Florida High Schools Model United Nations

GULF COAST 10

UNITED NATIONS SECURITY COUNCIL (UNSC)

GLOBAL CYBER CRISIS: SECURING SHARED INFRASTRUCTURE

Author: Isaiah Sloan

September 2024

Introduction

The global cyber landscape has evolved rapidly in recent years, transforming from a niche concern into a critical pillar of international security and economic stability. As our world becomes increasingly digitized and interconnected, the potential for cyber attacks to disrupt vital services, compromise sensitive information, and undermine national sovereignty has grown exponentially.[1] From state-sponsored hacking campaigns to ransomware attacks on critical infrastructure, the threats in cyberspace are diverse, sophisticated, and ever-evolving. While offering unprecedented opportunities for innovation and collaboration, this digital interdependence has also created new vulnerabilities that span national borders and traditional security paradigms.

In this complex and dynamic environment, cybersecurity has become a paramount concern for governments, businesses, and individuals. Protecting shared digital infrastructure is a technical challenge and geopolitical imperative. The need for coordinated global action has become increasingly apparent as cyber threats grow in scope and severity. In this context, the United Nations, mainly through its First Committee (Disarmament and International Security) or GA1, has taken on a crucial role in addressing cyber threats. By providing a forum for international dialogue, norm-setting, and capacity-building initiatives, the UN is working to foster a more secure and stable cyberspace.[2] To adequately address the crisis at hand, we must first address the challenges in securing shared infrastructure, as well as the ongoing efforts of the UN and GA1 to promote responsible state behavior and international cooperation in the digital realm.

Historical Context

The history of cybercrime and cyberterrorism on the international stage is inextricably linked to the rapid evolution of digital technologies. In the early days of the internet, cyber threats were primarily limited to individual hackers and small-scale fraud. However, as digital infrastructure became more integral to global commerce and governance, the nature and scale of cyber threats grew exponentially. The late 1990s and early 2000s saw the emergence of more sophisticated attacks, including distributed denial-of-service (DDoS) attacks and the spread of malicious software on a global scale. This period also marked the beginning of state-sponsored cyber activities, with nations recognizing the strategic potential of offensive cyber capabilities. The 2007 cyber attacks on Estonia, widely attributed to Russia, served as a wake-up call to the international community, highlighting the potential for cyber operations to disrupt an entire nation's digital infrastructure.

As cyber threats evolved, so too did international responses. The early 2000s saw the first attempts at global cooperation in cybersecurity, with the Council of Europe's Convention on Cybercrime (Budapest Convention) in 2001 marking a significant milestone. This treaty, which

---

[1] "Rising Cyber Threats Pose Serious Concerns for Financial Stability." 2024. IMF. April 9, 2024. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.

[2] "Digital Breakthroughs Must Serve Betterment of People, Planet, Speakers Tell Security Council During Day-Long Debate on Evolving Cyberspace Threats | Meetings Coverage and Press Releases." 2024. June 20, 2024. https://press.un.org/en/2024/sc15738.doc.htm.

aimed to harmonize national laws and improve investigative techniques, represented the first international agreement on crimes committed via the Internet, and the following years witnessed an increase in bilateral and multilateral agreements on cybersecurity, as well as the establishment of national cyber defense units and Computer Emergency Response Teams (CERTs) in many countries.[3] The creation of the NATO Cooperative Cyber Defence Centre of Excellence in 2008 further underscored the growing recognition of cybersecurity as a critical component of national and international security.[4]

The United Nations has played a pivotal role in addressing cybersecurity challenges at the global level. In 2003, the UN General Assembly adopted Resolution 58/32, which called for examining existing and potential threats to information security.[5] This was followed by the establishing of the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security in 2004. The GGE has since produced several influential reports, most notably in 2013 and 2015, which affirmed the applicability of international law to cyberspace and proposed norms of responsible state behavior. In 2018, the UN General Assembly established two parallel processes - a new GGE and an Open-Ended Working Group (OEWG) - to continue discussions on cybersecurity. These initiatives have been instrumental in fostering dialogue, building consensus, and developing frameworks for international cooperation in addressing the ever-evolving landscape of global cyber threats.[6]

Current State of Global Cybersecurity

A diverse array of sophisticated and evolving challenges characterizes the contemporary landscape of cyber threats. State-sponsored cyber operations, ranging from espionage to sabotage, have become increasingly prevalent and complex. These attacks often target government institutions, defense systems, and strategic industries, potentially compromising national security and economic stability. Simultaneously, cybercriminal organizations have grown in both scale and capability, launching devastating ransomware attacks that can paralyze entire sectors. The rise of Advanced Persistent Threats (APTs) has introduced a new level of persistence and stealth in cyber attacks, often remaining undetected in systems for extended periods.[7] Moreover, the proliferation of Internet of Things (IoT) devices has exponentially expanded the attack surface, introducing vulnerabilities in everything from smart home systems to industrial control mechanisms. Supply chain attacks, exploiting the interconnected nature of global commerce, have emerged as a particularly insidious threat, allowing malicious actors to compromise multiple targets through a single point of entry.

---

[3] "Budapest Convention." 2024. Cybercrime. February 8, 2024. https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[4] "CCDCOE - the NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defence Expertise." n.d. https://ccdcoe.org/.
[5] United Nations. 2003. "Developments in the Field of Information and Telecommunications in the Context of International Security." Report A/RES/58/32. *United Nations*. https://documents.un.org/doc/undoc/gen/n03/454/83/pdf/n0345483.pdf.
[6] "CCDCOE." n.d. https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/.
[7] "Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA." n.d. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors.

The impact of these cyber threats on critical infrastructure and essential services cannot be overstated. Power grids, water treatment facilities, healthcare systems, and transportation networks are increasingly vulnerable to cyber attacks, with potentially catastrophic consequences for public safety and national security. The 2021 Colonial Pipeline ransomware attack in the United States, which led to fuel shortages across multiple states, starkly illustrated the far-reaching implications of cyber incidents on critical infrastructure.[8] In essential services, the healthcare sector has become a prime target, with hospitals facing ransomware attacks that can disrupt life-saving care. Financial systems, too, are under constant threat, with cyber attacks capable of destabilizing markets and eroding public trust in financial institutions. The challenge of securing this shared digital infrastructure is compounded by several factors: the rapid pace of technological change, which often outstrips security measures; the inherent complexity of interconnected systems, which creates unforeseen vulnerabilities; and the global nature of cyberspace, which complicates jurisdictional and regulatory efforts. Moreover, the asymmetric nature of cyber warfare, where small groups can wield disproportionate power, presents unique challenges for traditional security paradigms. As our reliance on digital infrastructure grows, addressing these vulnerabilities and developing robust, adaptive cybersecurity measures has become critical for governments and organizations worldwide.

International Cybersecurity Frameworks and Initiatives

The United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security has been a cornerstone of international efforts to address cybersecurity challenges since its inception in 2004. The UN GGE has convened six times, bringing together experts from various countries to discuss norms of responsible state behavior in cyberspace, the application of international law to cyber operations, and confidence-building measures. The group's most significant achievements include the 2013 and 2015 consensus reports, which affirmed that existing international law applies to cyberspace and outlined a set of voluntary, non-binding norms for responsible state behavior.[9] These norms include prohibitions on damaging critical infrastructure, protecting Computer Emergency Response Teams (CERTs), and cooperating in investigating cyber attacks. Despite facing challenges in reaching consensus in recent years, the UN GGE remains a crucial forum for diplomatic dialogue on cybersecurity issues, fostering understanding and promoting stability in the digital realm.

The Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001, represents the first international treaty to address cybercrime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.[10] The convention covers various cybercrimes, including illegal access, system interference, and computer-related

[8] "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years | CISA." 2023. Cybersecurity and Infrastructure Security Agency CISA. May 7, 2023. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[9] "CCDCOE." n.d. https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

[10] "Budapest Convention." 2024. Cybercrime. February 8, 2024. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

fraud.[11] It also establishes procedures for obtaining electronic evidence and facilitating mutual legal assistance among signatories. As of 2024, 68 states, including non-Council of Europe members like the United States, Japan, and Australia, ratified the Budapest Convention, making it the most far-reaching binding international instrument on cybercrime.[12] While the convention has been criticized for potential privacy concerns and implementation challenges in rapidly evolving technological landscapes, it remains a significant framework for international cooperation in combating cybercrime.

The Paris Call for Trust and Security in Cyberspace, launched by French President Emmanuel Macron in November 2018, represents a multi-stakeholder initiative to address cybersecurity challenges. Unlike the UN GGE or the Budapest Convention, the Paris Call is a non-binding declaration that brings together states, private sector companies, and civil society organizations. The initiative outlines nine principles for securing cyberspace, including protecting individuals and infrastructure, defending electoral processes, and promoting the widespread acceptance of international cyber norms.[13] As of 2024, the Paris Call has garnered support from over 1,000 signatories, including 80 states, 700 companies, and hundreds of civil society organizations.[14] While its non-binding nature limits its enforceability, the Paris Call has been instrumental in fostering dialogue and building consensus among diverse stakeholders on crucial cybersecurity issues. It is complementary to formal intergovernmental processes, promoting a more inclusive and comprehensive approach to global cybersecurity governance.

Challenges in Global Collaboration

The concept of sovereignty and jurisdiction in cyberspace presents a fundamental challenge in global cybersecurity collaboration. Unlike physical domains, cyberspace transcends traditional geographical boundaries, making applying conventional notions of state sovereignty difficult. This ambiguity often leads to conflicting claims of jurisdiction over digital infrastructure, data, and cyber activities. For instance, cloud storage services may house data in multiple countries, raising questions about which nation's laws apply. Similarly, the global nature of the internet means that cyber attacks can originate from one country, transit through several others, and impact targets worldwide, complicating legal and diplomatic responses. Some nations advocate for a state-centric approach to internet governance, emphasizing their right to control information flows within their borders. In contrast, others push for a more open, globally interconnected model. This tension between national digital sovereignty and the inherently borderless nature of cyberspace continues to hinder the development of comprehensive international cybersecurity frameworks.

---

[11] "Budapest Convention." 2024. Cybercrime. February 8, 2024. https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[12] "Ad Hoc Committee on Cybercrime | Digital Watch Observatory." n.d. Digital Watch Observatory. https://dig.watch/processes/cybercrime-ad-hoc-committee.
[13] Co-Chairs, Introduction, Microsoft, F-Secure, and University of Florence. n.d. *Advancing International Cyber Norms: Multistakeholder Recommendations*. *Advancing International Cyber Norms: Multistakeholder Recommendations*. https://pariscall.international/assets/files/WG4-Final-Report-101121.pdf.
[14] "Paris Call for Trust and Security in Cyberspace — Paris Call." n.d. https://pariscall.international/en/.

Attribution of cyber attacks remains one of the most persistent and complex challenges in global cybersecurity efforts. The anonymity and technical complexity of cyberspace make it exceedingly difficult to identify the perpetrators of cyber attacks conclusively. Sophisticated actors can use various techniques to obscure their origins, such as routing attacks through multiple countries, using compromised systems as proxies, or employing false flag operations to implicate innocent parties.[15] Even when technical evidence points to a particular source, proving the involvement of specific individuals, organizations, or state actors can be challenging. This difficulty in attribution complicates diplomatic responses, legal action, and the application of deterrence strategies. Moreover, the time-consuming nature of cyber forensics often conflicts with the need for rapid response to ongoing threats. The attribution challenge also raises questions about the burden of proof in international forums and the potential for misattribution leading to escalated conflicts.

Balancing national security concerns with the need for international cooperation presents another significant hurdle in global cybersecurity collaboration. Nations are often reluctant to share sensitive information about their cyber capabilities, vulnerabilities, or ongoing threats, fearing that such disclosure could compromise their security or strategic advantages.[16] This hesitancy can impede effective information sharing and coordinated responses to global cyber threats. Additionally, some countries view certain cybersecurity technologies and practices as dual-use, having both defensive and offensive applications, leading to export controls and restricted collaboration in research and development. Cyber capabilities for espionage further complicate matters, as nations must navigate the fine line between protecting their interests and maintaining diplomatic relations. There's also the challenge of reconciling different national approaches to internet freedom and content regulation with the need for a unified front against cyber threats.[17] Striking the right balance between protecting national interests and fostering the trust and transparency necessary for practical international cooperation remains a key challenge in global cybersecurity efforts.

Emerging Technologies and Their Impact

Emerging technologies are reshaping the cybersecurity landscape, introducing new capabilities and challenges. Artificial Intelligence (AI) and Machine Learning (ML) are increasingly deployed in cybersecurity systems, offering enhanced threat detection, automated response mechanisms, and predictive analytics.[18] These technologies can process vast amounts of data to identify patterns and anomalies far more quickly and accurately than human analysts, potentially revolutionizing cyber defense. However, they also present new vulnerabilities and can

[15] Tran, Delbert, J.D. Class of 2018, Yale Law School, Scott Shapiro, Joan Feigenbaum, Oona Hathaway, Allison Douglis, Jeff Guo, et al. 2018. "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack." *Yale Journal of Law & Technology*. Vol. 20. https://yjolt.org/sites/default/files/20_yale_j._l._tech._376.pdf.
[16] "Cybersecurity | Homeland Security." 2024. U.S. Department of Homeland Security. August 30, 2024. https://www.dhs.gov/topics/cybersecurity.
[17] United Nations. n.d. "Cyberconflicts and National Security | United Nations." https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security.
[18] Roshanaei, Maryam, Mahir R. Khan, and Natalie N. Sylvester. 2024. "Enhancing Cybersecurity Through AI and ML: Strategies, Challenges, and Future Directions." *Journal of Information Security* 15 (03): 320–39. https://doi.org/10.4236/jis.2024.153019.

be weaponized by malicious actors to create more sophisticated attacks. Quantum computing poses a significant threat to current encryption methods, potentially breaking widely used cryptographic algorithms and necessitating the development of quantum-resistant encryption.[19] This looming threat has spurred research into post-quantum cryptography to safeguard sensitive data in the long term. Simultaneously, the proliferation of Internet of Things (IoT) devices has dramatically expanded the attack surface for cyber threats. The IoT ecosystem introduces millions of potentially vulnerable endpoints into networks, often with limited security features, from smart home devices to industrial sensors. This expansion increases the potential entry points for attackers and raises the stakes of breaches, as cyber incidents could directly impact connected systems.[20] As these technologies evolve, they underscore the need for adaptive, forward-looking cybersecurity strategies to anticipate and respond to emerging threats in an increasingly complex digital ecosystem.

Case Study

The TRITON malware attack, discovered in 2017, represents a watershed moment in the evolution of cyber threats against critical infrastructure. This sophisticated attack targeted a Saudi Arabian petrochemical plant's safety instrumented systems (SIS), marking one of the first known instances where malicious actors demonstrated the intent and capability to manipulate industrial safety mechanisms directly.[21] The potential consequences of this attack were particularly alarming - had it been successful, it could have led to a catastrophic toxic gas leak or explosion, putting lives at risk and potentially causing severe environmental damage. The TRITON incident underscores the growing vulnerability of industrial control systems (ICS) and the potential for cyber attacks to have devastating real-world consequences.

What makes the TRITON attack especially relevant to the global cyber crisis is its attack vector and the lessons it imparts about securing shared infrastructure. The initial compromise was achieved through spear phishing, a technique that exploits human vulnerabilities rather than technical ones. This method of entry highlights the critical importance of comprehensive cybersecurity strategies encompassing technological defenses, human factors, and organizational processes.[22] The attack's success in penetrating the plant's systems also reveals the challenges in securing complex, interconnected industrial environments where various stakeholders - including equipment manufacturers, software providers, and maintenance contractors - all play a role in the overall security posture.

The TRITON incident is a stark reminder of the need for enhanced global cooperation in securing critical infrastructure. It demonstrates how vulnerabilities in one nation's industrial

---

[19] Baseri, Yaser, Vikas Chouhan, and Abdelhakim Hafid. 2024. “Navigating Quantum Security Risks in Networked Environments: A Comprehensive Study of Quantum-safe Network Protocols.” *Computers & Security*, May, 103883. https://doi.org/10.1016/j.cose.2024.103883.
[20] Institute for Defense & Business. 2021. “Cybersecurity and the Internet of Things (IoT) | IDB.” Institute for Defense and Business. February 1, 2021. https://www.idb.org/cybersecurity-and-the-internet-of-things/.
[21] Giles, Martin. 2024. “Triton Is the World’s Most Murderous Malware, and It’s Spreading.” *MIT Technology Review*, August 22, 2024. https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/.
[22] “Anatomy of the Triton Malware Attack.” n.d. Anatomy of the Triton Malware Attack. https://www.cyberark.com/resources/threat-research-blog/anatomy-of-the-triton-malware-attack.

systems can have far-reaching implications for global safety and security. The attack has prompted calls for more rigorous international standards for industrial cybersecurity, improved information-sharing mechanisms between countries and industries, and the development of global best practices for securing industrial control systems. Moreover, it highlights the importance of regular security audits, continuous monitoring of industrial networks, and improved communication channels between infrastructure operators and their technology suppliers. As nations increasingly rely on shared digital infrastructure for their critical operations, incidents like TRITON underscore the urgent need for a coordinated, global approach to cybersecurity that can effectively address modern cyber threats' complex, transnational nature.

The Way Forward

The path forward in addressing the global cyber crisis and securing shared infrastructure necessitates a multi-faceted approach that combines legal, technological, and diplomatic efforts. Strengthening international legal frameworks is crucial to establishing clear rules and consequences for malicious cyber activities. This involves updating existing treaties like the Budapest Convention to address emerging threats and potentially developing new binding agreements targeting state-sponsored cyber operations. Enhancing public-private partnerships is equally vital, as the private sector often owns and operates critical digital infrastructure. These partnerships can facilitate more effective information sharing, joint threat analysis, and coordinated response strategies. Government agencies can provide intelligence and resources, while private companies can offer technical expertise and rapid innovation. Promoting cyber norms and responsible state behavior remains a cornerstone of international cybersecurity efforts. Building upon the work of the UN GGE and initiatives like the Paris Call, the international community must continue to develop, refine, and advocate for norms that discourage destructive cyber activities and promote stability in cyberspace. This includes norms against attacking critical infrastructure, interfering with the internet's core functions, and conducting cyber operations that could escalate into kinetic conflicts. Crucially, these efforts must be accompanied by capacity-building initiatives to ensure that all nations, regardless of their level of technological development, can participate in and benefit from a secure cyberspace. By pursuing these strategies in tandem, the global community can work towards a more resilient, stable, and secure digital ecosystem that supports continued innovation and economic growth while mitigating the risks of cyber threats.

Conclusion

The global cyber crisis presents an unprecedented challenge to our interconnected world, demanding a coordinated and multifaceted response from the international community. As we have explored throughout this paper, the threats to our shared digital infrastructure are diverse, complex, and ever-evolving, ranging from state-sponsored attacks to sophisticated criminal enterprises. The TRITON malware attack on a Saudi petrochemical plant is a stark reminder of

the potential real-world consequences of cyber threats, highlighting the urgent need for robust protection of critical infrastructure.

International initiatives such as the UN Group of Governmental Experts, the Budapest Convention on Cybercrime, and the Paris Call for Trust and Security in Cyberspace have laid important groundwork for global cooperation. However, significant challenges remain, including issues of sovereignty in cyberspace, attribution of attacks, and balancing national security with international collaboration. The rapid advancement of technologies like artificial intelligence, quantum computing, and the Internet of Things further complicates cybersecurity, introducing new vulnerabilities even as they offer potential solutions.

As we move forward, it is clear that securing our shared digital future will require a concerted effort from all stakeholders - governments, private sector entities, civil society organizations, and individual citizens. Strengthening international legal frameworks, enhancing public-private partnerships, and promoting responsible state behavior in cyberspace are critical steps toward building a more secure and resilient global digital ecosystem. We aim to address the global cyber crisis effectively and ensure that the digital realm remains a force for progress and prosperity rather than a vector for conflict and instability only through sustained cooperation, innovation, and commitment to shared norms and values. The path ahead is challenging, but we can work towards a safer, more secure cyberspace for all with collective action and shared responsibility.

Guiding Questions for Research

1. What is your country's current cybersecurity policy and infrastructure?
2. How has your nation been affected by or responded to major cyber incidents in the past?
3. What international cybersecurity agreements/initiatives has your country participated in?
4. How does your country balance national security interests with international cooperation in cyberspace?
5. What is your nation's stance on the application of international law to cyberspace?

Guiding Questions for Debate

1. How can the international community effectively attribute and respond to state-sponsored cyber attacks?
2. What measures can be taken to reduce the digital divide and ensure equitable access to cybersecurity resources globally?
3. How can we strengthen international legal frameworks to address emerging cyber threats while respecting national sovereignty?
4. What role should the private sector play in securing critical shared infrastructure, and how can public-private partnerships be enhanced?
5. How can the UN promote the development and adoption of universal cyber norms and responsible state behavior in cyberspace?