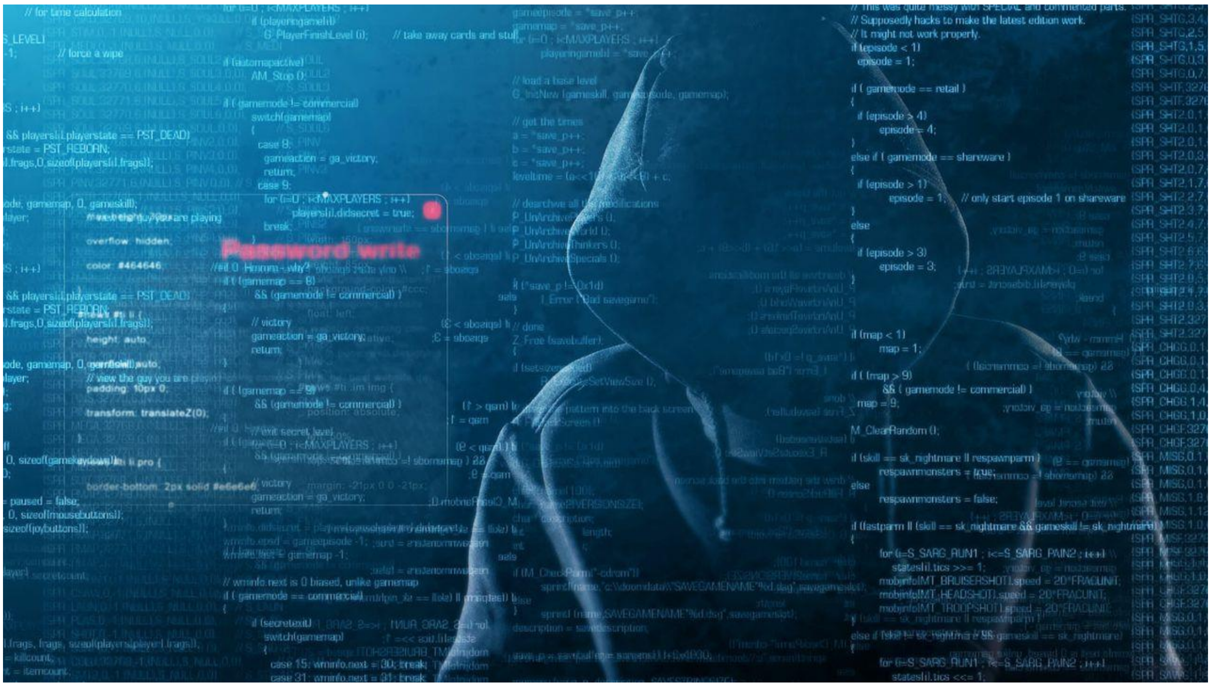
General Assembly 1

Addressing the progressive militarization and weaponisation in cyber conflicts



German International School
of The Hague
Model United Nations

Luisa Fiedler

Forum: General Assembly 1

Issue: Addressing the progressive militarization and weaponisation in cyber conflicts

Student Officer: Luisa Fiedler

Position: President of the General Assembly

Introduction

In an era where digital technology influences nearly every aspect of modern life, cyberspace has become both an asset and a battleground. Originally designed for communication and economic growth, it has evolved into a domain of strategic competition, security threats, and geopolitical tensions. As nations expand their cyber capabilities, the militarization and weaponization of cyberspace have emerged as major global concerns. Unlike traditional warfare, cyber operations transcend borders, occur in real time, and often lack clear attribution, making conflicts harder to regulate and escalating risks for global stability. This General Assembly session will explore these challenges, examining the risks posed by cyber conflicts and potential pathways for international cooperation.

Definition of Key Terms

Advanced Persistent Threat (APT)

A sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures and fly under the radar.

Critical Infrastructure

Systems and assets, whether physical or virtual, so vital to a country that their incapacitation or destruction would have a debilitating effect on national security, economic security, public health, or safety.

Cyber Attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Cyber Deterrence

Strategies and actions taken to discourage cyber-attacks by increasing the perceived costs and risks associated with such attacks for potential adversaries.

Cyber Espionage	The use of digital techniques to obtain secrets and confidential information without the permission of the holder of the information, typically for military, political, or economic advantage.
Cyber Norms	Shared expectations of appropriate behaviour in cyberspace, often developed through international dialogue and agreements to promote stability and reduce the risk of conflict.
Cyber Resilience	The ability of an organization or system to prepare for, respond to, and recover from cyber-attacks and incidents while continuing to operate effectively.
Cyber Sovereignty	The concept that states have the right to govern and control the digital infrastructure and activities within their borders, often used to justify national control over internet content and access.
Cyber Warfare	Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.
Cyberspace	An amorphous, supposedly “virtual” world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet’s infrastructure. As opposed to the Internet itself, however, cyberspace is the place produced by these links.
Distributed Denial of Service (DDoS) Attack	An attempt to make an online service unavailable by overwhelming it with traffic from multiple sources, often using a network of compromised computers (botnet).
Information Warfare	The use of information and communication technologies to gain an advantage over an adversary, which may include the dissemination of propaganda, the manipulation of information, or the disruption of enemy command and control systems.
Internet of Things (IoT):	The network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data, potentially creating new vulnerabilities for cyber-attacks.
Militarisation in Cyberspace	The process of integrating cyber capabilities into military doctrine, strategy, and operations. This includes establishing dedicated cyber units within armed forces, developing cyber-

specific tactics, and incorporating cyber elements into broader military planning and exercises.

Petya

Petya malware is a family of encrypting malware that was first discovered in 2016. The malware targets Microsoft-based systems, infecting the master boot record to execute a payload that encrypts a hard drive file’s system table and prevents Windows from Booting. It subsequently demands that the users make a payment in Bitcoin in order to regain access to the system.

Weaponisation in Cyberspace

The development, deployment, and use of tools, techniques, or malware designed to cause damage, disruption, or unauthorized access through cyber means. This can include viruses, worms, trojans, and more sophisticated tools like zero-day exploits.

Zero-Day Exploit

A zero-day exploit is a cyberattack vector that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware. "Zero day" refers to the fact that the software or device vendor has zero days to fix the flaw because malicious actors can already use it to access vulnerable systems.

General Overview

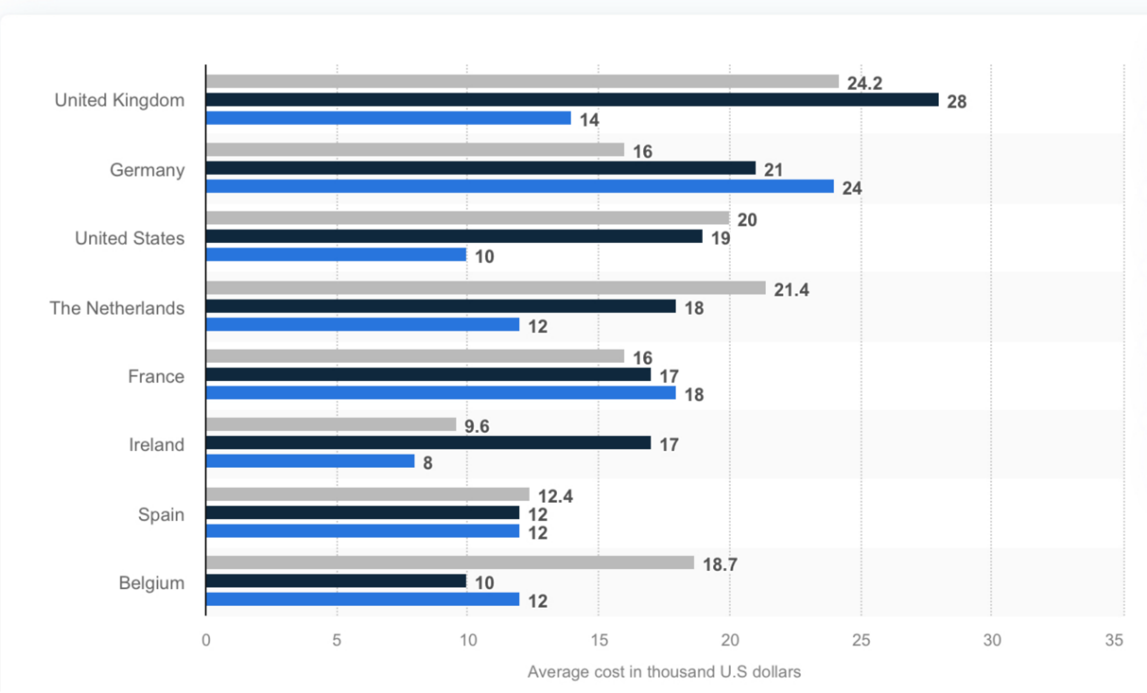
The militarization and weaponization of cyberspace have become defining aspects of modern security challenges. As digital infrastructure continues to shape economies, governance, and communication, cyberspace has transformed into a critical domain for both national security and geopolitical competition. Unlike conventional warfare, cyber conflicts can be carried out remotely, across borders, and often without clear attribution, making them difficult to regulate and counteract effectively. The rapid evolution of cyber warfare has brought new risks, particularly as state and non-state actors leverage cyber capabilities for espionage, sabotage, and disruption.

Cyber warfare has developed over time, from early forms of information warfare and network-centric military strategies to sophisticated cyber operations that directly target critical infrastructure and state institutions. Historically, military interest in cyber capabilities grew alongside advancements in digital technology. The 1990s and early 2000s saw the emergence of cyber intelligence gathering and communication disruptions as strategic tools. However, by the early 2010s, offensive cyber capabilities had become more advanced, with incidents like the Stuxnet attack on Iranian nuclear facilities demonstrating the potential for cyber operations to cause real-world damage. As cyber threats became more prominent, many nations began integrating cyber warfare into their military doctrines, expanding offensive and defensive capabilities within their armed forces.

The militarization of cyberspace refers to the systematic incorporation of cyber tools and strategies into military operations. Governments worldwide have established specialized cyber commands and units dedicated to both defensive security and offensive operations. Countries such as the United States, China, and Russia have developed extensive cyber capabilities, often using them to gain strategic advantages. The increasing reliance on cyber operations within military frameworks raises concerns about escalation, retaliation, and the potential for cyber conflicts to spill over into conventional warfare. The blurring of the lines between cyber espionage, cybercrime, and acts of war complicates international responses, as cyber operations often take place in a legal grey zone.

The weaponization of cyberspace is another critical issue, as cyber tools are increasingly used to disrupt or manipulate systems. Cyberattacks have targeted national power grids, financial institutions, election systems, and healthcare networks, illustrating their potential for large-scale disruption. Attacks such as the Not Petya malware and disruptions to Ukraine's power grid highlight the growing threats posed by cyber warfare. The rise of ransomware and other malicious cyber operations further emphasizes the vulnerabilities of digital infrastructure. With the expansion of the Internet of Things (IoT), artificial intelligence, and cloud computing, cyberattacks are expected to become even more sophisticated, making it essential to develop stronger cyber defences.

Average costs of all cyber attacks in the United States and Europe from 2021-2023, by country:

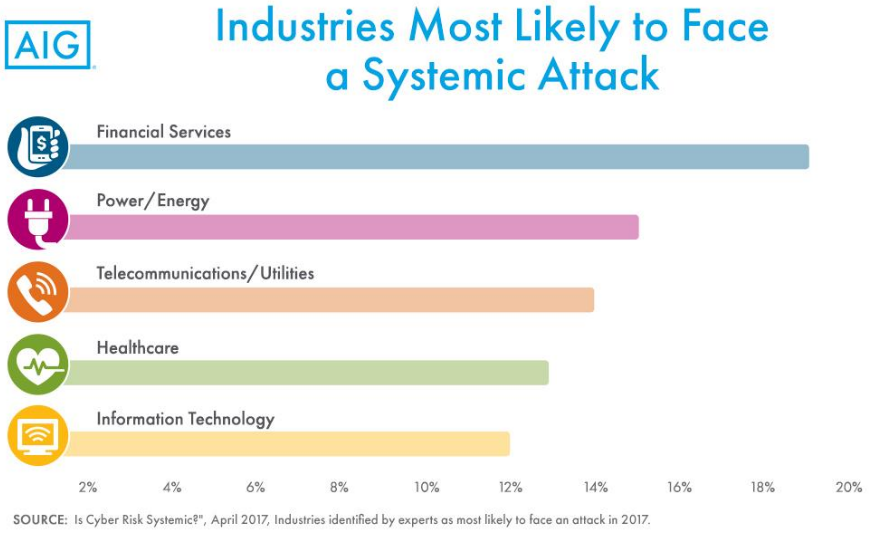


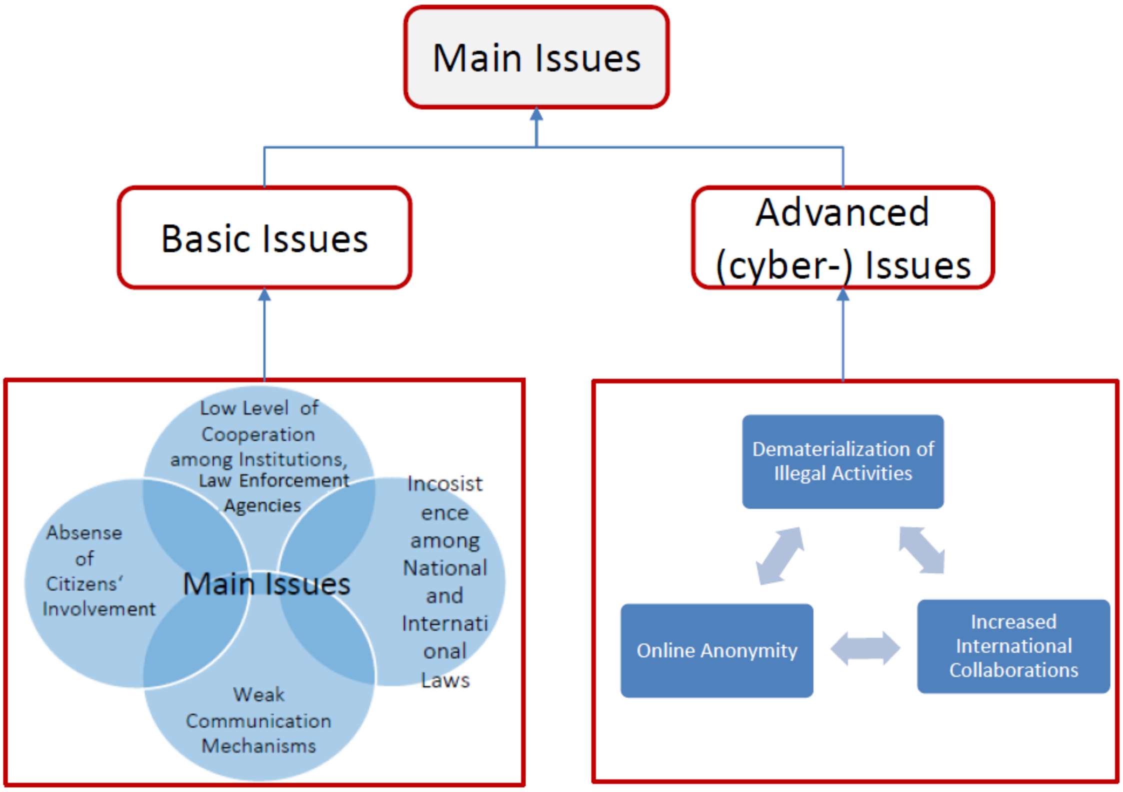
Despite the growing risks, the legal and international frameworks regulating cyber conflicts remain limited. Unlike conventional warfare, which is governed by established international laws, cyber warfare lacks clear regulations and accountability mechanisms. Efforts such as the UN Group of Governmental Experts (GGE) and the Tallinn Manual have sought to establish guidelines, but enforcement remains a challenge. While certain international agreements address cybercrime and espionage, they do not fully cover military cyber operations. As a result, cyber conflicts continue to escalate without clear deterrence strategies or defined consequences.

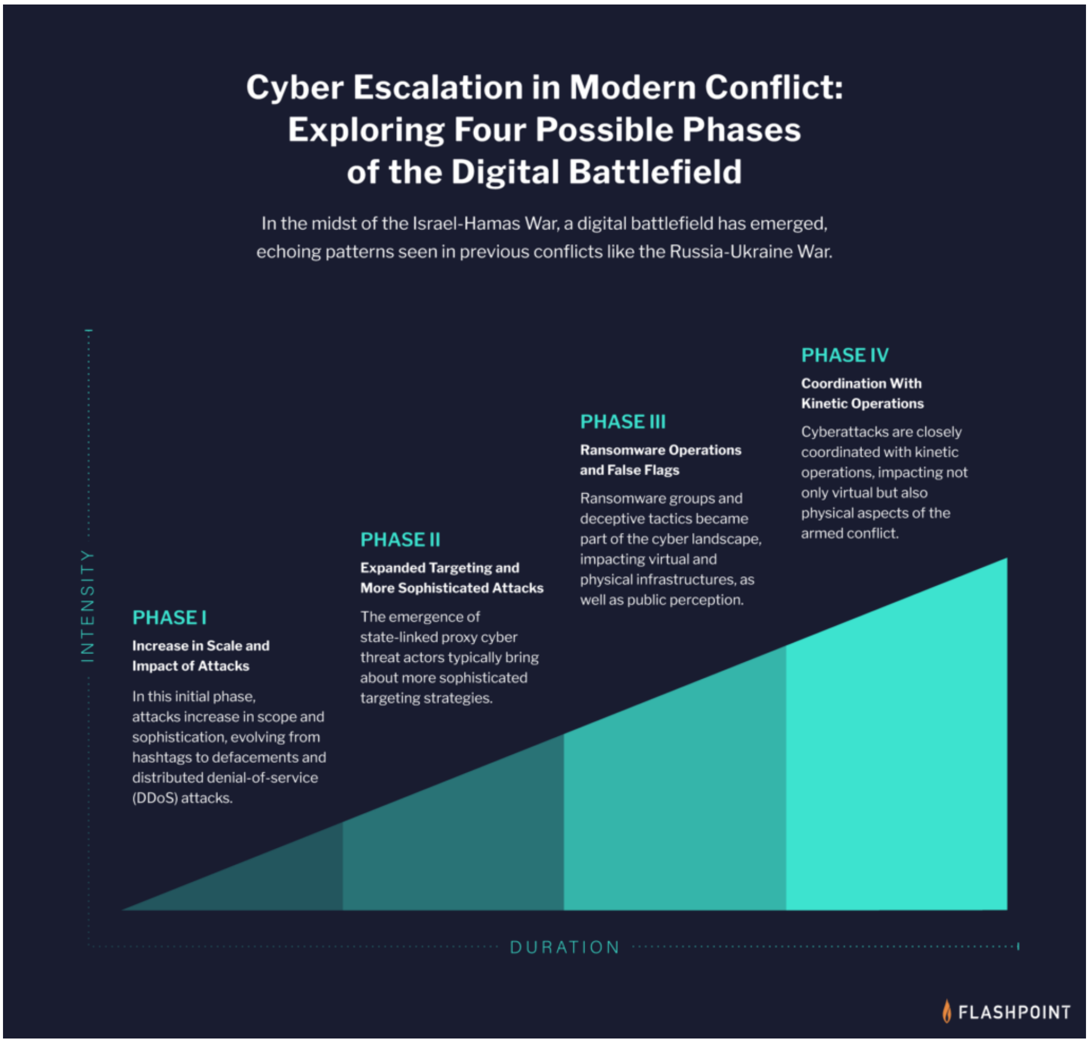
As cyber warfare evolves, various methods have emerged, including cyber espionage, cyber sabotage, and informational warfare. Cyber espionage is commonly used for intelligence gathering, allowing state and non-state actors to access sensitive data without direct confrontation. Cyber sabotage, on the other hand, targets infrastructure and digital systems, with the goal of causing disruption or destruction. Propaganda and information warfare have also become significant tools, as cyber operations are frequently used to manipulate public perception and influence political events. Denial-of-service attacks and ransomware campaigns further illustrate how cyber tools are used for both strategic and financial gain.

As the international community struggles to address these challenges, cyber conflicts continue to pose serious risks to global stability. Without clear regulations, effective deterrence, and enhanced cooperation, the escalation of cyber warfare could have severe consequences for international security. While some efforts have been made to promote responsible state behaviour in cyberspace, there is still a need for comprehensive strategies to prevent the unchecked militarization of the digital domain. The future of cyber warfare will likely be shaped by emerging technologies, geopolitical rivalries, and the ongoing struggle to balance national security interests with global stability.

Here are a couple more infographics that might help you understand the impact of cyber conflicts:




Main Issues
Basic Issues
Advanced (cyber-) Issues
Low Level of Cooperation among Institutions, Law Enforcement Agencies
Absense of Citizens' Involvement
Main Issues
Incosistence among National and International Laws
Weak Communication Mechanisms
Dematerialization of Illegal Activities
Online Anonymity
Increased International Collaborations



Cyber Escalation in Modern Conflict: Exploring Four Possible Phases of the Digital Battlefield

In the midst of the Israel-Hamas War, a digital battlefield has emerged, echoing patterns seen in previous conflicts like the Russia-Ukraine War.

PHASE I

Increase in Scale and Impact of Attacks

In this initial phase, attacks increase in scope and sophistication, evolving from hashtags to defacements and distributed denial-of-service (DDoS) attacks.

PHASE II

Expanded Targeting and More Sophisticated Attacks

The emergence of state-linked proxy cyber threat actors typically bring about more sophisticated targeting strategies.

PHASE III

Ransomware Operations and False Flags

Ransomware groups and deceptive tactics became part of the cyber landscape, impacting virtual and physical infrastructures, as well as public perception.

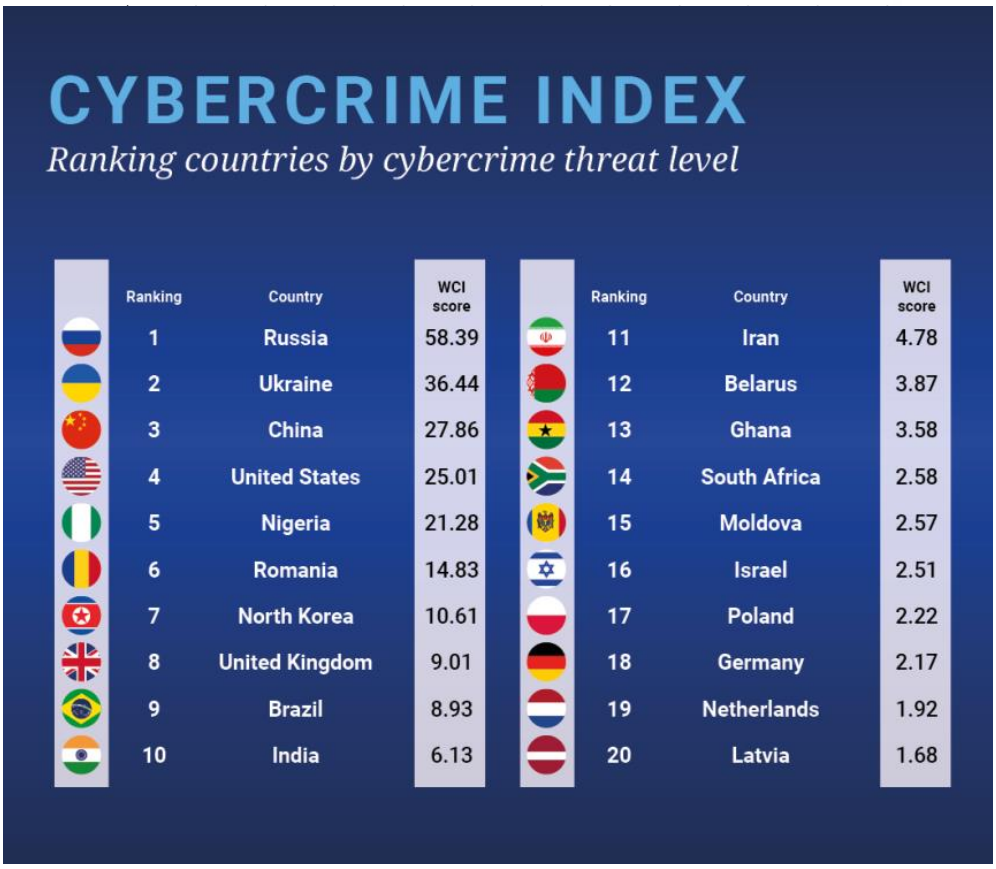
PHASE IV

Coordination With Kinetic Operations

Cyberattacks are closely coordinated with kinetic operations, impacting not only virtual but also physical aspects of the armed conflict.

Major Parties Involved

Countries with the highest number of initiated cyber incidents with political dimension from 2000-2024:



CYBERCRIME INDEX

Ranking countries by cybercrime threat level

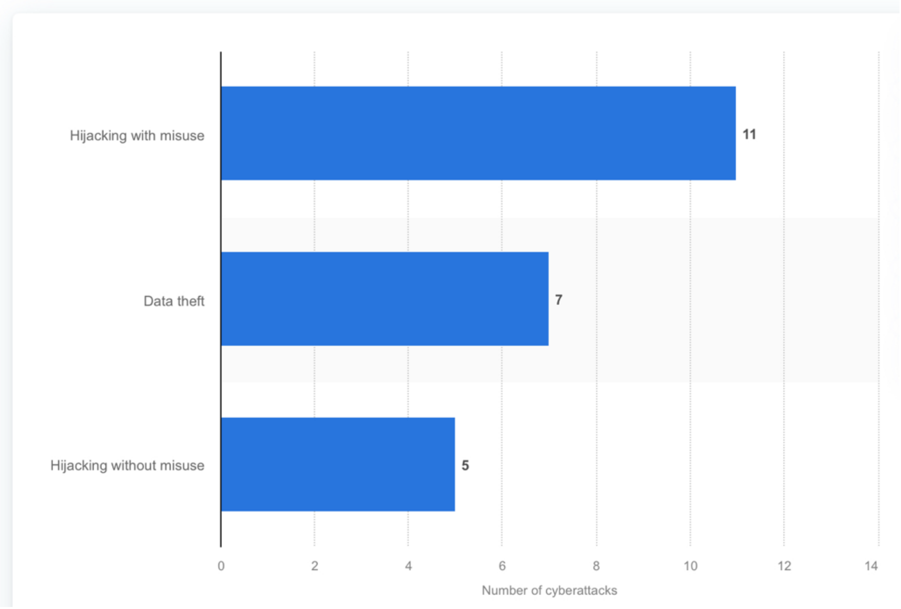
Ranking	Country	WCI score
1	Russia	58.39
2	Ukraine	36.44
3	China	27.86
4	United States	25.01
5	Nigeria	21.28
6	Romania	14.83
7	North Korea	10.61
8	United Kingdom	9.01
9	Brazil	8.93
10	India	6.13
11	Iran	4.78
12	Belarus	3.87
13	Ghana	3.58
14	South Africa	2.58
15	Moldova	2.57
16	Israel	2.51
17	Poland	2.22
18	Germany	2.17
19	Netherlands	1.92
20	Latvia	1.68

The World’s first Cybercrime Index

“Figuring out why some countries are cybercrime hotspots, and others aren’t, is the next stage of the research. There are existing theories about why some countries have become hubs of cybercriminal activity – for example, that a technically skilled workforce with few employment opportunities may turn to illicit activity to make ends meet [...]” - Dr. Miranda Bruce, Department of Sociology, University of Oxford and UNSW Canberra.

China views cyber capabilities as an essential part of its national defence strategy and as a tool for economic and political power. The Chinese government is generally resistant to international regulation on cyber activities, arguing that state sovereignty should be respected in cyberspace. China emphasizes the need for non-interference in domestic affairs and believes that cyber operations, including espionage and cyberattacks, are legitimate means of safeguarding national security. China also advocates for the development of its own set of international norms in cyberspace, focusing on mutual respect and non-aggression, while opposing foreign interference in its cyber policies.

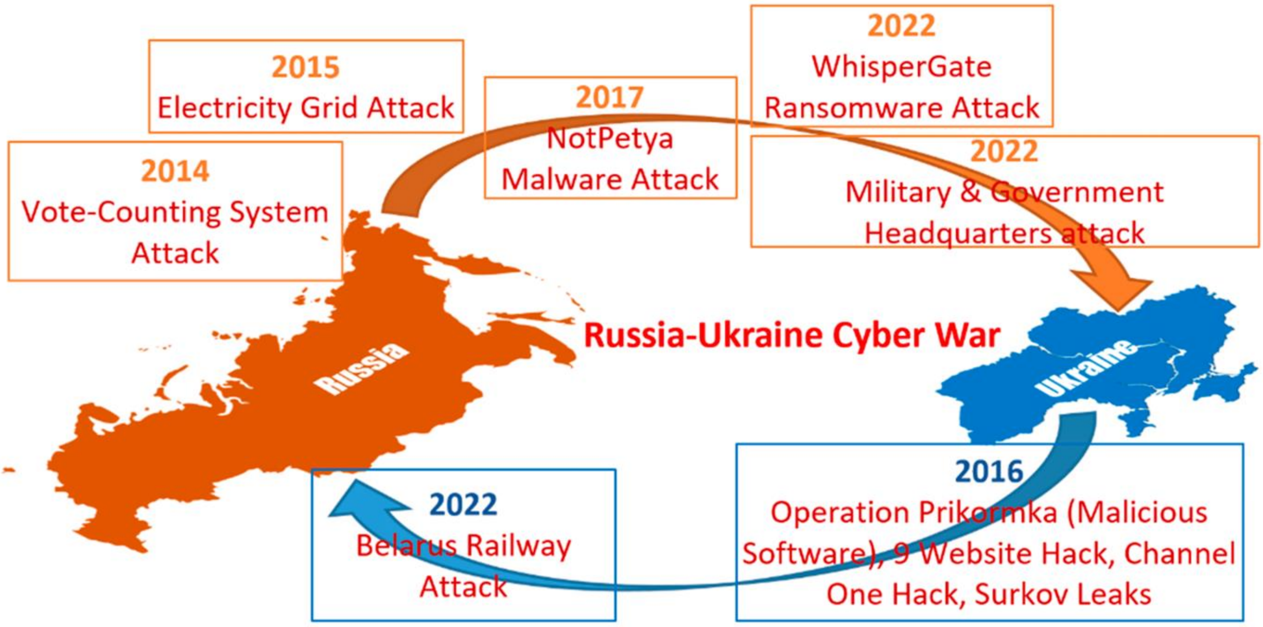
Main types of cyber incidents with a political dimension launched by China in 2024



Russia just like China, strongly defends its sovereignty in cyberspace and argues against external regulation or restrictions on cyber activities. Russian officials often frame cyber capabilities as a necessary tool for national security, citing the role of cyber operations in modern warfare and intelligence gathering. Russia's perspective emphasizes deterrence, using cyber weapons as a means of signalling power in international relations. The Russian government is wary of international frameworks that might limit its freedom of action in cyberspace, particularly in the context of potential military conflict. Russia also advocates for the creation of a new international cyber order that reflects the interests and security concerns of sovereign states.

It is also important to know about the Russia-Ukraine cyberwar. The Russia-Ukraine cyber war is a prolonged series of cyberattacks, primarily conducted by Russian state-sponsored actors against Ukraine, beginning as early as 2014 and intensifying alongside military conflicts. Russia has used cyber operations as part of its hybrid warfare strategy, targeting Ukraine's critical infrastructure, government agencies, and media to destabilize the country, spread disinformation, and disrupt military and civilian operations.

Key cyber incidents include the 2015 and 2016 power grid attacks, which left thousands without electricity, and the Not Petya attack in 2017, which initially targeted Ukrainian systems but spread globally, causing billions in damages. Since Russia's full-scale invasion in 2022, cyberattacks have escalated, with Russian hackers launching DDoS attacks, deploying wiper malware, and attempting to disrupt Ukrainian military communications and critical services. In response, Ukraine has bolstered its cyber defences with assistance from Western allies and private sector firms, engaging in cyber countermeasures against Russian assets. The conflict highlights the growing role of cyber warfare in modern military strategy and the challenge of defending against state-sponsored cyber threats.


2015
Electricity Grid Attack
2014
Vote-Counting System Attack
2017
NotPetya Malware Attack
2022
WhisperGate Ransomware Attack
2022
Military & Government Headquarters attack
Russia-Ukraine Cyber War
Russia
Ukraine
2022
Belarus Railway Attack
2016
Operation Prikormka (Malicious Software), 9 Website Hack, Channel One Hack, Surkov Leaks

Iran: views cyber capabilities as a critical tool for both national defense and asserting influence in the region. The Iranian government has developed significant cyber capabilities, often citing the need to protect itself from foreign threats and cyberattacks, particularly from Western powers. Iran has been accused of engaging in cyber operations aimed at both state actors and private sectors, including attacks on critical infrastructure. While Iran is open to discussions on cyber norms, it remains cautious about international frameworks that could limit its ability to defend itself or retaliate in cyberspace. Iran advocates for a multilateral approach to cybersecurity, emphasizing the importance of sovereignty in cyberspace and the need for non-interference in domestic cyber affairs.

United States: is a major proponent of international norms that regulate cyber conflicts. It advocates for the application of existing international laws, such as the United Nations Charter, to cyberspace, arguing that the same rules governing traditional warfare should apply to cyber warfare. The U.S. supports the development of a global framework that enhances transparency, accountability, and the protection of critical infrastructure from cyberattacks. While the U.S. has its own cyber capabilities, it promotes dialogue and cooperation to prevent cyber escalation and the use of cyber weapons that could cause widespread harm to civilian populations. The U.S. emphasizes the importance of deterrence and the need for clear consequences for malicious cyber activities.

European Union: recognizes the growing threat posed by cyber militarization and weaponization and calls for international agreements that establish norms and rules to regulate state behaviour in cyberspace. The EU advocates for strengthening cyber resilience, particularly for critical infrastructure, and for increased cooperation between member states and external partners in combating cyber threats. While the EU supports initiatives that promote the peaceful use of cyberspace, it faces internal divisions regarding the level of regulation needed and the potential impact of cyber policies on national sovereignty. The EU pushes for greater multilateral cooperation to ensure a stable and secure global cyberspace while balancing the need for security with the protection of individual rights.

United Nations (UN): seeks to address the militarization of cyberspace through its Group of Governmental Experts (GGE) and other initiatives. The UN's position emphasizes the application of international law, including the UN Charter, to cyber conflicts, calling for the prevention of cyber warfare that targets civilian infrastructure or violates human rights. The UN advocates for the establishment of norms to guide state behaviour in cyberspace, with a particular focus on the principle of non-interference and respect for sovereignty. While the UN encourages multilateral cooperation, it faces challenges in reconciling the differing interests of member states, especially regarding issues of cyber governance and control.

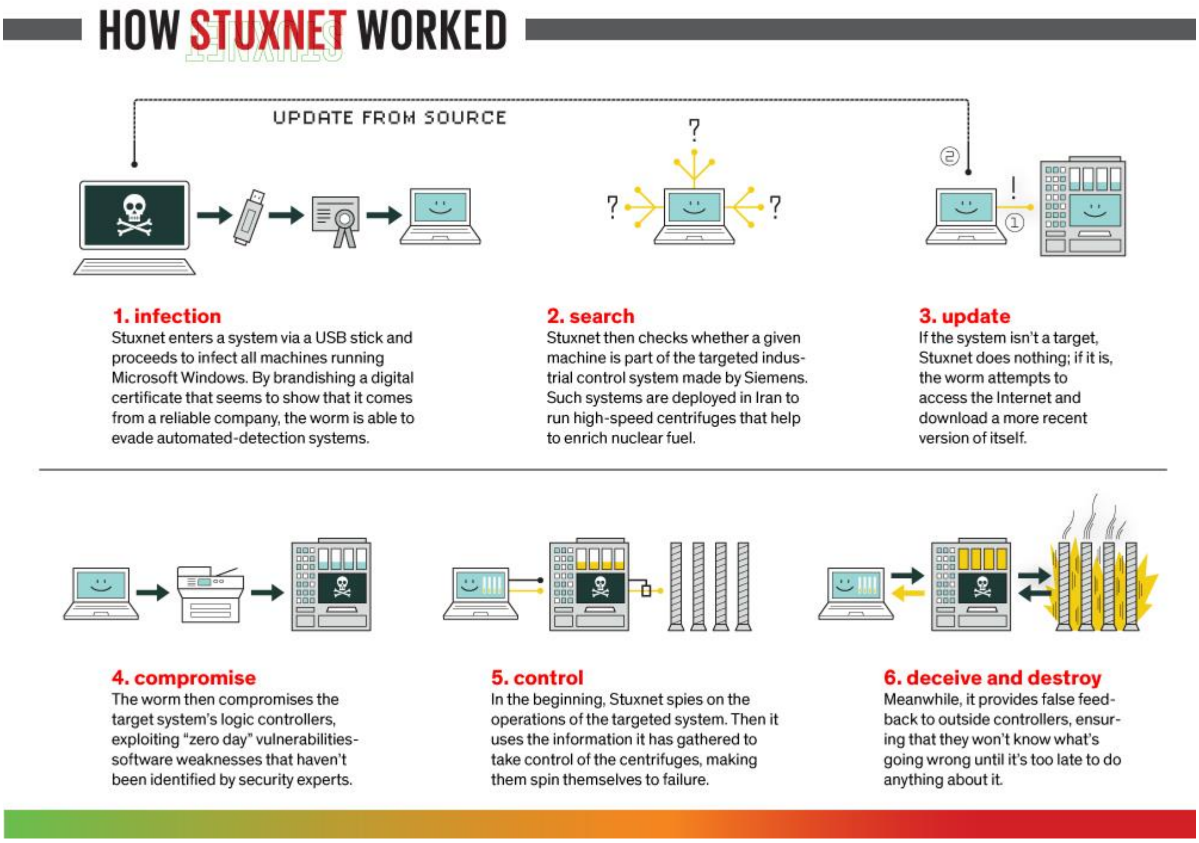
Private Sector (Tech Companies and Cybersecurity Firms): play a critical role in the debate over cyber militarization. These private entities stress the importance of protecting global networks from cyber threats and call for greater transparency, accountability, and collaboration between governments and the private sector. They argue that clear frameworks and regulations are necessary to prevent the use of cyber weapons that could undermine global economic stability and individual privacy. The private sector also emphasizes the need for enhanced cybersecurity resilience, including the protection of infrastructure, businesses, and individuals from potential cyberattacks, and advocates for the development of international standards to safeguard the digital economy.

Civil Society (Human Rights Organizations): are concerned about the impact of cyber warfare on individuals and society. They advocate for strong international treaties and ethical guidelines to prevent the weaponization of cyberspace from violating human rights, particularly in areas such as privacy, data protection, and freedom of expression. These organizations emphasize the importance of accountability and transparency in state cyber activities and argue for protecting civilians from the collateral damage of cyber conflicts. They stress the need for clear rules that prohibit cyber operations that harm non-combatants or destabilize society, urging global cooperation to ensure that the use of cyber weapons remains in line with international humanitarian law.

Timeline of Events

2007 - *Cyberattacks on Estonia:* In April 2007, Russia-based attackers launched a serial of denial-of-service attacks against Estonian public and private sector organizations in response to the governments removal of a Soviet war monument from downtown Tallinn. For three weeks, threat actors targeted state and commercial websites, ranging from foreign and defence ministries to banks and media outlets, by overloading their bandwidth and flooding their servers with junk traffic, rendering them inaccessible to the public, Estonia then briefly closed ist digital borders and blocked all international web traffic. This was the first time that a foreign actor threatened another nation’s security and political independence primarily through cyber operations.

2010 - *Stuxnet Worm:* Stuxnet is a highly sophisticated computer worm that became widely known in 2010. It exploited previously unknown Windows zero-day vulnerabilities to infect target systems and spread to other systems. Stuxnet was mainly targeted at the centrifuges of Iran’s uranium enrichment facilities, with the intention of covertly derailing Iran’s then-emerging nuclear program. However, Stuxnet was modified over time to enable it to target other infrastructure such as gas pipes, power plants, and water treatment plants.
Whilst Stuxnet made global headlines in 2010, it’s believed that development on it began in 2005. It is considered the world’s first cyber weapon and for that reason, generated significant media attention. Reportedly, the worm destroyed almost one-fifth of Iran’s nuclear centrifuges, infected over 200,000 computers, and caused 1,000 machines to physically degrade.



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn’t a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system’s logic controllers, exploiting “zero day” vulnerabilities-software weaknesses that haven’t been identified by security experts.

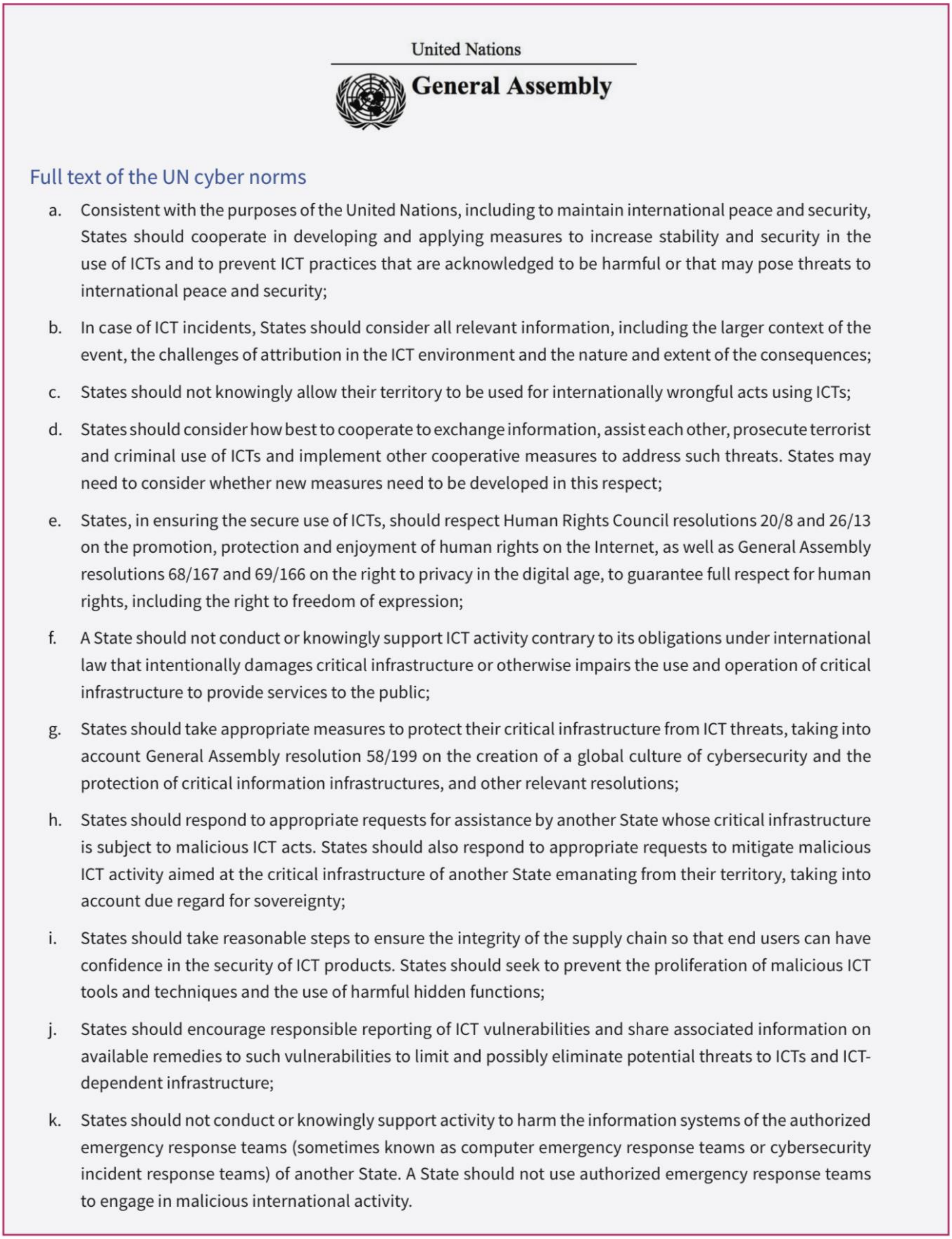
5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won’t know what’s going wrong until it’s too late to do anything about it.

2013 - *U.S. and China Cybersecurity Agreement*: In 2013, after years of escalating tensions over cyber espionage, the United States and China reached a landmark agreement to curb cyberattacks targeting private sector companies. This was one of the first international efforts to address cyber espionage at a state level, though it did not address broader concerns around cyber warfare and weaponization.

2013 - *The Tallinn Manuals*: The Tallinn Manual has long been the flagship research initiative of the CCDOE. The original Tallinn Manual published in 2013 by Cambridge University Press addressed the most severe cyber operations- those that violate the prohibition of the use of force, entitle states to exercise their right of self-defence, or occur during armed conflicts. The Tallinn Manual 2.0, published in 2017, built on that work by considering the rules of international law governing cyber incidents that states encounter on a day-to-day basis, but which falls below the thresholds of the use of force or armed conflict.

2015 - *The United Nations Group of Governmental Experts (GGE) Report*: The UN GGE released a report in 2015, recommending the application of international law to cyberspace, including the UN Charter. The report urged states to refrain from using cyberattacks that would harm civilian infrastructure and emphasized the importance of establishing norms for state behaviour in cyberspace, marking a significant step toward formalizing global cybersecurity standards.



United Nations

General Assembly

Full text of the UN cyber norms

a. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

b. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

d. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

e. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

f. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

g. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

h. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

i. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

j. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

k. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

2017 - *NotPetya Cyberattack:* A series of powerful cyber-attacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms. Similar infections were reported in Germany, France, Italy, Poland, Russia, the UK, the USA and Australia. 80% for all infections were however in Ukraine. It was later reported that experts agreed that Petya was masquerading as ransomware, while it was actually designed to cause maximum damage, with Ukraine being the main target.

Petya malware is a family of encrypting malware that was first discovered in 2016. The malware targets Microsoft-based systems, infecting the master boot record to execute a payload that encrypts a hard drive file's system table and prevents Windows from Booting. It subsequently demands that the users make a payment in Bitcoin in order to regain access to the system.

2018 - *U.S. National Cyber Strategy:* In 2018, the United States released its National Cyber Strategy, emphasizing the development of offensive cyber capabilities to deter and respond to cyberattacks. The strategy highlighted the U.S.'s commitment to using cyber operations as part of its broader defence and national security strategy, reinforcing the militarization of cyberspace.

2020 - *SolarWinds Cyberattack:* The SolarWinds cyberattack, discovered in late 2020, involved a sophisticated hacking campaign believed to be carried out by Russian state-sponsored actors. The attack compromised several U.S. government agencies and private companies, raising concerns about the vulnerability of national security systems to cyber espionage and demonstrating the increasing scale and complexity of state-led cyber operations.

2021 - *EU Cybersecurity Act:* In 2021, the European Union adopted the Cybersecurity Act, which aimed to strengthen the EU's cybersecurity resilience, improve the protection of critical infrastructure, and enhance coordination among member states. This was a significant move toward developing a more unified approach to countering cyber threats in Europe, as part of broader efforts to regulate and protect cyberspace.

Previous attempts to solve the issue

There have been several significant attempts to address the militarization and weaponization of cyberspace, but each has faced challenges.

The Tallinn Manual (2009-2013): The Tallinn Manual, developed by a group of international law experts and under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence, is one of the most notable attempts to apply existing international law to cyber warfare. The manual proposed that the laws of armed conflict, including the prohibition of attacks on civilians and the principles of proportionality and necessity, should apply to cyber operations. However, it was not universally accepted as binding law, as some countries, especially non-NATO members like Russia and China, questioned its applicability. Furthermore, its focus on applying traditional laws to a rapidly evolving domain like cyberspace led to concerns that existing frameworks might not adequately address new cyber tactics, such as espionage and sabotage, making it a partial and incomplete solution.

The UN Group of Governmental Experts (GGE) Reports (2010-2017): The United Nations Group of Governmental Experts (GGE) has attempted to create norms and principles for the responsible use of cyberspace. Its 2013 and 2015 reports recommended applying international law to cyberspace, including the UN Charter, and called for norms to prevent the targeting of critical infrastructure. However, while the reports have garnered broad international support, they have not resulted in binding agreements or significant actions. Disagreements between member states, especially between those with different views on cyber sovereignty (such as the U.S. versus Russia and China), have hindered the development of stronger, enforceable norms. For example, Russia and China prefer more state control over cyberspace and resist global regulatory frameworks that might limit their ability to use cyber tools for national defense.

The 2015 U.S.-China Cybersecurity Agreement: During the state visit on September 24-25, 2015, President XI Jinping of China and President Barack Obama reached a cyber agreement. In principle, the USA and China agreed, among other things to

-provide timely responses to requests for information and assistance concerning malicious cyber activities,

-refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property,

-pursue efforts to further identify and promote appropriate norms of state behaviour in cyberspace within the international community

-establish a high-level joint dialogue mechanism on fighting cybercrime and related issues

The European Union's Cybersecurity Act (2019-2021): The European Union adopted the Cybersecurity Act in 2021 to create a more secure and resilient cyber environment by setting up a cybersecurity certification framework for digital products and services and establishing the European Cybersecurity Agency (ENISA) as a central authority. While the Act has bolstered cybersecurity in the EU, its focus on protecting critical infrastructure and certification schemes does not address the militarization of cyberspace directly. The law is also challenged by the need for coordination between EU member states, which have varying levels of cybersecurity capabilities and different national interests. As a result, enforcement of consistent standards across the region remains an issue.

The Paris Call for Trust and Security in Cyberspace (2018): In 2018, over 70 countries, as well as numerous companies and organizations, endorsed the Paris Call, which seeks to promote norms for a secure and stable cyberspace, including the prevention of cyberattacks against critical infrastructure and support for the protection of human rights. While it garnered broad support, the Paris Call is non-binding and lacks strong enforcement mechanisms. Additionally, some major cyber powers, including the U.S. and Russia, did not sign the agreement, limiting its effectiveness as a global solution to the weaponization of cyberspace.

The Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. (2018-Present): The U.S. established the Cybersecurity and Infrastructure Security Agency (CISA) in 2018 to defend the nation's critical infrastructure against cyberattacks, including those of a military nature. While CISA has made significant strides in improving national cyber defences, its role is primarily focused on securing the U.S. rather than addressing the global challenges of militarization and weaponization. Moreover, the absence of a global cyber treaty or cooperative framework leaves countries vulnerable to state-sponsored cyberattacks and complicates efforts to prevent the weaponization of cyberspace.

Attempts at Bilateral Agreements (e.g., U.S.-Russia Cybersecurity Dialogues): Bilateral dialogues between countries like the U.S. and Russia have also attempted to establish cybersecurity norms and prevent cyber conflict. However, these talks often stall due to distrust, conflicting priorities, and a lack of transparency. Russia, for example, has consistently rejected proposals for international treaties that would limit its cyber capabilities, viewing such measures as infringements on its sovereignty and security.

Possible Solutions

A potential solution is the creation of a legally binding international treaty specifically aimed at regulating state behaviour in cyberspace. This treaty could outline clear norms for the responsible use of cyber capabilities, with a focus on protecting critical infrastructure, preventing cyberattacks against civilians, and ensuring accountability for malicious cyber operations. By establishing enforceable penalties for violations, this treaty would help mitigate the risks of cyber warfare and create a more predictable international environment for state actors.

Cyber Confidence-Building Measures (CBMs) could be expanded to reduce the likelihood of conflict and misunderstanding between states in cyberspace. These measures could include transparency in military cyber capabilities, prior notification of large-scale cyber operations, and mechanisms for the peaceful resolution of cyber incidents. Confidence-building measures would help increase trust between nations, reducing the chances of accidental escalation and promoting international cooperation on cybersecurity.

A dedicated, global organization, similar to the International Atomic Energy Agency (IAEA) for nuclear weapons, could be established to monitor and regulate cyber activities. This organization could promote international norms, monitor compliance, and mediate disputes between states. It would facilitate dialogue on the responsible use of cyberspace, assist in developing shared standards for cyber defence, and help states build capacity for defending against cyber threats while preventing the escalation of cyber conflicts.

Bibliography

https://www.statista.com/statistics/1428563/countries-launched-highest-number-of-cyberattacks-political/
https://www.statista.com/statistics/1428527/china-launched-political-cyberattacks-types/
https://www.statista.com/statistics/1327147/median-cost-attacks-in-cyber-security-united-states-europe/
https://www.mdpi.com/2078-2489/14/9/485
https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level
https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf
https://en.wikipedia.org/wiki/Petya_(malware_family)
https://www.cfr.org/cyber-operations/estonian-denial-service-incident#:~:text=In%20April%202007%2C%20Russia%2Dbased,war%20monument%20from%20downtown%20Tallinn.
https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet
https://sgp.fas.org/crs/row/IN10376.pdf
https://www.businesswire.com/news/home/20170510005781/en/AIG-Study-Systemic-Cyber-Attacks-Likely-in-2017-Financial-Services-PowerEnergy-International-Cyber-Conflicts-Key-Concerns
https://www.britannica.com/topic/cyberspace

https://www.rand.org/topics/cyber-warfare.html

https://csrc.nist.gov/glossary/term/cyber_attack

https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/

https://www.ibm.com/think/topics/zero-day

https://www.neit.edu/blog/what-is-a-cyber-war-explained#:~:text=The%20history%20of%20cyber%20warfare%20goes%20back%20to%20the%201980s,digital%20warfare%20and%20espionage%20increased.

https://dictionary.cambridge.org/dictionary/english/cyberspace

https://www.statista.com