UN Reforms in the 21st Century: Bridging the Gap Between Cyber Threats and Global Governance

Kruti Hudka, Harshil Khokhar & Prasann Barot

Abstract

The rapid growth of network technology in the 21st century introduces various new challenges for global governance especially when it comes to cybersecurity. Cybersecurity has been a major concern for United Nation and other international organisations which leads to the demand for the reforms in United Nation regulations. United Nation's rigid framework inspired by Western philosophy and Anglo-Saxon ideology of national interest and non-interference faces hinderance in collaboration at global level. The dynamic nature of growth in Cybersecurity makes it more difficult for United Nation to shift its rigid laws to flexible ones. The increasing intersection between international cooperation, national sovereignty and human rights within cyberspace calls for reforms in international framework according to the nature of cybersecurity. This paper finds the gap in today's international framework while suggesting the idea of international co-operation to avoid cyberattacks with better future dynamics of cybersecurity and digital space.

Keywords: Cybersecurity, Global Governance, UN Regulations Reforms, International Cooperation, National Sovereignty, Digital Space, Anglo-Saxon Ideology

Introduction

1. Background on Network Technology in the 21st Century

The advancement of Internet technology in the 21st century has transformed the way people are connected globally and information is shared, forming the backbone of modern prosperity (Ronchi, 2020). Economic innovation in terms of economic growth is supported by telecommunications and energy projects, while biological factors influence natural ecosystems (UNIDIR & Kavanagh, 2017). However, this complexity has brought to light inefficiencies that need to be reformed through policy (Tikk et al., 2010). Network technology has transformed strategies in military systems through the tools of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems (Buckland, Schreier, & Winkler, n.d.). It enhances the efficiency of operations and situational awareness. Though Network Centric Warfare has provided the benefits of improved coordination, challenges of complexity and interoperability continue to exist (Mason, 2021). The performance and reliability of a network architecture depend on the topology models applied, including client-server and cloud-based systems (Humayun et al., 2020). As reliance on the Internet increases, robust security measures are called for, using firewalls, encryption, and multi-factor authentication in order to establish trust (Johnson et al., 2016). Overall, the integration of technology in the civilian and military spheres underlines its importance today (Li & Liu, 2021).

2. Cybersecurity as a Global Governance Challenge

Global Internet governance has transcended state control, incorporating diverse actors like governments, civil society, academia, international bodies, and private entities to tackle issues like cybersecurity and privacy through collaboration and dialogue (UNODC et al., 2013). This decentralised approach is particularly vital in cybersecurity, evolving through varying stages with regional and local actors (ITU et al., 2021).

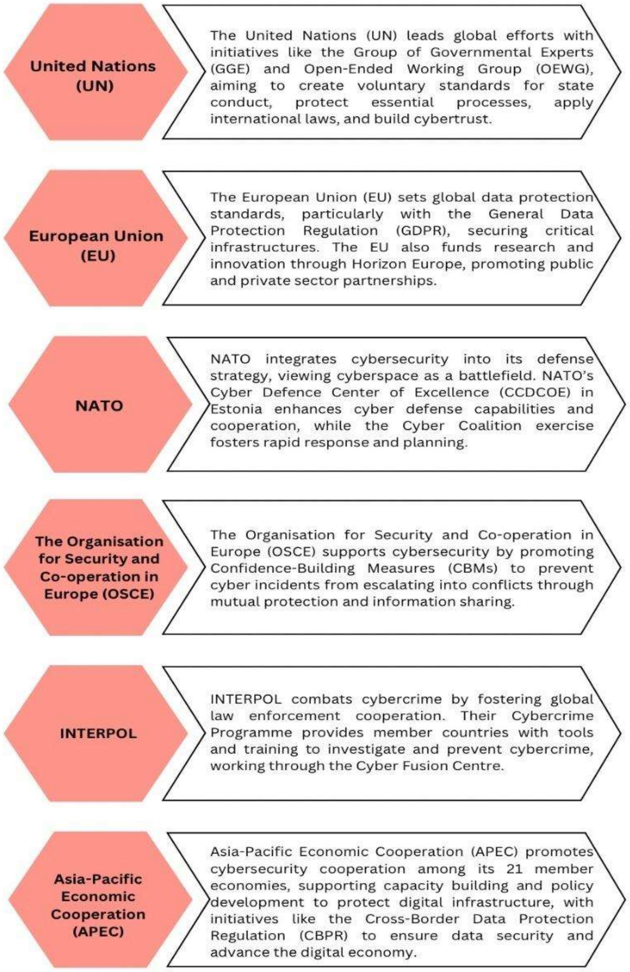
The evolution of digital governance started with the International Telecommunication Union (ITU), which originally dealt with telecommunications and pioneered internet governance (ITU et al., 2021). It eventually transitioned to the Internet Corporation for Assigned Names and Numbers (ICANN), which took on oversight for domain names and other crucial elements of the internet (UNIDIR & Kavanagh, 2017). The U.S. government had significant influence during the formative years of ICANN, but its creation marked a crossroad toward a more multinational governance system and emphasized the need for international collaboration, especially in the digital context (Nye et al., 2014).

Based on existing initiatives, the World Summit on the Information Society (WSIS) in 2003 urged the creation of a more diverse governance structure that includes various stakeholders and promoted integrative policy efforts (ITU et al., 2021). The Working Group on Internet Governance (WGIG) later proposed the multistakeholder model to balance governmental policy influence with civil society and private sector expertise (UNIDIR & Kavanagh, 2017). While these efforts represent significant strides, gaps remain—particularly in cybersecurity governance, which lacks centralized oversight (Li & Liu, 2021). China and Russia advocate for cyber-sovereignty, asserting that states should have full control over digital activities within their borders (Ronchi, 2020), while the U.S. supports a multi-actor model that emphasizes open internet access, privacy, transparency, and democratic freedoms (Baham, 2020). This ideological divide between sovereignty and open governance creates persistent conflicts in efforts to regulate cyberspace globally (Tran Dai et al., 2017).

Therefore, effective global cybersecurity governance requires flexible and collaborative frameworks that balance international cooperation, state sovereignty, and individual human rights. Establishing resilient, transparent, open, secure, and inclusive policies for cyberspace is essential (UNODC et al., 2013).

3. Role of International Organisations in Cybersecurity

International organizations establish themselves in international relations with the intent of strengthening cyber resilience by creating laws, fostering collaboration, and developing technical skills. The frameworks advanced by the United Nations (UN), International Telecommunication Union (ITU), and the Organisation for Economic Co-operation and Development (OECD) are responsible for guiding and encouraging both state and non-state actors to demonstrate responsible conduct in cyberspace (ITU et al., 2021; UNIDIR & Kavanagh, 2017).



United Nations (UN)

The United Nations (UN) leads global efforts with initiatives like the Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG), aiming to create voluntary standards for state conduct, protect essential processes, apply international laws, and build cybertrust.

European Union (EU)

The European Union (EU) sets global data protection standards, particularly with the General Data Protection Regulation (GDPR), securing critical infrastructures. The EU also funds research and innovation through Horizon Europe, promoting public and private sector partnerships.

NATO

NATO integrates cybersecurity into its defense strategy, viewing cyberspace as a battlefield. NATO's Cyber Defence Center of Excellence (CCDCOE) in Estonia enhances cyber defense capabilities and cooperation, while the Cyber Coalition exercise fosters rapid response and planning.

The Organisation for Security and Co-operation in Europe (OSCE)

The Organisation for Security and Co-operation in Europe (OSCE) supports cybersecurity by promoting Confidence-Building Measures (CBMs) to prevent cyber incidents from escalating into conflicts through mutual protection and information sharing.

INTERPOL

INTERPOL combats cybercrime by fostering global law enforcement cooperation. Their Cybercrime Programme provides member countries with tools and training to investigate and prevent cybercrime, working through the Cyber Fusion Centre.

Asia-Pacific Economic Cooperation (APEC)

Asia-Pacific Economic Cooperation (APEC) promotes cybersecurity cooperation among its 21 member economies, supporting capacity building and policy development to protect digital infrastructure, with initiatives like the Cross-Border Data Protection Regulation (CBPR) to ensure data security and advance the digital economy.

Figure 1: Role of International Organisations

Threats emerging from the use of the internet are international in nature, and therefore, organizations like the G7, G20, and Association of Southeast Asian Nations (ASEAN) are crucial for fostering dialogue and building trust toward the harmonization of cybersecurity policies (Tran Dai et al., 2017). Capacity-building programs by the World Bank, INTERPOL, and the Global Forum on Cyber Expertise help developing countries strengthen their cyber defenses and address threats that could impact global security (ITU et al., 2021). Cybersecurity necessitates collaboration from industry, civil society, and international bodies like the ITU, especially under multi-stakeholder strategies such as those employed by the Internet Governance Forum (UNODC et al., 2013). Additionally, the EUROPOL Cybercrime Centre coordinates responses among countries to serious cybercrime incidents (CSIS, 2024). However, persistent challenges remain, such as conflicting state interests and the rapid pace of technological advancement (Li & Liu, 2021).

4. Objectives and Scope of the Study

Cyber threats, which include cyberattacks and information warfare, pose an evolving challenge for international governance and raise questions about the UN framework's ability to address them effectively (UNODC et al., 2013). This study examines the intersection between state governance, international cooperation, and human rights in cyberspace, highlighting the need for flexible and efficient policies that can adapt to the rapidly changing digital landscape (UNIDIR & Kavanagh, 2017). It also assesses existing UN laws and frameworks, analyzing their strengths and weaknesses in dealing with cybersecurity challenges (Tikk et al., 2010). Additionally, the paper advocates for the establishment of open, secure, inclusive, adaptive, and resilient policies that would be effective in enforcing cybersecurity regulations and countering evolving cyber threats (Li & Liu, 2021).

Conceptual Framework: Cyber Threats, Global Governance, and Human Rights

2.1 Defining Cyber Threats: Scope and Types

With the massive use of cyberspace for business activities, banking, shopping, and communication, there has been a corresponding increase in cybercriminal activities. This trend is largely due to the high dependency on web applications, which are often rife with design flaws that criminals exploit for unauthorized access. As a result, cybersecurity has become a critical concern for researchers and professionals (NIST, 2016).

Cybersecurity is defined as the prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems (NIST, 2016).

Rosenau (1992) defines global governance as "a system without any centralized authority but able to enforce decision at the global level."

Human rights are defined as rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, and the right to work and education, among others. Everyone is entitled to these rights without discrimination (UN, 2013).

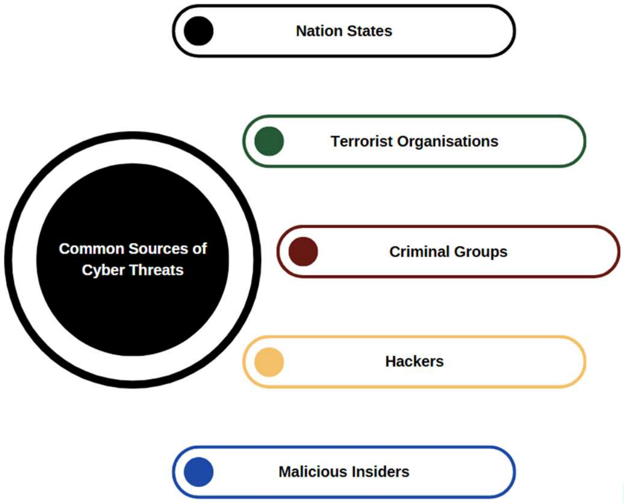


Figure 2: Common Sources of Cyber Threats

Nation States

Nation-state actors like China, Russia, North Korea, and Iran utilize Advanced Persistent Threat (APT) groups for espionage, economic disruption, and political interference. These actors are responsible for some of the most damaging cyberattacks, with costs exceeding $1.6 million per incident (CSIS, 2024). Over 90% of organizations have faced or suspect they will face nation-state-backed cyberattacks (Masas, 2023).

Terrorist Organisations

Terrorist groups aim to destroy critical infrastructure, spread fear, and disrupt economies. While their cyber activities are less frequent, they pose significant risks to national security. Data on specific groups is limited, but their impact is closely monitored by global agencies (UNODC et al., 2013).

Criminal Groups

Organized cybercriminal groups exploit tools like phishing, ransomware, and malware for financial gain. Cybercrime costs the global economy over $1 trillion annually (Hemsley & Fisher, 2018). These groups often operate from regions with weak enforcement against cybercrime (Masas, 2023).

Hackers

Individual hackers seek personal or financial gains and often evolve their techniques to stay ahead. Their motivations range from showcasing skills to gaining reputation within the hacker community (Zetter & Crown Publishing Group, n.d.).

Malicious Insiders

Insiders, such as employees or contractors, abuse their access to steal information or harm systems. Outsiders compromising insider accounts can also act as this threat, making it challenging to detect (Buckland et al., n.d.).

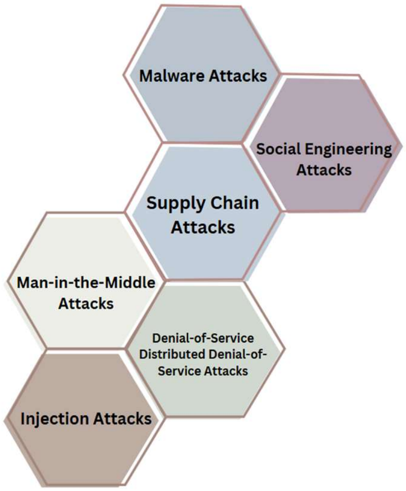
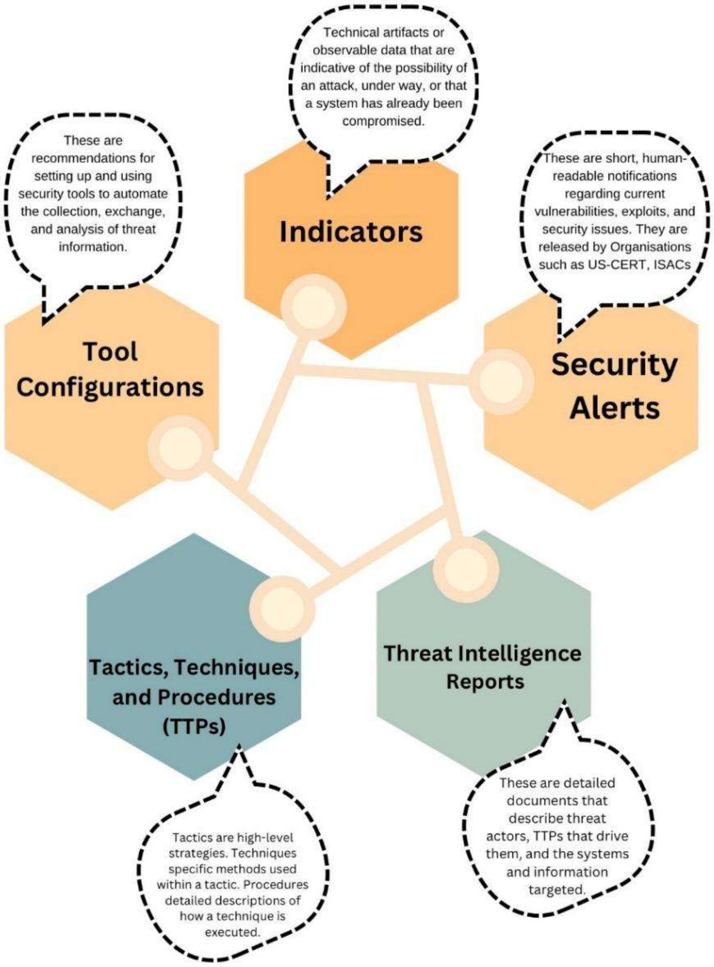

Malware Attacks
Social Engineering Attacks
Supply Chain Attacks
Man-in-the-Middle Attacks
Denial-of-Service Distributed Denial-of-Service Attacks
Injection Attacks

Figure 3: Types of cyber security Threats

Attack Type	Cause	Method	Impact	Data/Example	Reference
Malware Attacks	Exploitation of vulnerabilities; user-triggered	Viruses, worms, trojans, ransomware, spyware,	Data theft, disruption, remote control	**WannaCry ransomware** (2017) infected 230,000+ computers in 150	[Europol (2017), Malwarebytes Labs (2020)]

	actions	fileless malware, rootkits		countries, $4 billion in damages. **Fileless malware** grew by 265% in 2019 alone.	
Social Engineering Attacks	Human psychology exploitation (trust, fear, urgency)	Baiting, pretexting, phishing, vishing, smishing, piggybacking, tailgating	Unauthorized access, data theft	**Verizon DBIR 2022**: 82% of breaches involved human element. Phishing responsible for over 36% of breaches.	[Verizon DBIR (2022)]
Supply Chain Attacks	Trust in vendors and software updates	Compromised software/code signed with legitimate certificates	Stealth access, massive compromise	**SolarWinds Attack (2020)** compromised 18,000+ companies/government bodies; cost estimates over $90 million.	[CISA SolarWinds Report (2021)]
Man-in-the-Middle (MitM) Attacks	Weak encryption, insecure networks	Wi-Fi sniffing, DNS spoofing, HTTPS hijacking, email hijacking	Data theft, session hijack, impersonation	**Firesheep tool (2010)** exposed millions to Wi-Fi hijacking vulnerabilities; **HTTPS Spoofing** exploited in past LinkedIn attacks.	[EFF (Electronic Frontier Foundation)]
Denial-of-Service (DoS/DDoS) Attacks	Lack of anti-DDoS systems, network	SYN flood, HTTP flood, UDP flood, NTP	Website/service outages, financial loss	**Mirai Botnet (2016)** led to a 1.2 Tbps DDoS attack affecting Dyn,	[Krebs on Security (2016), Cloudflare

	flaws	amplification		Twitter, Netflix, Reddit.	Analysis]
Injection Attacks	Poor input validation in applications	SQL injection, OS command injection, LDAP injection, XXE, XSS	Data breaches, session hijacking, remote control	**Sony PSN Hack (2011)** used SQLi; 77 million accounts breached; ~$171 million in losses.	[OWASP, BBC News (2011)]


Indicators
Tool Configurations
Security Alerts
Tactics, Techniques, and Procedures (TTPs)
Threat Intelligence Reports

Technical artifacts or observable data that are indicative of the possibility of an attack, under way, or that a system has already been compromised.

These are recommendations for setting up and using security tools to automate the collection, exchange, and analysis of threat information.

These are short, human-readable notifications regarding current vulnerabilities, exploits, and security issues. They are released by Organisations such as US-CERT, ISACs

Tactics are high-level strategies. Techniques specific methods used within a tactic. Procedures detailed descriptions of how a technique is executed.

These are detailed documents that describe threat actors, TTPs that drive them, and the systems and information targeted.

Figure 4: Threat Information Types

2.2 Timeline of Major Cyber Incidents

Date	Event	Details	Impact
27 August 2012	RasGas Attack	Malware spread across networks, using command-and-control communications.	ICS/SCADA unaffected, but caused operational disruption.
October 2018	Global Cyber Incidents	Iran neutralized a Stuxnet variant; U.S. indicted Chinese hackers; linked a Saudi attack to Russian institutes; targeted Russian election operatives; China, Russia spying on Trump's calls; DHS election cyber warnings; Ukraine accused Russia; U.S. charged GRU officers.	Global spread of cyber activities, exposing vulnerabilities across sectors.
May 2021	Ransomware and Cyberattacks	LineStar and Colonial Pipeline ransomware attacks; North Korea hacked South Korea's KAERI; REvil attacked JBS; Fujitsu hacked; Irish health services hit by Conti ransomware; Avaddon ransomware spread worldwide.	Highlighted ransomware and cyber espionage threats to critical sectors globally.
March 2022	Global Cyberattacks	Greenland parliament hacked; China accused U.S. of cyberattacks; Chinese actors exploited Microsoft vulnerabilities; Russian sites hacked for protests; NRC Canada breached; U.S. networks accessed via Log4j exploit.	Demonstrated cyber vulnerabilities in government and financial sectors.
June 2023	Cyber Events	Illinois hospital closed due to 2021 ransomware; Pro-Russian DDoS on Swiss sites; North Korea stole $3 billion for missiles; Ukrainian hackers targeted Russian telecom; Russia accused Apple of aiding U.S. hacking.	Financial and political impacts; escalation of cyber warfare accusations.
March	Recent	Iranian hackers breached Israeli nuclear	Rising cyber

2024	Cyberattacks	site network; Russian phishing attacks on German political parties; Indian government sectors targeted; U.S. indicted Chinese hackers for EU and Italian MP spying; Canada's FINTRAC attacked.	conflicts among nation-states; critical government sectors targeted.

Center for Strategic and International Studies (CSIS). (2024). Significant cyber incidents since 2006

2.3 Trends in Cyber Attacks, Cyber Crimes, and Information Warfare

Trend/Statistic	**Details**	**Source**
Cyber Attacks	50 percent of UK businesses experienced cyberattacks in 2023, with SMEs being major targets.	Cybersecurity & Infrastructure Security Agency [CISA], 2023
Phishing	323,972 internet users fell victim to phishing in 2021, accounting for half of all data breaches.	Verizon. (2022). 2022 Data breach investigations report
Ransomware Attacks	236.1 million ransomware attacks reported globally in the first half of 2022, with double extortion tactics becoming common.	Cybersecurity Ventures. (2022). Global ransomware statistics report
Cost of Data Breaches	Average cost of a data breach in 2024 is $4.88 million. Industries like healthcare, finance, and retail are most affected.	IBM. (2024). Cost of data breaches: 2024 report
Cybercrime Financial Impact	Global cost of cybercrime expected to reach $24 trillion by 2027. The average cost of a	Cybersecurity Ventures. (2022). Global ransomware statistics report

	ransomware attack is $1.85 million.	
SMBs Vulnerability	46 percent of cyberattacks worldwide affect SMBs. 50 percent of SMBs lack a cybersecurity plan.	Accenture. (2023). Cybersecurity vulnerability in SMBs
Cybersecurity Workforce Growth	9 percent growth in cybersecurity employment in 2023, projected to grow by 32 percent by 2032.	U.S. Bureau of Labor Statistics. (2023). Cybersecurity employment growth.
Regional Cybercrime Insights	U.S. accounts for 59 percent of all ransomware attacks. Poland has the highest cybersecurity preparedness (NCSI score: 90.83).	McAfee. (2022). Cybercrime and regional insights, National Cyber Security Centre. (2023). Cybersecurity preparedness by country
Increase in Cybercrime	Cybercrime victim count increased by 1517 percent from 2001 to 2021. Hourly loss from data breaches: $787,671 in 2021.	Verizon. (2021). 2021 Data breach investigations report
Geopolitical Cyberattacks	Russian-backed hackers targeted U.S. election systems and infrastructure, including the Democratic National Committee in 2016.	U.S. Department of Justice. (2020). Russian-backed cyberattacks on U.S. election systems.
COVID-19 Impact	Malware attacks increased by 358 percent from 2019 to 2020, highlighting new vulnerabilities created by remote work.	McAfee. (2021). COVID-19 and the surge in cybercrime

This table summarises key trends and statistics related to cyberattacks, cybercrime, and information warfare, along with their sources

2.4 Global Socio-Economic and Political Impacts of Cyber Threats

Cyber threats have profound implications for global socio-economic systems and political structures. The interdependence of modern societies amplifies the risks of cyberattacks, cybercrime, and information warfare, leading to wide-ranging impacts across various sectors. These threats challenge the resilience of national and international institutions, disrupt economies, and shape geopolitical dynamics, thus requiring robust global responses (The United Nations Institute for Disarmament Research & Kavanagh, 2017).

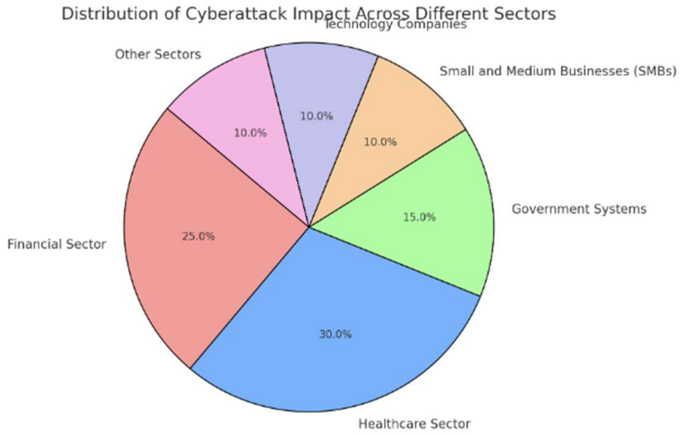
Socio-Economic Impacts

Cyber threats against international financial systems and key infrastructure are growing, representing substantial socio-economic risk. The WannaCry ransomware attack of 2017 that disabled healthcare networks around the world and the Bangladesh central bank cyberheist in 2016 identify weaknesses capable of triggering comprehensive financial insecurity. Cybercrime has been estimated to cost the worldwide economy $10.5 trillion each year by 2025, and the small and medium-sized enterprises (SMBs) are specifically exposed (UNODC et al., 2013).

In Canada, cyber election interference, such as efforts by foreign powers like China to influence the political process, is another economic threat. These threats are politically destabilizing, causing market disruption and investor confidence. Examples in the past, such as the 2016 U.S. election interference, demonstrate how disinformation campaigns can destabilize the financial system (U.S. Department of Justice, 2020). In order to counteract these risks, companies need to actively track political events, employ political analysts, establish government contacts, and invest in lobbying, financial hedging, and political risk insurance.

The escalating digital evolution of the financial system, hastened by the COVID-19 crisis, enhances exposure to cyber threats. These attacks, usually state-sponsored or criminal, are directed at the integrity of financial data, which jeopardizes public confidence and financial stability (McAfee, 2021). The global financial community is confronted with an uneven response to these threats, with ill-defined roles and responsibilities.

To solve these problems, authorities propose tighter coordination among governments, banking institutions, and technology firms, along with international cooperation. Bolstering cybersecurity, raising workforce capability, and enhancing regulatory systems are key moves in protecting the world economy from future cyberattacks. Joint, well-coordinated action is required to reduce the escalating cyber threat to financial stability (ITU et al., 2021).



Political Impact

Cyber threats increasingly redefine global power dynamics, ushering in new conflict areas and reallocating influence. High-visibility attacks like the 2020 SolarWinds attack against U.S. government institutions exemplify the mounting ability of state-sponsored cyber-attacks to compromise national security (CISA, 2020; Hemsley & Fisher, 2018). At the political level, cyber campaigns have profoundly affected democratic processes; in the 2016 United States presidential election, Russian attempts at interference in the form of leaked emails and disinformation campaigns undermined public trust in institutions and exposed weaknesses in electoral systems (COLOMINA et al., 2021; UNODC et al., 2013).

Canada's experience confirms this trend as well. Though its democratic processes are lower-priority targets than the U.S., events like the recent confirmation of Chinese interference attempts during the 2019 federal election demonstrate that even stable democracies are not exempt (Office of the Privacy Commissioner of Canada, 2015; UNIDIR & Kavanagh, 2017). Even though paper ballots protect the fundamental act of voting, digital components—like voter registers and political campaign management—continue to be vulnerable to manipulation, compromising the integrity and reliability of democratic institutions.

As digital activities increasingly become part of the political processes globally, cyber threats are turning into instruments of data warfare, narrative manipulation, and obdurescence of dissent, particularly from the hands of players like China and Russia as they attempt to push back against Western hegemony in cyberspace (Ronchi, 2020; CSIS, 2024; Li & Liu, 2021). This new development calls for quick global governance changes. Improving global standards, strengthening interagency coordination, and establishing human capital resilience through strategic training are important steps toward defending democratic processes against cyber threats, reaffirming the United Nations' role in closing governance gaps in cyberspace (UNIDIR & Kavanagh, 2017; ITU et al., 2021; Nye et al., 2014).

Cyber Threats and International Relations

3.1 Diplomacy: Opportunities and Challenges

The incorporation of digital instruments into diplomatic practice has made it more susceptible to cyberattacks, such as espionage, disinformation, and data theft, as seen in the case of the 2016 Democratic National Committee (DNC) email hack (COLOMINA et al., 2021). This highlights the vital shortfall of the international system as it is now: the lack of shared norms and legally binding mechanisms for regulating state conduct in cyberspace (Tikk et al., 2010). As new technologies like artificial intelligence, blockchain, and big data analytics are rapidly developing, the effects of these technologies on diplomatic processes become increasingly complicated and uncertain (Li & Liu, 2021). It demands a rebalancing of international governance systems, with emphasis laid on the development of global cyber norms, strengthened cybersecurity collaboration, and substantial capacity-development for the developing states (United Nations Institute for Disarmament Research & Kavanagh, 2017). Unless these steps are taken, the digital divide will grow, disenfranchising major segments of the global South and compromising the legitimacy and inclusivity of global governance (International Telecommunication Union et al., 2021). Therefore, digital diplomacy has to be addressed not as a convenience tool but as a sensitive space needing strong regulation, moral stewardship, and fair access so that it contributes to the common good of the international community (Nye, 2011).

3.2 National Sovereignty in the Digital Era

The digital era has dramatically reconfigured the concept of national sovereignty, especially in the field of diplomacy. Digital technologies like Twitter, Facebook, and video conferencing have completely transformed diplomatic practice by facilitating immediate communication and more representative global discourse (Bjola & Holmes, 2015). These media were a key enabler during the COVID-19 pandemic, facilitating fast coordination and information exchange between states and global institutions (Nye, 2011). While these developments have increased transparency and extended participation in global governance, they also bring diplomatic processes under unprecedented risks. Cyber espionage, disinformation campaigns, and electronic surveillance have emerged as core challenges, compromising the confidentiality and integrity of diplomatic communication (COLOMINA et al., 2021). The hack of the DNC emails in 2016 illustrates how cyberattacks can interfere with democratic processes and undermine confidence in international relations (Tikk et al., 2010).

More seriously, these threats are compounded by the lack of universally accepted norms governing state behavior in cyberspace. The international legal framework currently is not well suited to deal with the novel challenges presented by cyber operations, so digital sovereignty is fragmented and frequently disputed (United Nations Institute for Disarmament Research & Kavanagh, 2017). With increasingly rapid progress being made in new technologies such as artificial intelligence, blockchain, and big data analytics, the complexity of these challenges rises exponentially (Li & Liu, 2021). These technologies not only extend state and non-state actors' possibilities but also mix national and transnational spheres of influence (International Telecommunication Union et al., 2021).

Here, the protection of national sovereignty in the digital age requires a radical redefinition of classical governance models. States need to focus on building strong cybersecurity measures and ensure the formulation of enforceable international norms governing conduct in cyberspace (Tikk et al., 2010). Equally crucial is the imperative for inclusive multilateral cooperation that bridges the digital divide. It is critical to support the developing nations, which may not possess the technical base and regulatory institutions, through focused capacity-building programs and public-private partnerships (United Nations Institute for Disarmament Research & Kavanagh, 2017). This will not only facilitate their effective involvement in digital diplomacy but also assure that essential issues like data privacy, digital rights, and disinformation are tackled fairly. Ultimately, national sovereignty in the age of the Internet cannot be safeguarded alone—it demands a cooperative, concerted, and visionary global action that strikes a balance between innovation and accountability (Nye, 2011).

3.3 Cyber Threats and International Power Dynamics

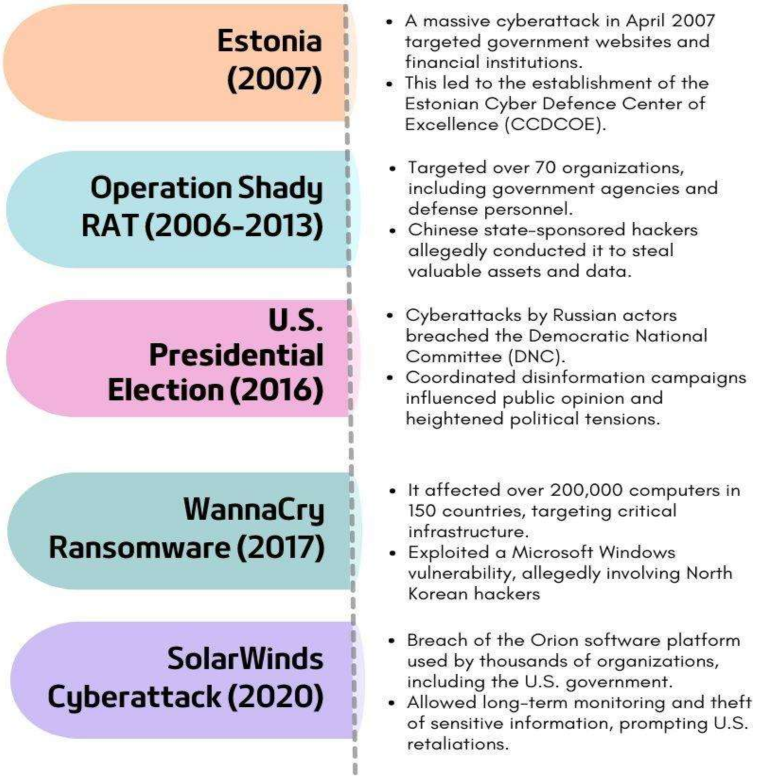
The emergence of cyber threats has profoundly changed the international power balance, turning cyberspace into the focal battleground of contemporary national art. Unlike other conventional military tools, cyber activities enable states to shape strategic objectives like espionage, obstruction, and operational effects without having to contend with evident physical struggles (Tikk, Kaska, & Vihul, 2010). The first of these examples is the Stuxnet attack in 2010 on the Iranian nuclear program. This is claimed to have been coordinated by Israel and the US, and provides an example of how cyber weapons can be applied to inflict very significant damage yet still have a plausible degree of denial (Zetter, 2014). It will turn cyberspace into an affordable and highly effective conduit through which states can manipulate, chase geopolitical ambitions and transform the character of contemporary conflict (Carr, 2011).

The charges of hacking the 2016 US presidential election and the suspected hack of China's US personnel management in 2015 demonstrate the manner in which cyber intrusion discredits national security, undermines democratic institutions, and probes the integrity of global norms (Rid, 2020). Beyond state actors, the cyber space facilitated small states and non-state actors, hindering traditional hierarchies of power. The case of North Korea covered in the WannaCry Ransomware Attack 2017 illustrates how conventionally weak actors can utilize cyber technology to cause global barriers and pursue economic or political gains (Greenberg, 2019). This diffusion of cyberskills blurs the power advantage within the international system (Valeriano & Maness, 2015).

The United Nations addresses the development of government expert groups (GGE) and open-ended working groups (OEWGs), but these are only attempts with non-binding principles (UNODA, 2021). The absence of bonds in global law leaves cyberspace open to manipulation and escalation. With great powers making the digital world more militarized, there is a growing risk of miscalculation and unintended wars (Maurer, 2018). With cooperation and shared responsibility, the world desires stability, sovereignty, and confidence in the virtual world (UNIDIR & Kavanagh, 2017).

3.4 Case Studies: High-Profile Cybersecurity Incidents Impacting International Relations

Cyber threats significantly shape international power dynamics, transforming social relations, shifting power balances, and determining future global security (Hathaway & Levitz, 2018). Greater international cooperation is essential to combat evolving cyber threats (Lewis, 2018).



Estonia (2007)

- A massive cyberattack in April 2007 targeted government websites and financial institutions.
- This led to the establishment of the Estonian Cyber Defence Center of Excellence (CCDCOE).

Operation Shady RAT (2006-2013)

- Targeted over 70 organizations, including government agencies and defense personnel.
- Chinese state-sponsored hackers allegedly conducted it to steal valuable assets and data.

U.S. Presidential Election (2016)

- Cyberattacks by Russian actors breached the Democratic National Committee (DNC).
- Coordinated disinformation campaigns influenced public opinion and heightened political tensions.

WannaCry Ransomware (2017)

- It affected over 200,000 computers in 150 countries, targeting critical infrastructure.
- Exploited a Microsoft Windows vulnerability, allegedly involving North Korean hackers

SolarWinds Cyberattack (2020)

- Breach of the Orion software platform used by thousands of organizations, including the U.S. government.
- Allowed long-term monitoring and theft of sensitive information, prompting U.S. retaliations.

Figure 5: Case Studies

These case studies reflect the seriousness of high-profile cybersecurity breaches towards international relations and governance, underscoring that urgent global cooperation and robust frameworks are needed to grapple with this challenge (Masas, 2023).

The United Nations and Cybersecurity

4.1 Overview of the UN's Traditional Governance Structures

There is significant decentralisation in the traditional governance structures offered by the United Nations on cybersecurity. These are characterised by the different frameworks within which the separate entities operate based on their mandate, operational environment, and priority. Thus, there is a significant variation of preparedness, resources, and technology applied across the UN system since each entity manages its cybersecurity risks. This has resulted in fragmented models of cybersecurity maturity whose differences range from data types, the priorities of the leadership in terms of cybersecurity, historical ICT investment, and access to financial and technical resources (Masas, 2023).

The approach of the UN is primarily vertical, focusing on internal resilience within each organisation. Such efforts cover endpoint device management, vulnerability remediation in legacy systems, secure adoption of cloud computing, and risk mitigation in shadow IT. Even distribution of best practice implementation and a different technological advancement level across entities are prohibitive factors for such efforts. Legacy systems are the most difficult to manage as they may not support the latest security measures, making organisations susceptible to state-of-the-art cyberattacks.

Horizontal governance or interagency coordination, cooperation, and information sharing is important in such an integrated setting as the United Nations system; however, after some progress here, a lack of system-wide cybersecurity strategy also exists, thus underpinning current constraints to successful cooperation. Probably few coordination mechanisms have been underutilised or less adopted, among them shared threat intelligence platforms and collective security solutions, which present one of the biggest pain areas of cohesive cybersecurity governance within a loosely coupled system.

COVID-19 highly unveiled vulnerabilities and accelerated transformations in UN entities' cybersecurity. Widespread work-from-home arrangements made urgent improvements to remote-access security necessary, pushing a number of ICT projects and necessitating further efficiencies within security management frameworks. It also showed how innovation could bring long-standing problems with poorly coordinated approaches and outdated governance models more broadly into prominence (Masas, 2023).

4.2 The UN's Role in Cybersecurity: Past and Present

The UN has played a crucial role in building the global cybersecurity landscape through norms, frameworks, and cooperation to combat surging cyber threats. Such a role has transformed from what it used to be centuries ago up to this date because of changes in the nature of cyber threats and the geopolitical climate. Following is a more detailed analysis of the efforts exerted by the UN in the past and the current initiatives, including achievements, challenges, and future directions.

The first engagement of the UN was in the establishment of the International Telecommunication Union in 1865, which it used to advance international cooperation in telecommunications. Later, it provided a platform for cybersecurity discussions through this organisation. Some of the critical steps taken were the World Summit on the Information

Society in 2003 and 2005, where it set focus on the significance of a secure information society and capacity building for developing nations. The General Assembly of the UN also passed several resolutions since 1998 that gave way to the development of cooperation globally in cybercrime.

During recent years, the UN has made several efforts to mitigate increasing cybersecurity problems. The office for disarmament affairs of the UN has made major contributions by bringing together world forums on information and communication technologies and international security. The United Nations Office for Disarmament Affairs (UNODA) provides support to Group of Governmental Experts (GGE) and Open-ended Working Group (OEWG) that advance norms, rules, and principles for responsible state behaviour in cyberspace. The above groups highlight the importance of international cooperation in avoiding cyber conflicts as well as putting in place responsible actions in the cyber world.

The UN Conference on Trade and Development deals with cybersecurity in e-commerce and the digital economy. The organisation acknowledges the demand for security and trust and has been offering analysis and technical assistance to developing countries to strengthen their cybersecurity capabilities and improve their engagement in the global digital marketplace. The Cyber Peace Institute, though not the offspring of the UN, collaborates with it and many other international bodies to strengthen global cybersecurity. The concentration areas of the institute are support for vulnerable communities, cyber threat analysis, and advocacy for accountability in cyberspace, each of which aligns with the UN's focus areas of building digital peace and security.

4.3 Influence of Western and Anglo-Saxon Philosophies on the UN Framework

The UN framework since its inception in 1945 was constructed in the image of Western and Anglo-Saxon philosophies. Most work in formulating its Charter involved the United States, the United Kingdom, and their allies, who played a central role in shaping the international organisation around principles of state sovereignty, individual rights, rule of law, and liberal democracy that form the core of Western political thought.

The principle of state sovereignty and non-intervention, therefore, is an Anglo-Saxon contribution to philosophy. It appears in Article 2(7) of the UN Charter. That provision forbids interference by the organisation in member states' internal affairs. Derived from the

Treaty of Westphalia (1648), thinkers such as John Locke, and Hugo Grotius, this principle was essentially to prevent interference with national independence. However, it has been attacked in its viewpoint of having limited the response of the UN to human rights violations and cyber threats in a globally interconnected world. Emphasis on liberal democracy and human rights is also one of the defining features, influenced by the ideologies of Enlightenment thinkers, including Immanuel Kant and John Stuart Mill. These principles reflect the Universal Declaration of Human Rights (1948), which are the basis of many UN undertakings and agencies, such as the Human Rights Council and the International Court of Justice. However, some non-Western nations are critical of it for imposing the norms of the West on diversified cultural and political contexts, thus creating conflicts within the organisation.

Western philosophies also inspired the economic and security aspects of the UN. The Bretton Woods institutions, formed alongside the UN, were based on free-market principles and Western economic models. The UN Security Council (UNSC), dominated by its Permanent Five members (the U.S., U.K., France, Russia, and China), reflects post-World War II power dynamics favouring Western allies. The veto power granted to the P5 is often seen as perpetuating Western dominance and hindering equitable representation of emerging powers in global decision-making. In terms of cybersecurity, open internet governance, free information, and privacy rights in Western philosophies contrast with state sovereignty and the control of virtual spaces by the state in authoritarian regimes. These ideological conflicts are reflected in the debates taking place within the UN, GGE, and OEWG on issues of cybersecurity, with Western nations trying to promote the norms of openness and accountability and others advocating state-centric approaches.

Critics often argue that in some instances, this Western influence fails to incorporate the diverse needs of non-Western countries, and most developing nations have the view that UN liberal values and market-oriented solutions forget their own socio-economic plight. Reforming calls for the UN mostly address such imbalances to make the system more inclusive.

On the other hand, despite such criticisms, Western and Anglo-Saxon philosophies have also facilitated the UN in projecting universal principles of peace, justice, and cooperation. The challenge in the 21st century is to find a balance between foundational values and changing priorities in a multipolar, digitally interconnected world.

4.4. Challenges of Consensus-Based Decision-Making in Cyberspace

It is difficult to reach consensus on decisions in cyberspace because of the complexity of the digital environment. Agreement on one matter by multiple stakeholders with differing priorities can cause delay and impede a timely response to cyber threats. A Forbes article highlights the need for structured decision-making frameworks when navigating differences in viewpoints (Forbes, 2025).

The consensus principle may be very demanding on international organisations such as ASEAN. According to a report on cyber norms in ASEAN, it is found that consensus-based decision-making has hindered the development of collective expectations as member states would have to reach an agreement; this may often be undermined by national interests and levels of cyber capability, thereby being only superficial adherence and not a real commitment, as the latter may do just to ensure the consensus is met rather than agreeing on a value for the norms. This fast-evolving nature of cyber threats calls for quick responses that consensus-based approaches might find hard to provide. The need for unanimity might delay decision-making and put systems at risk. According to an article published in War on the Rocks, delays are leveraged by the adversary through deceptions and espionage in the course of manipulating the process of decision-making and compromise on security (War on the Rocks, 2025).

Besides that, the nonexistence of one reference framework has made it harder to evaluate and compare the level of maturity across organisations in their cybersecurity. Lacking standardisation may result in less consistent security and defence gaps between organisations, just as discussed during the management convergence on cyber risk management.

4.5. Limitations of Current UN Mechanisms for Cyber Threat Management

The United Nations has significant limitations in managing cyber threats due to differences in the maturity and coordination of cybersecurity measures within its organisations. While organisations that handle politically sensitive data, such as the World Health Organization (WHO) and International Civil Aviation Organization (ICAO), are placing a high priority on cybersecurity, others have been less proactive, making the readiness not uniform (United Nations, 2025).

An important weakness is an integrated framework to assess and manage cybersecurity risks. Self-evaluations showed that there are differences in cybersecurity maturity from "average" to "weak" across the areas of identification, protection, detection, response, and recovery. The lack of integrated benchmarks makes it difficult to compare and measure strategies against one another, further affecting unified security implementations..

Decentralised investments in IT systems aggravate this issue. Most organisations have outdated or incompatible infrastructure that hinders an effective response to cyber threats. Differences in priorities and availability of resources among leadership further widen the gaps in cybersecurity measures. UN organisations are interdependent, with shared infrastructure and data centers; therefore, poor security in one entity can easily compromise others. The system is only as strong as its weakest link, making this a dangerous risk. Despite this, collective mechanisms for mitigating threats are underdeveloped.

Human-related vulnerabilities include configuration errors and inadequate training. Phishing and malware are so common that current mechanisms do not adequately address the need for widespread user education and awareness (United Nations, 2025).

Key Challenges in International Cooperation on Cybersecurity

5.1 Political and Ideological Barriers to Collaboration

Political and ideological barriers to international cooperation on cybersecurity have many political biases and influences. States are often interested in their special benefits and control over security issues. Regional competition between the U.S., China, and Russia plays a huge role in this area. The United States and its allies promote an open, free internet operating on privacy and personal freedom principles. Meanwhile, China and Russia explain their national sovereignty in cyberspace as "cyber sovereignty," pursuing increased control over events and activity within their borders (Bort, 2021).

Competing treaties include the Budapest Convention on Cybercrime and the Shanghai Cooperation Organisation Convention on Cyber Security. Countries generally distrust cybersecurity initiatives, viewing them through a national security lens, and fear that international agreements could be used to curtail their cyber capabilities. The U.S. has withdrawn from some UN discussions, citing concerns over surveillance and abuses. To Western countries, the cyber sovereignty proposition China is taking can be likened to trying to legitimise censorship and control. Escalating tensions of late include charges that Russia staged the 2020 SolarWinds cyberattack blamed on them as well as hacking into U.S. electoral machinery in the 2016 U.S. elections, hence damaging international relationships and cooperation (Sanger, 2020).

Cyber capabilities for national security may be used to commit terrorism. The 2020 SolarWinds attack
that exploited software vulnerabilities affected many countries and organisations worldwide, showing the potential of state-led cyber strategies to compromise global security. Richer countries with strong internet systems overshadow international conferences; thus, little representation is observed for developing countries. This fact deters engaging participation, spreading the digital gap, and makes collective security relatively weak. Hesitance to divulge threats or vulnerabilities undermines mutual trust and coordinated response. Thus, national and international security considerations need to strike a balance so that cooperation toward cybersecurity is effective (UNCTAD, 2021).

Current governance models are severely tested in dealing with the complexities of modern cybersecurity issues. Traditional models, such as the UN-led one, are centred on state sovereignty, consensus-based decision-making, and non-intervention but fail in the face of borderless cyber threats. A significant limitation is the lack of a global standard legal framework for cybersecurity. Agreements such as the Budapest Convention on Cybercrime have limited participation, and thus, the approaches are fragmented. For example, the EU's General Data Protection Regulation focuses on privacy, while other countries focus on offense and surveillance. International decision-making is slow and bureaucratic, which hinders the response to rapidly evolving cyber threats. Incidents like the SolarWinds breach and the WannaCry ransomware attack highlight the need for swift, coordinated action. However, consensus-based approaches can enable single nations to block progress, leading to delays (Naylor, 2020).

Major powers dominate the governance of cybersecurity, and frameworks from organisations such as NATO and the European Union are perceived as biased toward Western interests, thereby creating mistrust among non-Western nations who advocate for state-centric approaches, such as the Shanghai Cooperation Organisation (SCO). Economic and technological disparities also represent barriers because many developing countries have insufficient resources for robust participation in global efforts. The initiatives that the International Telecommunication Union initiates are faced with funding and alignment challenges, among others. Non-state actors, such as cybercriminals, hacktivists, and private corporations, complicate governance further, especially because the present models of governance are primarily founded on state behaviour (Paganini, 2020).

5.2 Case Studies: Successes and Failures in International Cyber Cooperation

International cooperation on cybersecurity has had both successes and failures, reflecting the complexities of addressing transnational cyber threats in a fragmented global landscape.

Successes:

1. **Budapest Convention on Cybercrime (2001):** The first binding treaty to combat cybercrime, fostering legal standards and international cooperation. However, its Western-centric approach limits global adoption, with key nations like Russia, China, and India refusing to join (Baker, 2020).
2. **NATO Cooperative Cyber Defence Centre of Excellence:** Founded after Estonia was attacked by cyberattacks in 2007, this center enhances cyber defense research and training and published the Tallinn Manual on cyber warfare law. However, its exclusivity alienates non-NATO states, especially those in the Global South. The center has played a crucial role in fostering cooperation and advancing knowledge of international law in cyberspace (Smith, 2021).
3. **EU Cyber Policies:** General Data Protection Regulation (GDPR) and the NIS Directive have been some of the initiatives that have strengthened cybersecurity and inspired global policies, though uneven implementation remains a challenge (O'Reilly, 2021).

Failures:

1. **UN Cyber Norms:** The effort by the UN Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG) to create binding norms about state cyber behavior has failed primarily because of rivalries in geopolitics and disagreements in cyber sovereignty. For example, the disagreement among Western democracies and authoritarian states, including Russia and China, on the regulatory body of cyber sovereignty and internet governance hinders meaningful efforts (Cohen, 2020).
2. **WannaCry Attack (2017):** Global cybersecurity vulnerabilities were thrown into the limelight, but fragmented responses and a lack of universal legal frameworks hindered accountability. Affecting over 150 countries, crippling institutions such as the UK's

National Health Service, the attack threw the vulnerabilities in global cybersecurity infrastructure into sharp relief (Jones, 2018).

3. **Russian Interference in the U.S. Election (2016):** Russia's alleged hacking and disinformation campaigns revealed challenges in attributing state-sponsored cyberattacks and enforcing norms, straining international relations. Despite broad recognition of the threat, lack of consensus on attributing state-sponsored cyberattacks and the absence of enforceable norms have impeded collective responses (Turner, 2017).

Hence, the case studies mentioned above highlight the substantial progress in international cooperation on cybersecurity, but the geopolitical tensions and ideological differences on cyber sovereignty continue to hinder global efforts. The successful cooperation highlights the capabilities of regional and alliance-based counter efforts for cybersecurity. At the same time, failures speak about the necessity for change, such as transparency, inclusivity, and practicality of the frameworks.

Recommendations for Reform

The rapidly changing landscape of cybersecurity presents significant challenges to global governance as the current legal and regulatory frameworks are no longer able to cope with the increasingly complex and scaled cyber threats. These range from state-sponsored cyberattacks to cybercrime, and are becoming increasingly more frequent and sophisticated, making robust and adaptive measures in cybersecurity imperative (Johnson, 2021). International organisations, including the UN, the European Union (EU), among others, have evolved to fill in part some of these gaps. However, important ones are still there. These include, among others, different types of jurisdictional arrangements, processes of collecting cross-border evidence, and mechanisms of cooperation amongst various nations. Diversities in legal structures, political concerns, and technology amongst different nations usually discredit partnerships towards successful collaboration on global efforts towards cybersecurity (Smith & Lee, 2020).

There must be a coordinated and flexible policy response to these challenges. Policymakers need to balance concerns for security against the protection of fundamental rights like privacy and freedom of expression (Chavez, 2020). Public-Private Partnerships (PPPs) shall be essential sources to tap private sector expertise, especially for companies in the high-tech sector who play a leading role in cyber threat detection and response (Baker & Johnson, 2021). The Global Forum on Cyber Expertise (GFCE) and the Internet Governance Forum (IGF) are collaborative initiatives that foster dialogue and trust among stakeholders, thus enhancing collective resilience against cyber threats (Rosen, 2021).

Adaptive policymaking is also important in keeping up with the rapid changes happening in technology, from artificial intelligence, blockchain, and quantum computing. The GDPR by the EU reflects how the rules are adapted to balance between privacy and security (O'Reilly, 2021). Governments should invest in real-time threat intelligence sharing and rapid response strategies, such as the collaboration between the U.S. government and private enterprise following the SolarWinds attack in 2020 (Turner, 2021). Estonia is a country that demonstrates resilience through frequent policy updates and robust cybersecurity infrastructures (Vik, 2021).

International legal frameworks should be strengthened in the face of cybercrime and digital threats. Agreements have been established between the international world through conventions, for example, the Convention on Cybercrime by the Council of Europe and the Convention on Cybersecurity and Protection of Personal Data of the African Union. Nevertheless, these conventions still fail at times in their cooperation towards the responding of state-sponsored cyberattacks, cyber espionage, and protection of critical infrastructure (Blake, 2020). Institutions in the sectors such as the International Atomic Energy Agency and NATO contribute a lot to the diminishment of cyber threats in their subdomains (Lynch, 2021). International agreements should be harmonised in terms of implementation across each country, reducing disagreement in jurisdictions and having better global cybersecurity (Klein, 2021).

Ensuring fair participation in the global governance of cybersecurity requires building capacity, especially for developing nations (Ghosh, 2020). Cyber diplomacy efforts are effective in facilitating cooperation and filling the technological gaps. Moreover, it is also essential to ensure that the views of civil society organisations, nongovernmental organisations, and academic institutions within the practice of cybersecurity are met to promote ethics and transparency and to determine the rights of human beings (Miller & Jones, 2020).

In conclusion, dealing with increasingly complex cyber threats calls for a collaborative, inclusive, and flexible global governance framework. Enhancing international standards, raising the level of information sharing, and promoting cooperation between governments, the private sector, and civil society will bring the global community closer to a digital future that is secure and resilient (Harvey, 2021).

References

- Active Exploitation of SolarWinds Software | CISA. (2020, December 13). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/alerts/2020/12/13/active-exploitation-solarwinds-software
- Bjola, Corneliu & Holmes, Marcus. (2015). Digital Diplomacy: Theory and Practice. 10.4324/9781315730844.
- Buckland, B. S., Schreier, F., & Winkler, T. H. (n.d.). DCAF HORIZON 2015 WORKING PAPER https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf
- Callejas, J. F., Afifi, A., Lozinskiy, N., United Nations, Hermie, V., Petkov, S., Baudat, H., Dincic, D., Claveau, C., Datsii, A., & Canevari, B. (2021). Cybersecurity in the United Nations system organisations. In Report of the Joint Inspection Unit.
- Center for Strategic and International Studies (CSIS). (2024). Significant cyber incidents since 2006. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240418_Cyber_Events.pdf?VersionId=TlrSq2hBc9eZ0dxXgNfkeJpmn169IIOh
- COLOMINA, C., SÁNCHEZ MARGALEF, H., YOUNGS, R., European Parliament coordinator: Policy Department for External Relations, & JONES, K. (2021). The impact of disinformation on democratic processes and human rights in the world. In Trans European Policy Studies Association (TEPSA), European Parliament (PE 653.635) [Report]. European Union. https://doi.org/10.2861/59161 (Original work published 2021)
- CT TECH, Voronkov, V., Kavanagh, S., United Nations Office of Counter-Terrorism, International Criminal Police Organisation, United Nations Counter-Terrorism Centre, & El Hilali, K. (2023). Establishing legislative framework, transparency mechanisms and oversight for online data collection. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_establishing_legislative_framework_web.pdf
- Don Baham & Forbes Technology Council. (2020, July 8). Gaining consensus in IT and cybersecurity. Forbes. https://www.forbes.com/councils/forbestechcouncil/2020/07/08/gaining-consensus-in-it-and-cybersecurity/
- Humayun, M., Niazi, M., Jhanjhi, N. et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng 45, 3171–3189 (2020). https://doi.org/10.1007/s13369-019-04319-2

- International Telecommunication Union (ITU), Council of Europe (CoE), Commonwealth Secretariat (ComSec), Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organisation (INTERPOL), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations University (UNU)., World Economic Forum (WEF). (2021). Guide to Developing a National Cybersecurity Strategy 2nd Edition. In Guide to Developing a National Cybersecurity Strategy 2nd Edition. International Telecommunication Union (ITU). https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf
- Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C., Computer Security Division, Information Technology Laboratory, & The MITRE Corporation. (2016). NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
- Kevin E. Hemsley, & Ronald E. Fisher. (2018). History of Industrial Control System Cyber Incidents. Idaho National Laboratory, INL/CON-18-44411-Revision 2
- Liyuan Sun, Hongyun Zhang, & Chao Fang. (2021). Data Security Governance in the era of Big Data: status, challenges, and prospects, (Vol. 2). https://doi.org/10.1016/j.dsm.2021.06.001
- Masas, R. (2023, December 20). Cybersecurity Threats | Types & Sources | Imperva. Learning Center. https://www.imperva.com/learn/application-security/cyber-security-threats/
- Mason, S. (2021, December 16). Cyber challenges for the new National Defense Strategy - War on the Rocks. War on the Rocks. https://warontherocks.com/2021/12/cyber-challenges-for-the-new-national-defense-strategy
- Marko. (2024, January 22). Achieving management consensus on how best to address cyber risks continues to be a challenge. Global Cyber Conference. https://globalcyberconference.com/achieving-management-consensus-on-how-best-to-address-cyber-risks-continues-to-be-a-challenge
- M Mikk. (2007). Cyber Defence and Cyberwarfare: A brief history of Estonia’s cybersecurity landscape. NATO Cooperative Cyber Defence Centre of Excellence.

- Nye, J. S., Jr., Centre for International Governance Innovation, & Royal Institute for International Affairs. (2014). The regime complex for managing global cyber activities. GLOBAL COMMISSION ON INTERNET GOVERNANCE PAPER SERIES. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf
- Nye, J. S., Jr. & Pacific Forum CSIS. (2011). The future of power. In Pacific Forum CSIS (Vols. 11–8, Issue No. 8)
- Office of the Privacy Commissioner of Canada. (2015, February 12). Privacy and Cyber Security. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/
- Ronchi, A. M. (2020). 21st century cyber warfare. In ISIJ (Vols. 44–44, pp. 53–61). https://isij.eu/system/files/download-count/2023-01/4405_ronchi_21_century_cyber_warfare.pdf
- T. G., W. (n.d.). Global Governance: Why? what? whither? Polity Press
- The MIT Press, Massachusetts Institute of Technology. (2024, June 18). Book details - MIT Press. MIT Press. https://mitpress.mit.edu/9780262517690/cyberpolitics-in-international-relations/
- The United Nations Institute for Disarmament Research, & Kavanagh, C. (2017). The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st century. In UNIDIR RESOURCES. https://unidir.org/files/publication/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf
- Tikk, E., Kaska, K., Vihul, L., & Cooperative Cyber Defence Centre of Excellence (CCD COE). (2010). INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS. https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf
- Tran Dai, C., Asia Centre, Gomez, M. A., & Centre for Security Studies. (2017). Challenges and opportunities for cyber norms in ASEAN [Journal-article]. Asia Centre, Paris, France; Centre for Security Studies, ETH, Zurich, Switzerland. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Challenges%20and%20Opportunities%20for%20Cyber%20Norms%20in%20ASEAN%20Revised%20Final.pdf
- United Nations. (2025). Cybersecurity and the United Nations: Risks, Gaps, and Responses. https://www.un.org/cybersecurity-report

- UNODC, Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., Ignatuschtschenko, E., Max Planck Institute for Foreign and International Criminal Law, Brown, I., Wright, J., Oxford Internet Institute and Cyber Security Centre, University of Oxford, Broadhurst, R., Krüger, K., Brandenburg Institute for Society and Security, Sieber, U., Tropina, T., & Mühlen, N. V. Z. (2013). Comprehensive study on Cybercrime. In Draft. UNITED NATIONS. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- Wilson, E. K. K. (2017, August 7). Cyber risk, market failures, and financial stability. IMF. https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104
- Yuchong Li, & Qinghui Liu. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7.
- Zetter, K & Crown Publishing Group. (n.d.). Countdown to zero day.

ABOUT THE AUTHORS

Harshil Khokhar is a B.Tech graduate in Computer Science and Engineering with a specialization in Cyber Security from Rashtriya Raksha University, an Institute of National Importance. He currently works as a Programmer Analyst at Meditab Software India Pvt. Ltd., where he develops .NET Core Web APIs and handles complex database operations. Harshil has prior experience in web development, database administration, and ICT through multiple internships and roles. He also served as the President of IncuBeta E-Cell and has participated in various national-level cybersecurity and innovation challenges.

Kruti Hudka is currently pursuing an M.A. in International Relations, with a specialization in Security and Strategic Studies. Her academic interests lie in cybersecurity policy, international cooperation, and South East Asian geopolitics. She has conducted in-depth research on comparative cybersecurity strategies of India and China, and is currently working on the economic and strategic implications of Saudi Vision 2030 and UAE Vision 2050. Kruti combines her academic pursuits with strong analytical and writing skills, making her an emerging voice in the field of international security and digital diplomacy.

Prasann Barot is currently pursuing a Ph.D. in Computer Engineering at Charutar Vidya Mandal University, India. He has served as an Assistant Professor at Rashtriya Raksha University, where he taught courses and guided student research in machine learning and cybersecurity. His academic interests include deep learning, data analytics, and artificial intelligence, with multiple publications in reputable international journals and conferences.