BIPSS Commentary

www.bipss.org.bd March -2025

BIPSS
Towards a Secure World

Cyber Warfare in Global Politics: The Evolving Landscape of Inter-State Conflict

Abida Farzana Muna[1]

Introduction

In the 21st century, cyber warfare has emerged as a critical component of inter-state conflict which is reshaping global security dynamics. Cyber warfare is using digital attacks by nations or state-sponsored groups to disrupt, damage or manipulate another country's critical infrastructure, data or communications networks. Unlike traditional warfare, which relies on physical force mainly, cyber warfare operates in the digital realm with a target on government institutions, financial systems, military operations and even civilian infrastructure[2]. Cyber capabilities have made cyberspace the newest battlefield, where nations compete for dominance without direct military confrontation. Cyber warfare has evolved significantly over the past few decades. Initially, it was limited to espionage and sabotage, with states using cyber tools to gather intelligence or disrupt adversary networks covertly[3]. However, modern cyber warfare has expanded into full-scale operations, influencing political, economic, and military strategies. The 2010 Stuxnet attack, which targeted Iran’s nuclear facilities demonstrates that cyber tools could inflict real-world damage. Since then, cyberattacks have played a crucial role in conflicts, from Russian cyber

[1] Abida Farzana Muna is a Research Assistant at Bangladesh Institute of Peace and Security Studies (BIPSS). She has completed her Bachelor of Social Science (BSS) in International Relations from Bangladesh University of Professionals.

[2] Hassan, Zohaib, Hamza Haroon, Ammara Khalid, and Sadaf Ghayoor. “Digital Warfare: The Evolution of U.S. and Russian Cybersecurity Strategies.” *Review of Education, Administration and Law* 7, no. 4 (December 4, 2024): 335–49. https://doi.org/10.47067/real.v7i4.386.

[3] Adeyeri, Aisha, and Hossein Abroshan. “Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era.” *Information* 15, no. 11 (November 1, 2024): 682. https://doi.org/10.3390/info15110682.

operations in Ukraine to Chinese cyber espionage targeting the U.S. and its allies[4]. The growing prominence of cyber warfare raises serious concerns for national security, global diplomacy and economic stability. Cyberattacks can cripple essential services, disrupt financial markets and even alter the course of elections. Understanding cyber warfare is crucial for nations to develop effective defense mechanisms, establish international regulations, and prevent large-scale digital conflicts that could destabilize the world[5].

The Rise of Cyber Warfare in Global Politics

Cyber warfare has its roots in the late 20th century when nations began exploring digital technologies for espionage and sabotage. As governments and critical infrastructures became increasingly reliant on digital systems, the potential for cyber-based attacks grew. The early 2000s saw the first major signs of cyber warfare, with states using cyber tools to infiltrate networks, steal sensitive data, and disrupt essential services[6]. However, it was not until the Stuxnet attack in 2010 that the world recognized the full potential of cyber warfare. Stuxnet, a sophisticated malware allegedly developed by the U.S. and Israel, targeted Iran's nuclear program, physically damaging centrifuges and setting back its nuclear ambitions. This event marked the beginning of cyber warfare as a strategic tool in geopolitical conflicts[7]. Since Stuxnet, cyber warfare has played a significant role in international conflicts.

Russia's cyber operations in Ukraine, including the NotPetya attack in 2017, disrupted financial systems and critical services[8]. Similarly, China has engaged in widespread cyber espionage,

[4] Anwer, Aml. "Cybersecurity and Political Warfare: The Weaponization of Information in the Digital Age" 1, no. 2 (December 1, 2024). https://doi.org/10.56830/ijhmps12202402.

[5] Çalışkan, Esra Merve. "State Cyber Warfare: The Strategic Shift Towards Private Sector Targets." *Güvenlik Çalışmalari Dergisi*, December 23, 2024. https://doi.org/10.54627/gcd.1598923.

[6] Wan Rosli, Wan Rosalili. "Waging Warfare against States: The Deployment of Artificial Intelligence in Cyber Espionage." *AI and Ethics*, January 8, 2025. https://doi.org/10.1007/s43681-024-00628-x.

[7] Aleke, Ngozi Tracy, Ivan Zziwa, and Kwame Opoku-Appiah. "Nation-State Cyber Attacks on Critical Infrastructure." *Advances in Information Security, Privacy, and Ethics Book Series*, December 26, 2024, 143–68. https://doi.org/10.4018/979-8-3373-1102-9.ch005.

[8] Aaltola, Mika. "Russian Cyber-Enabled Diversions in the West," 95–116. Palgrave Macmillan, Cham, 2021. https://doi.org/10.1007/978-3-030-54602-1_4.

targeting U.S. government agencies and corporations to steal intellectual property[9]. Other notable incidents include North Korea's WannaCry ransomware attack and Iran's cyber-attacks on global energy sectors. Recognizing the power of cyber warfare, nations have integrated cyber operations into their military strategies. Many countries now have dedicated cyber forces, such as the U.S. Cyber Command and China's Strategic Support Force[10]. Cyber warfare is no longer an isolated threat, and it is a key element of modern conflict, shaping global politics and security strategies.

Cyber Weapons and Their Capabilities

Cyber weapons are digital tools designed to infiltrate, disrupt, or damage computer systems and networks. They come in various forms, each with distinct capabilities and purposes. Malware (malicious software) is one of the most common cyber weapons, used to infect systems and steal or corrupt data[11]. Ransomware encrypts a target's data and demands payment for its release, as seen in attacks like WannaCry and Ryuk. Distributed Denial-of-Service (DDoS) attacks overwhelm networks with excessive traffic, crippling websites, financial systems, and government platforms[12]. Another sophisticated category is Advanced Persistent Threats (APTs), in which attackers gain prolonged access to a system to conduct espionage or sabotage without detection.

[9] Kim, Jin-Yong. "The Sino-US Technological Competition and China's Industrial Espionage Strategy." *Saneop Boan Yeon-Gu Hakoe Nonmunji*, December 31, 2023. https://doi.org/10.33388/kais.2023.13.3.153.

[10] Chang, Zen. "Cyberwarfare and International Humanitarian Law." *Social Science Research Network*, March 1, 2017. https://doi.org/10.2139/SSRN.2973182.

[11] Kadari, Srinivasa Rao, G. Radhika, Meera Shekar, Rahul Shankar, and Ch. Madhu. "A Study on the Key Applications of Malware." *International Journal of Advanced Research in Science, Communication and Technology*, August 14, 2024, 481–85. https://doi.org/10.48175/ijarsct-19359.

[12] Khoirunnisa, Khoirunnisa, and Cristy Sugiati. "Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare." *Jurnal Public Policy* 10, no. 2 (April 28, 2024): 138. https://doi.org/10.35308/jpp.v10i2.9026.

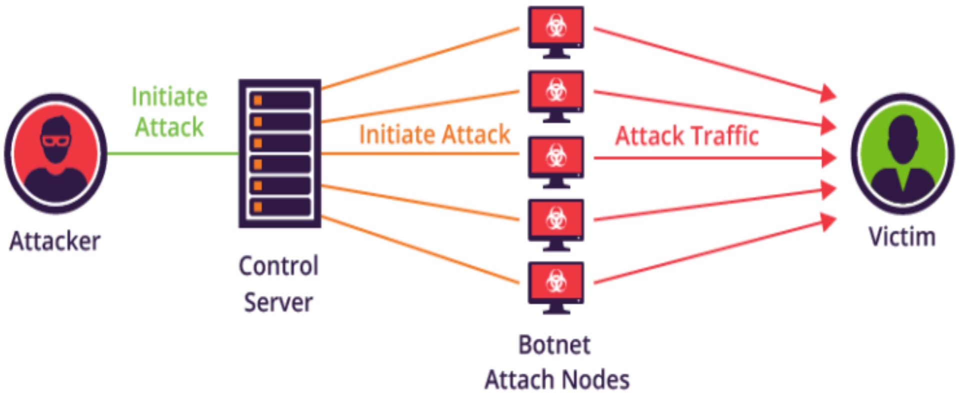

Figure: The Anatomy of DDoS, Source: securityboulevard

Cyber weapons are developed by state and non-state actors using a combination of software engineering, vulnerabilities in systems, and social engineering tactics. Governments invest heavily in cyber research to develop offensive and defensive capabilities, with some nations maintaining elite cyber units dedicated to cyber warfare. These weapons can be deployed remotely, allowing nations to strike without revealing their identity[13]. False-flag cyber operations further complicate attribution, making it difficult to pinpoint the real attacker. Artificial Intelligence (AI) and automation are revolutionizing cyber warfare by enhancing attack precision, speed, and adaptability[14]. AI-driven cyber weapons can autonomously identify vulnerabilities and execute attacks with minimal human intervention. Machine learning algorithms are also being used to develop more advanced cyber defense mechanisms, leading to an ongoing digital arms race between attackers and defenders. As AI continues to evolve, cyber warfare will become even more sophisticated and unpredictable[15].

[13] Kallberg, Jan. Designer Satellite Collissions from Covert Cyberwar. Strategic Studies Quarterly. Spring 2012.

[14] Pedro Gonçalves, Carlos. 'Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats'. Edited by Evon Abu-Taieh, Abdelkrim El Mouatasim, and Issam H. Al Hadid, 17 June 2020. https://doi.org/10.5772/intechopen.88648.

[15] Whyte, Christopher. 'Problems of Poison: New Paradigms and "Agreed" Competition in the Era of AI-Enabled Cyber Operations'. *2020 12th International Conference on Cyber Conflict (CyCon)*, May 2020, 215–32. https://doi.org/10.23919/CyCon49761.2020.9131717.

State-Sponsored Cyber Attacks and Attribution Challenges

State-sponsored cyber-attacks have become a key strategy in geopolitical conflicts, allowing nations to engage in warfare without conventional military confrontation. These cyber operations frequently target critical infrastructure, government institutions, and private enterprises, resulting in widespread disruption. One of the most well-documented cases is Russia's cyber warfare against Ukraine[16]. Before the 2014 annexation of Crimea, Russian hackers launched cyber-attacks on Ukrainian government websites and power grids. In 2017, the NotPetya attack, widely attributed to Russian state actors, crippled Ukrainian institutions and spread globally, causing billions in damages[17]. Similarly, U.S.-China cyber conflicts have escalated over the years, with China accused of large-scale cyber espionage, including the 2015 Office of Personnel Management (OPM) breach, where sensitive data of 22 million U.S. government employees was stolen[18].

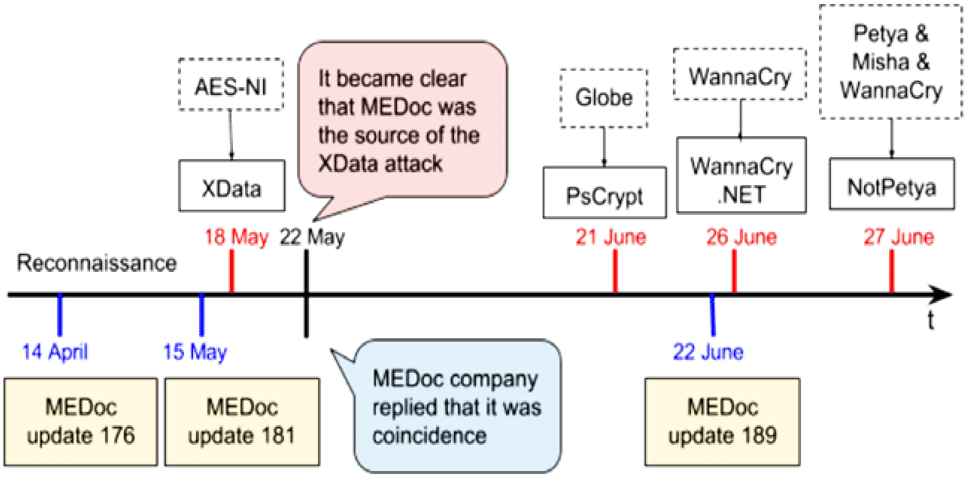

Figure: NotPetya attack through M.E.Doc

[16] Khoirunnisa, Khoirunnisa, and Cristy Sugiati. "Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare." *Jurnal Public Policy* 10, no. 2 (April 28, 2024): 138. https://doi.org/10.35308/jpp.v10i2.9026.

[17] Jenkinson, Andrew. "Digital Blood on Their Hands," December 15, 2022. https://doi.org/10.1201/9781003323273.

[18] Harvey, Sarah, and Diana Evans. "Defending Against Cyber Espionage: The US Office of Personnel Management Hack as a Case Study in Information Assurance," September 30, 2016.

One of the biggest challenges in cyber warfare is attribution—identifying the true source of an attack. Cyber operations can be conducted remotely, using sophisticated techniques to disguise the origin. Attackers often route operations through multiple countries, use stolen credentials, or employ false-flag tactics to mislead investigators[19]. This lack of clear attribution complicates diplomatic responses and can lead to misplaced retaliation or escalation of conflicts. False-flag cyber operations add another layer of complexity. Nations can launch cyber-attacks while making it appear as though another country is responsible, fueling misinformation and political tensions[20]. As cyber warfare evolves, the inability to attribute attacks with certainty increases the risk of unintended conflicts and deteriorates international trust.

The Role of Cyber Warfare in Geopolitical Conflicts:

Cyber warfare has become an essential tool in modern geopolitical conflicts, complementing traditional military strategies. Unlike conventional warfare, which relies on physical force, cyber operations allow nations to weaken adversaries by targeting critical infrastructure, communications, and military networks[21]. Cyberattacks are often used in conjunction with conventional warfare to disrupt enemy coordination, spread misinformation, and erode public morale. This strategy, known as hybrid warfare, integrates cyber operations with military actions to achieve strategic objectives without confrontation[22].

The Russia-Ukraine conflict is a prime example of how cyber warfare influences global conflicts. Since 2014, Russia has launched numerous cyber-attacks against Ukraine, targeting government institutions, power grids, and financial systems. The NotPetya malware attack (2017), believed to be a Russian operation, paralyzed Ukraine's infrastructure and inflicted economic losses

[19] Gootman, Stephanie. "OPM Hack: The Most Dangerous Threat to the Federal Government Today." *Journal of Applied Security Research* 11, no. 4 (September 8, 2016): 517–25. https://doi.org/10.1080/19361610.2016.1211876.

[20] Gootman, Stephanie. "OPM Hack: The Most Dangerous Threat to the Federal Government Today." *Journal of Applied Security Research* 11, no. 4 (September 8, 2016): 517–25. https://doi.org/10.1080/19361610.2016.1211876.

[21] Fedotenko, K. "Cyber Warfare as Part of Information Warfare of Russia against Ukraine since the Beginning of the 2022 Russian Invasion." *Věda a Perspektivy*, August 27, 2023. https://doi.org/10.52058/2695-1592-2023-8(27)-351-357.

[22] "Cyberwarfare." 2023. *Advances in Digital Crime, Forensics, and Cyber Terrorism Book Series*, May, 128–45. https://doi.org/10.4018/978-1-6684-6741-1.ch007.

worldwide. In the 2022 full-scale invasion, Russia used cyber-attacks to disable Ukrainian defense networks and spread disinformation, demonstrating how cyber warfare can be synchronized with ground operations[23].

Beyond military conflicts, cyber warfare is increasingly used for political destabilization and election interference. Foreign actors deploy cyber tactics to manipulate public opinion, spread disinformation, and undermine democratic institutions. The 2016 U.S. presidential election saw Russian cyber operatives hack emails and use social media disinformation campaigns to influence voter behavior. Similar tactics have been observed in European elections, raising concerns about digital interference in democratic processes[24]. As geopolitical tensions rise, cyber warfare will continue to shape global conflicts, making cybersecurity a crucial aspect of national defense and political stability.

Cybersecurity Strategies and Defense Mechanisms:

As cyber warfare becomes an integral part of global conflicts, nations have developed robust cybersecurity strategies to protect their critical infrastructure and digital assets. Governments implement multiple layers of security, including firewalls, encryption, intrusion detection systems, and threat intelligence networks. Firewalls act as the first line of defense, blocking unauthorized access, while encryption ensures that sensitive data remains secure even if intercepted. Advanced threat intelligence systems analyze cyber threats in real-time, allowing nations to predict and prevent attacks before they occur[25].

Several countries have established dedicated cyber defense agencies to combat cyber threats. The United States National Security Agency (NSA) plays a crucial role in cyber intelligence and

[23] Khoirunnisa, Khoirunnisa, and Cristy Sugiati. “Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare.” *Jurnal Public Policy* 10, no. 2 (April 28, 2024): 138. https://doi.org/10.35308/jpp.v10i2.9026.

[24] Lipton, Eric, David E. Sanger, and Scott Shane. ‘The Perfect Weapon: How Russian Cyberpower Invaded the U.S.’ *The New York Times*, 13 December 2016, sec. U.S. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[25] Roopesh, Ms. “Cybersecurity Solutions and Practices: Firewalls, Intrusion Detection/Prevention, Encryption, Multi-Factor Authentication” 4, no. 3 (July 25, 2024): 37–52. https://doi.org/10.69593/ajbais.v4i3.90.

defense, while the NATO Cyber Defense Center of Excellence helps member nations coordinate their cybersecurity efforts. China has developed a powerful cyber force within its Strategic Support Force (SSF), specializing in cyber espionage and defense[26]. These agencies actively monitor global cyber activities, defend against attacks, and conduct offensive cyber operations when necessary.

Figure: National Security Agency. Source: Intelligence.gov

In addition to government efforts, cooperation between the public and private sectors is essential for effective cybersecurity. Many cyber attacks target corporations, financial institutions, and infrastructure managed by private entities[27]. Tech companies, cybersecurity firms, and national security agencies must collaborate to share threat intelligence and strengthen cyber defenses. Global cooperation is also crucial, as cyber threats transcend national borders. Initiatives like the EU's Cybersecurity Act and U.S.-led international cybersecurity alliances highlight the need for joint efforts to combat evolving cyber threats[28]. With cyber warfare evolving rapidly, a unified

[26] Ayobami, Adedeji. "Global Cybersecurity Resilience: Advanced Strategies and Emerging Technologies for Protecting Critical Digital Infrastructure." *International Journal of Research and Innovation in Social Science* VIII, no. VIII (January 1, 2024): 1547–53. https://doi.org/10.47772/ijriss.2024.8080112.

[27] Simu, Sumiya Jahan, and Fardin Ibn Zaman. "Advanced Cybersecurity Strategies for Protecting Critical Infrastructure: Strengthening the Backbone of National Security." *International Journal of Scientific Research and Management*, December 13, 2023. https://doi.org/10.18535/ijsrm/v11i12.ec07.

[28] Adegbite, Abimbola Oluwatoyin, Deborah Idowu Akinwolemiwa, Prisca Ugomma Uwaoma, Simon Kaggwa, Odunayo Josephine Akindote, and Samuel Onimisi Dawodu. "Review of Cybersecurity Strategies in Protecting National Infrastructure: Perspectives from the Usa." *Computer Science & IT Research Journal* 4, no. 3 (December 24, 2023): 200–219. https://doi.org/10.51594/csitrj.v4i3.658.

global defense strategy is critical to maintaining cybersecurity and preventing large-scale cyber conflicts.

International Laws and Ethical Dilemmas in Cyber Warfare

Despite the growing threat of cyber warfare, there is a lack of comprehensive global regulations governing cyber conflicts. Unlike conventional warfare, which is regulated by international laws such as the Geneva Conventions, cyber warfare remains in a legal gray area[29]. Nations often disagree on defining cyber aggression, making it difficult to establish binding international treaties. As a result, countries continue to develop and deploy cyber weapons without clear legal or ethical constraints, increasing the risk of large-scale cyber conflicts[30].

Several international organizations, including the United Nations (UN), NATO, and the European Union (EU), have made efforts to regulate cyber warfare. The UN's Group of Governmental Experts (GGE) has worked to establish norms for responsible state behavior in cyberspace, advocating for the protection of critical infrastructure and civilian networks. NATO has recognized cyber attacks as a potential trigger for collective defense under Article 5, treating them on par with traditional military attacks[31]. The EU has also strengthened its cybersecurity policies through initiatives like the EU Cybersecurity Act, aiming to enhance cooperation among member states. However, these efforts remain non-binding, and enforcement mechanisms are weak[32].

Ethical concerns surrounding cyber warfare are another pressing issue. Cyber-attacks on civilian infrastructure, such as power grids and hospitals, can cause widespread harm and violate human

[29] Fletcher, Michael. "The Law of Cyber Conflict," 103–22. Oxford University Press eBooks, 2022. https://doi.org/10.1093/oso/9780197626054.003.0007.

[30] Bokil, Rohit. "Cyber Warfare: Taking War to Cyberspace and Its Implications for International Humanitarian Law." *International Journal For Multidisciplinary Research* 5, no. 1 (January 27, 2023). https://doi.org/10.36948/ijfmr.2023.v05i01.1494.

[31] Broeders, Dennis, and Fabio Cristiano. "Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road." *Social Science Research Network*, April 2, 2020. https://doi.org/10.2139/SSRN.3819171.

[32] Broeders, Dennis, Els De Busser, Fabio Cristiano, and Tatiana Tropina. "Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching towards Lines in the Sand?" *Journal of Cyber Policy* 7, no. 1 (February 18, 2022): 97–135. https://doi.org/10.1080/23738871.2022.2041061.

rights[33]. Additionally, state-sponsored cyber surveillance and data breaches pose significant threats to digital privacy. As cyber warfare evolves, nations must balance national security with ethical responsibility, ensuring that cyber conflicts do not escalate into humanitarian crises[34].

The Future of Cyber Warfare

As technology advances, cyber warfare is expected to become even more sophisticated, with Artificial Intelligence (AI), quantum computing, and deepfake technology playing a pivotal role. AI-driven cyber attacks can autonomously identify vulnerabilities and launch adaptive attacks with minimal human intervention[35]. At the same time, AI-powered cybersecurity tools will enhance defense mechanisms, creating a continuous battle between attackers and defenders. Quantum computing poses an even greater risk, as it has the potential to break traditional encryption methods, rendering current cybersecurity systems obsolete[36]. If nations achieve quantum supremacy, they could decrypt classified information, leading to a major shift in cyber warfare capabilities. Additionally, deepfake technology which creates hyper-realistic fake videos and audio could be weaponized for disinformation campaigns, election manipulation, and diplomatic deception[37].

These technological advancements are fueling a cyber arms race, where nations rapidly develop offensive and defensive cyber capabilities. Some experts predict a “digital Cold War”, where cyber warfare becomes the primary battleground for global superpowers, much like the nuclear arms race of the 20th century. Countries such as the U.S., China, and Russia are already investing

[33] “Navigating the Gray Area: A Comprehensive Analysis of Cyber Warfare and Its Relationship to the Law of Armed Conflict.” *Global Legal Studies Review* VII, no. III (September 30, 2022): 32–36. https://doi.org/10.31703/glsr.2022(vii-iii).05.

[34] Bobrowski, Krzysztof. “Conventional Attack vs Digital Attack in the Light of International Law” 10, no. 1 (April 21, 2021): 77–101. https://doi.org/10.21697/PRIEL.2021.10.1.03.

[35] Rahimi, Nick, and Henry Jones. ‘Cyber Warfare: Strategies, Impacts, and Future Directions in the Digital Battlefield’. *Journal of Information Security* 16, no. 2 (31 March 2025): 252–69. https://doi.org/10.4236/jis.2025.162013.

[36] Glorioso, Ludovica. “Cyber Conflicts: Addressing the Regulatory Gap.” *Philosophy & Technology* 28, no. 3 (March 20, 2015): 333–38. https://doi.org/10.1007/S13347-015-0197-8.

[37] nuagenetz. ‘Cyber Warfare: Explore the Implications of Technology in Modern Warfare’, 14 November 2024. https://nuagenetz.com/blogs/cyber-warfare-explore-the-implications-of-technology-in-modern-warfare/.

billions in cyber military infrastructure, making cyber dominance a key strategic objective[38]. To mitigate these growing threats, global cooperation is essential. International agreements, cybersecurity alliances, and information-sharing initiatives between governments and private sectors will be crucial in maintaining cyber stability. Without coordinated efforts, the risk of large-scale cyber conflicts could escalate, disrupting economies, political systems, and global security. The future of cyber warfare will depend on how nations navigate this evolving digital battlefield.

Conclusion

Cyber warfare has become a critical element of modern inter-state conflict, significantly influencing global politics, security, and diplomacy. As discussed, cyber weapons, from malware and ransomware to advanced persistent threats, are reshaping military strategies and disrupting both national infrastructure and international relations. The challenges of attribution, along with the growing role of AI and automation in cyber-attacks, highlight the complexity of defending against and responding to digital threats. State-sponsored cyber-attacks, such as those witnessed in the Russia-Ukraine and U.S.-China conflicts, have demonstrated the profound impact that cyber operations can have on geopolitics and national security. Given the evolving nature of cyber warfare, nations need to strengthen cybersecurity policies and develop comprehensive international agreements to regulate cyber conflicts. The absence of clear global regulations creates opportunities for cyber threats to escalate uncontrollably. Furthermore, global cooperation is critical to prevent large-scale cyber conflicts. Countries must work together to share intelligence, establish cybersecurity norms, and develop defense strategies that can mitigate digital threats. As cyber warfare becomes more integrated into global politics, the world's ability to address and prevent devastating cyber conflicts will depend on collaboration, trust, and proactive action in cyberspace. Ensuring a secure digital future is not just a national priority, but a collective global responsibility.

[38] Hauqe, Ziaul. 'Nation-State Cyber Attacks: Are You at Risk?' The Business Standard, 4 April 2025. https://www.tbsnews.net/thoughts/nation-state-cyber-attacks-are-you-risk-1107981.