*The Shivapuri*

Volume: XXVI, 2025

DOI: https://doi.org/10.3126/shivapuri.v26i1.75831

Army Command and Staff College, Nepali Army

Shivapuri, Kathmandu, Nepal

# From Battlefield to the Servers: Cyber Warfare and the Conflicts

- ***Maj Ashok Gurung***

**Abstract**

Cyber warfare has emerged as a critical component of modern conflicts, influencing national security, military strategy, and global stability. This paper explores the evolution of cyber warfare from intelligence gathering during the Cold War to its current role in geopolitical conflicts. Key tactics include cyberattacks in the form of Distributed Denial of Service (DDoS) attacks, malware, and cyber-espionage, with case studies such as the Stuxnet attack and Russia's cyber offensives against Ukraine illustrating its impact. The research employs a mixed-method approach, incorporating case study analysis and qualitative data to assess cyber warfare's economic, psychological, and strategic consequences. Findings highlight the challenges of global cybersecurity coordination, the increasing sophistication of cyber threats, and the role of artificial intelligence in cyber defence. The study concludes that while cyber warfare has transformed modern conflicts, current international frameworks remain inadequate in mitigating threats. Strengthening global collaboration, investing in advanced cybersecurity strategies, and developing unified policies are essential to securing the digital battlefield.

**Keywords**

*Cyber Warfare, Digital Conflict, Cyberattacks, Cybersecurity, Artificial Intelligence, Cyber-Espionage, International Security*

## Introduction

In the modern era, cyber warfare has emerged as a pivotal domain of conflict, reshaping the dynamics of global power and national security. As Carr (2011) aptly states, "Cyber warfare is the art and science of fighting without fighting: of defeating an opponent without spilling their blood." This statement underscores the transformative nature of cyber warfare, where battles are fought in the digital realm, targeting critical infrastructure, military systems, and civilian networks. The growing dependence on digital technologies has made nations vulnerable to cyber-attacks, which are now a key tool for asserting geopolitical influence. Schreier (2015) highlights that states are not only engaging in cyber espionage and reconnaissance but are also developing offensive cyber capabilities, launching frequent attacks with disturbing regularity. The development of cyber warfare has fundamentally reshaped both military strategies and international relations. As cyber capabilities become more sophisticated, they have altered global power dynamics, prompting nations to strengthen their cyber defences and engage in strategic cyber espionage to protect their national security and geopolitical interests.

The Russia-Ukraine conflict exemplifies the growing significance of cyber warfare as an integral element of contemporary conflicts. From the Not Petya attack in 2017, which crippled Ukraine's' banking, energy, and government sectors, and inadvertently caused global disruption (Greenberg, 2018), and the recent Sandstorm attack in December 2023, which disrupted Ukraine's telecoms giant Kyivstar, cyberattacks have proven to be a potent weapon in hybrid warfare. These incidents

illustrate the growing significance of cyber warfare in contemporary conflicts, where digital tools are used to disrupt, destabilize, and demoralize adversaries.

This article examines the evolution of cyber warfare, its influence on contemporary conflicts, and the strategies needed to address emerging cyber threats. It argues that cyber warfare has significantly transformed the nature of conflict, creating new vulnerabilities that necessitate strong cybersecurity measures, global collaboration, and technological innovation. Through an analysis of historical trends, key case studies, and international cybersecurity initiatives, this study provides a comprehensive insight into the role of cyber warfare in modern conflicts and proposes recommendations for mitigating its risks.

**Research Design and Methodology**

This study employs a mixed-method approach, combining qualitative and quantitative research designs to explore the evolution, impact, and defence strategies of cyber warfare. The research is based on a desk study, utilizing secondary data from books, journal articles, reports, and online resources. The research adopts a descriptive and explanatory design, analyzing case studies of significant cyberattacks, such as the NotPetya malware attack and the Russia-Ukraine cyber conflict.

**The Evolution of Cyber Warfare: Cold War to Modern Conflicts**

Cyber warfare has redefined modern conflict, shifting from traditional kinetic battles to digital operations. Emerging during the Cold War, early cyber tactics focused on electronic surveillance and signals intelligence, with the U.S. and Soviet Union investing heavily in disrupting enemy communications. Though "cyber warfare" was not yet a formal concept, the progression of ARPANET in the 1960s exposed vulnerabilities in digital infrastructure (Norberg, 1998), and events like the 1988 Morris Worm attack, which infected approximately 10% of all internet connected machines at the time,

revealed the vulnerabilities of interconnected systems from the software-based attacks (Denning, 1999).

The post-Cold War era saw cyber operations integrated into military strategies. The integration of electronic warfare in Operation Desert Storm (1990–1991) signified cyber operations' role in military strategy (Libicki, 2009). The Kosovo War in 1999 demonstrated cyberattacks' ability to disrupt communication networks, while Estonia's 2007 DDoS attacks showcased the potential to paralyze national infrastructure (Rid, 2020). Furthermore, the 2010 Stuxnet malware attack, allegedly a U.S.-Israeli operation, proved cyber weapons could cause physical destruction, targeting Iran's nuclear program (Zetter, 2014). These incidents underscored the increasing character of cyber warfare in both military and political conflicts.

Since 2011, cyber warfare has become central to hybrid conflicts, with non-state actors and state-sponsored hackers using digital tools for strategic advantage. Russia's 2016 U.S. election interference blurred the line between cyber warfare and political manipulation (Sanger, 2018), while the 2017 NotPetya malware attack on Ukraine proved the potential for cyber operations to destabilize economies and governments (Greenberg, 2018). This is evident that the advancement of cyber warfare has fundamentally transformed the nature of modern conflict, introducing new vulnerabilities and challenges. The weaknesses revealed during the Cold War and early cyber incidents established the foundation for today's unconventional cyber conflicts. From its origins in Cold War-era electronic surveillance to the sophisticated cyber operations seen in the Russia-Ukraine conflict, cyber warfare has become a critical element of national and international security strategies. As cyber operations moved from surveillance and disruption to full-scale attacks on critical infrastructure, they reshaped modern warfare, blurring the lines between military and civilian targets.

**The Impacts of Cyber Attacks on Modern Conflicts**

Cyberattacks have become a pivotal tool in contemporary warfare, transforming cyberspace into a critical battleground. Unlike traditional conflict, cyber warfare employs digital tools for espionage, disruption, and destruction, targeting infrastructure, government systems, and private entities. Cyberattacks can be executed by different actors, such as criminal organizations, hacktivists, and even individual hackers. Rid (2013) emphasizes that the increasing integration of digital technologies into critical infrastructure has made cyberattacks a central element of modern warfare and conflict

The Russia-Ukraine conflict provides a compelling case study of the strategic use of cyberattacks in modern warfare. The NotPetya malware attack in 2017, attributed to Russian state-backed hackers, exemplifies the destructive potential of cyber warfare. Initially disguised as ransomware, NotPetya was a wiper malware designed to cause widespread disruption. It targeted Ukrainian critical infrastructure, including government firms, banks, and utilities, crippling the economy and sowing chaos. The attack also had global repercussions, affecting multinational companies like Maersk and Merck, demonstrating the far-reaching impact of cyber warfare (Greenberg, 2018). NotPetya highlighted how cyber operations can serve as non-kinetic tools to achieve geopolitical objectives, complementing traditional military tactics in hybrid warfare (Giles, 2016).

Another significant example is the 2022 cyberattacks on Ukraine, which included Distributed Denial of Service (DDoS) attacks and website defacements. These attacks targeted Ukrainian government websites and critical infrastructure, disrupting communication and spreading disinformation. The psychological effect was profound, as the attacks aimed to weaken public morale and erode trust in the Ukrainian government. The international community, including NATO and the European Union,

condemned these actions, underscoring the global risks posed by cyberattacks (Cherepanov, 2022).

The rise of cyber warfare has introduced new vulnerabilities and challenges. Cyberattacks have the potential to cripple critical infrastructure, propagate disinformation, and undermine governments, making them a powerful weapon in contemporary conflicts. As nations become increasingly dependent on digital technologies, their susceptibility to such threats grows, underscoring the urgent need for strong cybersecurity measures and global cooperation. The Russia-Ukraine conflict highlights the necessity of fortifying cybersecurity defences, particularly for essential infrastructure, and fostering international collaboration to combat the escalating risks posed by cyber warfare.

**Measures to Counter Emerging Cyber Warfare Threats**

Cyber warfare has developed as a significant threat to global security, targeting critical infrastructure, information systems, and political stability. To counter these risks, nations must strengthen defences, foster international cooperation, and leverage advanced technologies like artificial intelligence (AI). International bodies, such as the United Nations, play a critical role in establishing rules and accountability to manage cyber threats. However, existing international laws, such as the United Nations Charter and the Tallinn Manual, face challenges in addressing cyber threats due to their non-binding nature and vague definitions. For instance, the 2007 Estonian DDoS attacks disrupted critical infrastructure but were not classified as "armed attacks," highlighting the limitations of current legal frameworks (CCDCOE, 2024).

***International Legal and Policy Measures***

Several international frameworks attempt to regulate cyber warfare, yet their effectiveness remains limited. The United Nations Charter (1945) prohibits ‘the use of

force', but cyberattacks often fall into a legal gray area, as seen in the 2007 Estonian DDoS attacks. The Tallinn Manual (2013, 2017) provides guidelines on applying international law to cyber warfare but lacks legal binding authority (CCDCOE, 2024). Similarly, the UN Group of Governmental Experts (UNGGE) reports stress cyber accountability but lack enforcement mechanisms, as demonstrated by the 2020 Solar Winds cyberattack (Romm et al., 2020). Without stronger legal enforcement and consensus on defining cyber aggression, these measures remain insufficient in preventing state-sponsored attacks, in particularly, small developing nations.

While international permissible frameworks apply to all nations, small developing states often struggle with limited technical and institutional capacity to implement them effectively. These states remain highly susceptible to cyber threats due to insufficient cybersecurity infrastructure and weak enforcement mechanisms. To address these challenges, capacity-building initiatives, financial and technical assistance from international organizations, and stronger regional cooperation are essential (CCDCOE, 2024). Furthermore, developing states should advocate for a more inclusive international cyber governance model that considers their specific needs, ensuring they are not left defenceless in the evolving cyber warfare landscape.

***National Cybersecurity Strategies***

In reaction to cyber threats, nations have developed distinct cybersecurity strategies. The United States adopted the "Defend Forward" strategy, using proactive cyber operations to disrupt adversarial threats before they materialize (White House, 2023). The U.S. Cybersecurity and Infrastructure Security Agency (CISA) coordinates efforts between public and private entities to protect critical infrastructure (CISA, 2020). Similarly, the United Kingdom's National Cyber Security Centre (NCSC) Strategy emphasizes resilience, collaboration, and proactive defence, with initiatives like the National Cyber Force (NCF) conducting offensive cyber operations against state-

sponsored attackers (NCSC, 2020). Russia integrates cyber capabilities into its military doctrine, employing state-sponsored actors for espionage and disruption, while China enforces strict cybersecurity regulations and conducts cyber espionage operations targeting global industries (Giles, 2016; Ji, 2018). The European Union (EU) has also taken significant steps, such as the NIS2 Directive, which sets higher cybersecurity standards for critical sectors, and the establishment of the European Cybersecurity Industrial, Technology, and Research Competence Centre (ECCC) to enhance cyber capabilities (EU, 2020). NATO has updated its Cyber Defence Policy, affirming that a significant cyberattack could trigger Article 5, which considers “an attack on one member as an attack on all” (NATO, 2021). These diverse approaches illustrate the growing importance of cyber resilience in national security policies.

***Emerging Cybersecurity Measures***

Despite these efforts, cyber threats remain pervasive. The 2022 Russia-Ukraine conflict demonstrated the importance of international cyber assistance, with countries like the U.S. providing intelligence support to Ukraine. With support from Western allies, Ukraine enhanced its cybersecurity posture, maintaining operational continuity in critical sectors such as energy and telecommunications amid ongoing threats (Graham-Harrison & Borger, 2022). In addition, Ukraine formed the "IT Army," a volunteer group of tech experts and cybersecurity professionals, to counter Russian cyber activities (Kramer, 2022). Strengthening intelligence-sharing, conducting joint cyber exercises, and investing in AI-driven defence mechanisms are crucial for future cyber resilience.

Technological advancements, including artificial intelligence (AI), are reshaping cyber defence. AI-driven threat detection enhances real-time responses to cyber threats, yet adversaries also exploit AI for automated attacks, deepfake propaganda, and sophisticated malware (Sharma & Kumar, 2022). This dual nature of AI underscores the need for robust ethical and legal frameworks to govern its use in cyber warfare. While

legal and national cybersecurity measures provide essential protections, the developing landscape of cyber warfare presents ongoing challenges. The lack of legally binding international agreements limits enforcement, and rapid technological advancements create new vulnerabilities. Strengthening global cooperation, refining cybersecurity frameworks, and establishing unified cyber defence protocols are essential for mitigating future cyber threats. Without proactive and collaborative efforts, cyber warfare will continue to threaten global stability.

**Recommendations**

The following major recommendations could be adopted by the international community to proactively mitigate the risks posed by cyber warfare and foster a collaborative approach towards building a more secure digital future:

***Strengthen National Cyber Defence***

Nations should focus on safeguarding critical infrastructure, including energy, healthcare, and communication systems, by investing in advanced cybersecurity technologies and promoting collaboration between governments and the private sector. The implementation of proactive defence strategies, such as the U.S. "Defend Forward" policy, demonstrates the effectiveness of early threat detection and preemptive cyber operations (White House, 2023).

***Enhance International Cooperation***

Establish legally binding international agreements with clear rules and enforcement mechanisms to address cyber threats. Promote information sharing, joint cyber exercises, and capacity-building initiatives, particularly for developing nations, can enhance global cybersecurity resilience (CCDCOE, 2024)

***Build Capacity for Vulnerable Nations***

Wealthier nations and global organizations should support developing countries with funding, training, and expertise to improve their cybersecurity. Setting up regional centres can help share knowledge, foster partnerships, and train skilled professionals, reducing the gap between well-equipped and less-equipped nations.

***Develop Robust Legal Frameworks***

Revise and clarify international laws, including the United Nations Charter and the Tallinn Manual, to effectively address the distinct challenges of cyber warfare. Establish clear definitions of "use of force" in cyberspace and implement accountability measures for cyberattacks.

***Leverage Emerging Technologies***

Using AI-powered cybersecurity can greatly improve real-time threat detection and system protection against new risks. However, it is essential to implement strict ethical guidelines to prevent the misuse of AI in offensive cyber operations, ensuring the technology is used to defend rather than exploit digital systems.

***Promote Policy and Public Awareness Education Initiatives***

Governments should create clear cybersecurity plans that balance defensive and offensive strategies. Educating the public through campaigns and training programs to raise awareness about cyber hygiene and the risks of cyber-attacks making individuals and organizations more aware of online risks. Developing more cybersecurity experts is crucial to meet the increasing demand for skilled professionals (World Economic Forum, 2024).

**Conclusion**

The development of cyber warfare has changed the nature of modern conflicts, with digital battlegrounds becoming as strategically significant as physical ones. The

Russia-Ukraine conflict exemplifies the far-reaching impact of cyber operations, revealing critical gaps in cybersecurity frameworks and international legal enforcement. While technologically advanced nations have strengthened their cyber defences, many developing states remain vulnerable due to limited resources and inadequate infrastructure. Addressing these disparities requires enhanced global cooperation, targeted capacity-building initiatives, and adaptive cybersecurity policies. Moreover, the assimilation of artificial intelligence in cyber operations presents both challenges and opportunities, underscoring the need for pre-emptive defence mechanisms. Without coordinated international efforts, cyber warfare will continue to advance, posing an escalating risk to national security and global stability.

**References**

Carr, J. (2011). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media, Inc.

CCDCOE. (2024). The Tallinn Manual. The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/research/tallinn-manual/

Cherepanov, A. (2022, February 24). Russia's cyberattacks on Ukraine: A new front in the war. *TechCrunch*. Retrieved from https://techcrunch.com

Denning, D.E. (1998). *Information Warfare and Security*. *EDPACS, 27*, 1 - 2.

Giles, K. (2016). *Handbook of Russian Information Warfare*. NATO Defence College. Retrieved from https://www.ndc.nato.int

Graham-Harrison, E., & Borger, J. (2022). *How Ukraine's cyber defences are holding up against Russia*. The Guardian. Retrieved from https://www.theguardian.com

Greenberg, A. (2018). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Ji, C. (2018). Cybersecurity and Data Protection: A Study on China's New Cybersecurity Legal Regime and How It Affects Inbound Investment in China. *The International Lawyer*, *51*(3), 537–552. https://www.jstor.org/stable/27009643

Kramer, A. (2022). *Ukraine's IT army takes the fight to Russian cyber attackers*. The New York Times. Retrieved from https://www.nytimes.com

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation. Retrieved from https://www.rand.org/pubs/monographs/MG877.html

National Cyber Security Centre. (2020). *Cybersecurity: The UK's strategic approach to national resilience*. Retrieved from https://www.ncsc.gov.uk

NATO. (2021). *Cyber defence*. NATO. Retrieved January 28, 2025, from https://www.nato.int/cps/en/natohq/topics_78170.htm

Norberg, A. L. (2005). *Computers and Commerce: A Study of Technology and Management at Eckert-Mauchly Computer Company, Engineering Research Associates, and Remington Rand, 1946-1957*. MIT Press.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Romm, T., Nakashima, E., & Timberg, C. (2020). SolarWinds hack: An unprecedented cyberattack.

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Crown Publishing Group.

Schreier, F. (2015). *On Cyberwarfare*. DCAF HORIZON. Retrieved from www.dcaf.ch

Sharma, R., & Kumar, S. (2022). Artificial intelligence in cybersecurity: A review of recent advancements and challenges. Journal of Cyber Defence Studies, 8(3), 45-59.

Strategic Cybersecurity Talent Framework: White Paper (2024, April). *World Economic Forum*. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

The EU's Cybersecurity Strategy for the Digital Decade. (2020, December 12). https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

White House. (2023). *National Cybersecurity Strategy*. Retrieved from https://www.whitehouse.gov

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishing Group.