OmZmMDM6NWewMCIsImRhGEiOnsidHlwZSI6Imlzc3ViZCIsInJlZil6IjIwMjYwO
TE2VDA5NTY1MFotMTc2OTY0NDg1NGI5cmt3YmhDMVNKQ3g5aG4wMDAwMDAwNGQw
MDAwMDAwMDAxcHpjiWiYil6lk6ejFfTG8tdnh2RmZfNjJDRDNETXZRWRnZzBBX3llTEZs
dEp1WWlpckUiLCJoIjoilRVg2aHBQMmZxczI0VmleblpkMTV5djF6NHewQUstOEcxMUJnbElf
NUJCWSJ9fQ.jZCsWfWBXwg9iazQ7ty6OsDs_xOv0k0GfzkHxEqylGl1-
MErJastdnELliErGyGAwRTrUANmd0DkVNRlbFeky1Gc51l60YUv7nlH9V8WiyTVz2n3ajiZ9a
6ZJmrsvCGSEYr2AecPg9PnDljU_TmWSM1Ze_3olyvt9zCocNZE3v6r2gCBYnveh77KsyFfXFah
YfBbLrKCswRsTipHWBdkpv0qxzeoqXrgnxAlPIyb_CKKQzGs5PajaENtIIExHCH8VypnPdjCHF
6PeLOJZctPmPA381p1_x68JQK0y9-jqCC6ZCflPsLvltLsl95Vzi7RY-
AKltQt5plIZ2IkilyXg.WF3obl2IDtgqvMFRqVdYkd5s.

Warfare and Iran: Operation Economic Outcast.

<https://www.digitalassetredemption.com/blog/cyber-warfare-and-iran-operation-economic-outcast>. Accessed 15 Sept. 2026.

ncryption in 2026: Algorithms, Use Cases, and Challenges'. Venn,

<https://www.venn.com/learn/data-security/data-encryption/>. Accessed 27 Sept. 2026.

Regulation Platform. <https://digitalregulation.org>. Accessed 20 Sept. 2026.

ent Viewer. <https://docs.un.org/en/a/res/73/27>. Accessed 30 Sept. 2026.

TO TASK FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE. European Commission, June 2023, https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf.

- ‘Every Iranian Strike Came with a Cyberattack, UAE Cyber Chief Says’. Euronews, 17 Sept. 2026, <https://www.euronews.com/2026/09/17/every-iranian-strike-came-with-a-cyberattack-uae-cyber-chief-says>.
- ‘ExploitBench Leaderboard’. LLM Stats, LLM Stats, 9 June 2026, <https://llm-stats.com/benchmarks/exploitbench>.
- Fabiana, Da Pieve. ‘Roadmap for the Transition to Post-Quantum Cryptography’. https://www.enisa.europa.eu/sites/default/files/2026-04/NEW-Fabiana_Da_Pieve_EC-for-sharing.pdf.
- Faizan, Ahmad. ‘What Distinguishes Cyberspace, the Internet, and the World Wide Web?’ Electrical Academia, 4 Mar. 2019, <https://electricalacademia.com/tech-articles/distinguishes-cyberspace-internet-world-wide-web/>.
- Finio, Teaganne Finn, Amanda Downie, Matthew. Agentic AI vs. Generative AI | IBM. 11 Feb. 2025, <https://www.ibm.com/think/topics/agentic-ai-vs-generative-ai>.
- ‘Global Cybersecurity Index 2024’. International Telecommunication Union (ITU), 1 June 2024, <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>.
- How Salt Typhoon Breached the National Guard — and What It Means for U.S. Cybersecurity - Federal News Network. <https://federalnewsnetwork.com/cybersecurity/2025/07/how-salt-typhoon-breached-the-national-guard-and-what-it-means-for-u-s-cybersecurity/>. Accessed 30 Sept. 2026.
- Hunt, Katie. A Quantum Computing Deadline Looms. It Threatens to Kick off the Biggest Cybersecurity Crisis Ever. News Article. CNN, 17 May 2026, <https://edition.cnn.com/2026/05/17/science/quantum-computing-cybersecurity-q-day>.
- InfoGuard Threat Intelligence Report Q2/26: Europe’s Cyber Risk, Salt Typhoon & Iran’s Return. <https://www.infoguard.ch/en/blog/threat-intelligence-report-europes-cyber-risk-salt-typhoon-iran>. Accessed 14 Sept. 2026.
- ‘Iran’s Hidden Weapon Leaves US Exposed to Catastrophic Attack’. Newsweek, 28 Aug. 2026, <https://www.newsweek.com/iran-hidden-weapon-leaves-us-exposed-to-catastrophic-attack-12375428>.

- Joint Chiefs of Staff, Joint Publication 3-12 (R), Cyberspace Operations, February 3, 2013. Unclassified. | National Security Archive. <https://nsarchive.gwu.edu/document/21377-document-18>. Accessed 19 Sept. 2026.
- Kaiser, Chelsea. 'Cyber Warfare: State Attacks Up 45% By 2025'. Global Views World, 11 Aug. 2026, <https://globalviewsworld.com/cyber-warfare-45-rise-in-state-attacks-by-2025/>.
- Labs, Keepnet. 'History of Cybersecurity: From the 1940s to Today - Keepnet'. Keepnet Labs, 25 Jan. 2024, <https://keepnetlabs.com/blog/cybersecurity-breaches-lessons-from-history>.
- LaMontagne, Beth. 'The Quantum Computing Race Is on, but Who's in the Lead?' MIT Initiative on the Digital Economy, 20 May 2026, <https://ide.mit.edu/insights/the-quantum-computing-race/>.
- Lewis, James A. 'Computer Espionage, Titan Rain and China'. Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/051214_china_titan_rain.pdf.
- Mathew, Schaaf, and Rogan Andrew. A Lesson in Resilience: Moldova's Resistance to Election Interference. International Foundation for Electoral Systems, 17 Dec. 2025, <https://www.ifes.org/publications/lesson-resilience-moldovas-resistance-election-interference>.
- Moonlight Maze. ScienceDirect, <https://www.sciencedirect.com/topics/computer-science/moonlight-maze>.
- Moschetta, Giulia, et al. Global Cybersecurity Outlook 2026. World Economic Forum, Jan. 2026, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.
- O'Connor, James. 'Critical Infrastructure Under Siege: 2026 Cyber Warfare'. Informed Clearly, 26 July 2026, <https://informedclearly.com/en/geopolitics/59071/critical-infrastructure-cyber-warfare-2026>.
- OEWG 2019-2021 Final Substantive Report. Geneva Internet Platform DigWatch, Mar. 2021, <https://dig.watch/resource/oewg-2019-2021-final-substantive-report>.
- 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security Final Substantive Report'. 2021, <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>.

- ‘Post Quantum Government Initiatives by Country and Region’. Newsroom, <https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/>. Accessed 14 Sept. 2026.
- ‘Post-Quantum Cryptography Migration Framework’. Cyber Security Brunei, 1 July 2026, https://www.csb.gov.bn/sites/default/files/downloads/PQC/PQC_MIGRATION_FRAMEWORK.pdf.
- Raymond Andre Hagen. ‘The APT Paradox: Sophisticated Simplicity in Nation-State Cyber Operations (2024–2025), Trends, Detection Provenance, and Practical Gaps’. Norwegian University of Science and Technology, <https://papers.academic-conferences.org/index.php/iccws/article/download/4404/4056/16171>.
- Rehman, Mohib Ur. ‘15+ Leading Quantum Computing Countries in 2026’. The Quantum Insider, 26 Mar. 2026, <https://thequantuminsider.com/2026/03/26/leading-quantum-computing-countries/>.
- Reuters. Romanian Court Rules to Detain Pro-Russian Former Presidential Candidate Pending Fraud Probe. 29 Sept. 2026, <https://www.reuters.com/world/romanian-court-rules-detain-pro-russian-former-presidential-candidate-pending-2026-09-29/>.
- Ribeiro, Anna. ‘Chinese APTs Running Persistent Campaign Target Critical Infrastructure, Telecom Networks’. Industrial Cyber, 28 Aug. 2025, <https://industrialcyber.co/news/chinese-apt-s-running-persistent-campaign-target-critical-infrastructure-telecom-networks/>.
- . ‘Forescout Reports Rise of State-Sponsored Hacktivism, as Geopolitics Rewrites Cyber Threat Landscape’. Industrial Cyber, 30 Apr. 2025, <https://industrialcyber.co/news/forescout-reports-rise-of-state-sponsored-hacktivism-as-geopolitics-rewrites-cyber-threat-landscape/>.
- ‘Russia Expected to Intensify Hybrid War on Europe’. Dw.Com, <https://www.dw.com/en/russia-expected-to-intensify-hybrid-war-on-europe/a-79444596>. Accessed 28 Sept. 2026.
- ‘Russian Hybrid Warfare Activities in Europe: Considerations for Congress’. Congressional Research Service, 11 Aug. 2026, https://www.congress.gov/crs_external_products/R/PDF/R49134/R49134.1.pdf.
- S.A, Telewizja Polska. Pro-Russian Hackers Hit Norway with Series of Cyberattacks. <https://tvpworld.com/95154212/pro-russian-hackers-hit-norway-with-cyberattacks-over-ukraine-aid>. Accessed 28 Sept. 2026.
- SentinelOne. ‘History of Cybersecurity: Everything You Need to Know’. SentinelOne, 10 Feb. 2019, <https://www.sentinelone.com/blog/history-of-cyber-security/>.

Significant Cyber Incidents | Strategic Technologies Program | CSIS.

<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>. Accessed 13 Sept. 2026.

Smalley, Josh Schneider, Ian. What Is Quantum Computing? | IBM. 30 Dec. 2024, <https://www.ibm.com/think/topics/quantum-computing>.

Smeets, Max. 'The Challenges of Military Adaptation to the Cyber Domain: A Case Study of the Netherlands'. *Small Wars & Insurgencies*, vol. 34, no. 7, Oct. 2023, pp. 1343–62. DOI.org (Crossref), <https://doi.org/10.1080/09592318.2023.2233159>.

SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (Infographic), U.S. Government Accountability Office, 22 Apr. 2021, <https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic>.

Spencer, Patrick. 'Attackers Operate at Machine Speed — Defenders Still Run on Human Timelines'. Kiteworks, 1 Apr. 2026, <https://www.kiteworks.com/cybersecurity-risk-management/ai-speed-gap-cybersecurity-booz-allen-2026/>.

Spokesperson's Remarks on Report Revealing Truths of US Hying up of "Volt Typhoon" _Ministry of Foreign Affairs of the People's Republic of China. https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/jkxw_665234/202410/t20241015_11507722.html. Accessed 30 Sept. 2026.

'Stuxnet Definition & Explanation'. /, 13 Sept. 2017, <https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet>.

'Stuxnet Explained: The First Known Cyberweapon'. CSO Online, <https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html>. Accessed 21 Sept. 2026.

Tahir. '👤 Titan Rain: How Cybercriminals Hacked The United States Cyberspace'. Medium, 23 Dec. 2024, <https://medium.com/@tahirbalarabe2/%EF%B8%8F-titan-rain-how-cybercriminals-hacked-the-united-states-cyberspace-8add64ca512f>.

Team82. 'Unpacking the Blackjack Group's Fuxnet Malware'. Claroty, 12 Apr. 2024, <https://claroty.com/team82/research/unpacking-the-blackjack-groups-fuxnet-malware>.

The CyberThreat Report. Trellix Advanced Research Center, Apr. 2026, <https://www.trellix.com/advanced-research-center/threat-reports/april-2026/>.

‘The Hugging Face Incident and the Road Ahead’. OpenAI, 12 May 2026, <https://openai.com/index/hugging-face-incident-and-the-road-ahead/>.

The UN GGE on Cybersecurity: What Is the UN’s Role? | Council on Foreign Relations. 15 Apr. 2015, <https://www.cfr.org/articles/un-gge-cybersecurity-what-uns-role>.

Thornburgh, Nathan. ‘Inside the Chinese Hack Attack’. TIME, 25 Aug. 2005, <https://time.com/archive/6918871/inside-the-chinese-hack-attack/>.

Timeline for PQC Migration Revealed. 20 Mar. 2025, <https://www.ncsc.gov.uk/news/pqc-migration-roadmap-unveiled>.

Traynor, Orlaith. ‘Volt Typhoon 2026: Still Active in US Critical Infrastructure’. CybelAngel, 10 May 2026, <https://cybelangel.com/blog/volt-typhoon/>.

‘Ukraine Power Cut “Was Cyber-Attack”’. BBC News, 11 Jan. 2017. Technology. www.bbc.com, <https://www.bbc.com/news/technology-38573074>.

UN Global Mechanism on ICT Security. Geneva Internet Platform DigWatch, <https://dig.watch/processes/un-gge>.

University, © Stanford, et al. Stuxnet: The World’s First Cyber Weapon. 3 Feb. 2015, <https://cisac.fsi.stanford.edu/news/stuxnet>.

‘US And China Reportedly Prepare For High-Stakes AI Safety Dialogue As Cyber Threats Surge Globally’. Yahoo News, 4 Sept. 2026, <https://www.yahoo.com/news/politics/articles/us-china-reportedly-prepare-high-185818871.html>.

Vanishka, Mohan Dubey, and Varshney Gaurav. Measurement Study of Post-Quantum Readiness of Internet: 2026. 15 June 2026, arXiv, <https://arxiv.org/html/2606.16473v1>.

What Are Information Communication Technologies? Meaning, Definition. <https://www.unesco.org/en/query-list/i/information-communication-technologies>. Accessed 19 Sept. 2026.

‘What Is an Advanced Persistent Threat (APT)? | CrowdStrike’. CrowdStrike.Com, <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/>. Accessed 16 Sept. 2026.

‘What Is Hacktivism? Meaning, Types, and More’. Fortinet,

<https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism>. Accessed 29 Sept. 2026.

‘What Is Q-Day? Quantum Computing and Cyber Risk’. Palo Alto Networks,

<https://www.paloaltonetworks.com/cyberpedia/what-is-q-day>. Accessed 17 Sept. 2026.

What Is Stuxnet? Trellix, <https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/>.

Zetter Details How Stuxnet Marked a Turning Point in Cyberwarfare by Enabling Physical Sabotage through Code. Industrial Cyber, 23 July 2025, <https://industrialcyber.co/industrial-cyber-attacks/zetter-details-how-stuxnet-marked-a-turning-point-in-cyberwarfare-by-enabling-physical-sabotage-through-code/>.