BIPSS Commentary
www.bipss.org.bd February -2025
BIPSS Towards a Secure World

Cyber Warfare in 2024: Are We Headed towards a Global Cyber Arms Race?

Saraf Wasima[1]

Source: The International Institute for Strategic Studies

Introduction

Warfare has evolved in the twenty-first century from physical battlefields into an invisible but very significant arena: cyberspace. Nations are increasingly participating in cyberwarfare, employing digital means to do damage, and strategic disruptions against enemies, transcending traditional

[1] Saraf Wasima is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS & MSS in International Relations from the Bangladesh University of Professionals (BUP)

military confrontations. This change has reshaped world security, erasing boundaries between war and peace, confusing state actors and cybercriminals, and offence and defence.[2]

From financial disruptions and election tampering to major infrastructure strikes, cyberwarfare has evolved into a main tool in geopolitics. States can use the cyberspace to exercise asymmetric power, therefore empowering even tiny countries and non-governmental entities to oppose world superpowers. The speed, anonymity, and potential of this new kind of warfare to cause broad disturbance without direct physical conflict define it. Cyberwarfare is one of the most urgent security issues of our day since it is likely to become more important in determining international power dynamics as world tensions rise.

Source: Threat Tec

The Rise of Cyber Warfare – How Nations Are Shifting from Conventional to Digital Combat

A modern extension of traditional military conflict, cyber warfare has profoundly altered the manner in which nations engage in power struggles.[3] Wars historically were fought on land, sea, and air with well-defined battle zones and obvious frontlines. But in the linked world of today, digital battlefields span national boundaries and allow enemies to launch strikes from thousands of miles distant without ever touching ground.

[2] Limnéll, Jarno. "The cyber arms race is accelerating–what are the consequences?." *Journal of Cyber Policy* 1, no. 1 (2016): 50-60.
[3] Healey, Jason. "Cyber Effects in Warfare: Categorizing the Where, What, and Why (Fall 2024)." (2024).

Several main elements have sped the change from traditional to digital warfare:

Unlike conventional warfare, which needs for large-scale military infrastructure and investment, cyberwarfare gives smaller states and renegade players an asymmetric advantage and low cost of entrance. Cyber agents with few resources can compromise financial institutions, destroy government systems, and disturb vital infrastructure.[4]

Plausible Deniability: Cyberattacks sometimes hide the identities of offenders, therefore challenging attribution. Often operating under layers of obscurity, state-sponsored hackers let governments deny involvement while nonetheless accomplishing strategic goals. As a result, mercenaries hacking for nations and proxy cyber groups have emerged.

Cyberwarfare is a tool for influencing elections, changing public opinion, and upsetting economies as much as it is for producing physical or digital damage.[5] Digital warfare is being applied to alter world political and economic results from Russia's meddling in Western elections to China's claimed cyber espionage targeting intellectual property.

Artificial intelligence and machine learning combined into cyberwarfare has made digital fighting even more complex. This is shown in cyberattacks. Real-time adaptation of AI-powered cyberattacks allows them to evade security systems, start automated phishing campaigns, and even create deepfake disinformation to an unparalleled extent.

[4] Kaloudis, Martin. "Digital Sovereignty as a Weapon of Diplomacy in Cyber Warfare in." *National Security in the Digital and Information Age* (2024): 17.
[5] Hansel, Mischa, Max Mutschler, and Marcel Dickow. "Taming cyber warfare: lessons from preventive arms control." *Journal of Cyber Policy* 3, no. 1 (2018): 44-60.

Source: Atlantic Council

Major Cyber Attacks in 2024 – Case Studies of Recent State-Sponsored Cyber Conflicts

Cyber battles surged in 2024 as state-sponsored strikes aimed targeted banking systems, national security networks, and critical infrastructure.

Energy Grid Attack (Eastern Europe): Blackouts and rising regional tensions resulted from a Russian-linked cybergroup damaging a nation's power system.

Financial Breach (U.S.: Millions of bogus transactions resulted from a cyber gang supported by North Korea using SWIFT weaknesses.[6]

Chinese-linked hackers broke through military systems in Southeast Asia to gather intelligence on naval activities in the South China Sea.[7]

Election disinformation (Latin America): traceable back to a foreign intelligence organisation, artificial intelligence-generated deepfakes affected voter attitude.

[6] Naseeb, Jannat, and Ahsan Tariq. "Impact of cyber-attacks on national security and international relations." *International Journal for Conventional and Non-Conventional Warfare* 1, no. 1 (2024): 86-96.
[7] Akoto, William. "International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks." *Journal of Peace Research* 58, no. 5 (2021): 1083-1097.

Ransomware on Government: Iranian hackers encrypted important databases, therefore interfering with diplomatic activities.[8]

Cyber Arms Race: Reality or Hype? – Evaluating the Global Race for Cyber Supremacy

Many people feel that countries are engaging in an unparalleled cyberarms race, where digital weapons are being produced, tested, and used exactly as traditional military assets have been in prior wars due of the fast militarisation of cyberspace. With committed forces emphasising both offensive and defensive cyber operations, nations including the United States, China, Russia, and Israel have greatly enlarged their cyberwarfare divisions. [9] Together with massive assaults on military networks, financial institutions, and essential infrastructure, these events point to a change towards a new kind of digital competitiveness.

Some analysts, meanwhile, contend that the cyberarms race is exaggerated. Cyber weapons are typically transient, always changing and needing regular updates to be efficient unlike conventional arms races. Lack of clear guidelines of engagement and the challenge to link attacks to particular countries help to prevent major cyber conflicts from fully developing. Furthermore discouraging factors against full-scale cyber warfare are mutual economic dependencies and the possibility of worldwide financial upheavals. Although cyberspace is clearly competitive, the character of cyberwarfare stays more of a continuing strategic fight than an all-out weapons race.

[8] Tay, Kai Lin. "Cyber Hype Versus Cyber Reality-How Severe Is The Threat That Chinese Cyber-Attacks Pose To United States' National Security?." (2019).
[9] Kshetri, Nir, and Nir Kshetri. "Global Cybersecurity: Key Issues and Concepts." *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies* (2016): 1-24.

Source:Sky News

Geopolitical Implications – How Cyber Warfare is Redefining International Relations

By giving countries fresh instruments for espionage, sabotage, and influence operations, cyberwarfare has profoundly changed the nature of world affairs. Unlike conventional battles requiring physical military presence, cyber operations let states exercise authority far away, generally without clear attribution. This change has caused a rearrangement of global power relations whereby non-governmental players and smaller countries may challenge established superpowers via cyberspace.[10]

Particularly between the U.S. and China, Russia and NATO, and regional countries like Iran and Israel, the emergence of cyber warfare has significantly heightened geopolitical tensions. Common tactics to undermine enemies without resorting to traditional combat are cyberattacks aiming at financial markets, energy infrastructure, and electoral systems. Allies like NATO and the Quad have thus enhanced their cyber defence projects, while organisations like the United Nations fight to create worldwide standards for ethical cyberspace behaviour.[11] Cyberwarfare is

[10] Saltzman, Ilai. "Cyber posturing and the offense-defense balance." *Contemporary Security Policy* 34, no. 1 (2013): 40-63.
[11] Eslam, Hisham, and Garima Tiwari. "Cyberspace: Reimagining Cybersecurity and Its Impact on State Sovereignty." In *Cybercrime Unveiled: Technologies for Analysing Legal Complexity*, pp. 93-112. Cham: Springer Nature Switzerland, 2025.

probably going to remain a significant tool of geopolitical manoeuvring in the lack of enforceable international rules.

Weaponization of AI and Cybersecurity – The Role of Artificial Intelligence in Modern Cyber Conflicts

Artificial intelligence (AI) is transforming cyberwarfare and enabling more complex attacks as well as more strong defences. Analysing enormous volumes of data, spotting weaknesses, and automating attacks with before unheard-of speed and accuracy, AI-powered cyber tools can AI-driven cyber weapons—such as autonomous malware that adapts to security measures, AI-generated phishing campaigns that mimic human behaviour, and machine-learning models that improve cyber-espionage operations—are being used by nation-states increasingly.[12]

AI is also being applied, though, to enhance cybersecurity protections. Real-time identification and neutralising of cyber hazards led by artificial intelligence helps to lower response times and stop major breaches by so negating cyber threats. Investing in AI-based cybersecurity solutions, governments and businesses want to safeguard their digital assets against changing cyberattacks. Notwithstanding these developments, the weaponization of artificial intelligence raises ethical questions since autonomous cyber weapons might intensify conflicts without human control. The international community has to create ethical rules to stop inadvertent escalation as artificial intelligence shapes contemporary cyberwarfare.

[12] Nobles, Calvin. "The weaponization of artificial intelligence in cybersecurity: A systematic review." *Procedia Computer Science* 239 (2024): 547-555.

Source: Linkedln

Challenges in Cyber Defense – Can Nations Protect Their Digital Infrastructures?

Nations have increasing difficulty protecting their digital infrastructure as cyberattacks get increasingly complex. Cybercriminals and state-sponsored hackers aiming to cause operations to be disrupted, steal sensitive data, or change information often target government agencies, financial institutions, and operators of key infrastructure. Conventional cybersecurity policies are insufficient given the growing complexity of cyber threats—including supply chain exploits, zero-day vulnerabilities, and ransomware assaults.[13]

The absence of worldwide coordination and information-sharing between countries presents one of the main challenges in cyberdefense. Although cyberattacks are often global, multinational cybersecurity cooperation is still scattered. Many governments also battle antiquated cyberdefense strategies and inadequate cybersecurity expertise to properly handle new risks. Nations have to give cyber resilience a priority as more frequent and destructive cyberattacks call for strong public-private partnerships and proactive defence policies to guard their vital digital infrastructure from future attacks.

[13] Benouachane, Hassan. "Cyber Security Challenges in the Era of Artificial Intelligence and Autonomous Weapons." In *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*, pp. 24-42. CRC Press, 2025.

The Need for Global Cyber Regulations – Is International Cooperation the Only Way Forward?

The lack of worldwide rules controlling cyber operations poses a serious security threat as cyberwarfare turns into a main tool of geopolitical conflict. Unlike conventional warfare, in which international conventions like the Geneva Conventions set guidelines of engagement, cyberspace is still mostly unbridled. With little regard for legal repercussions, nations conduct cyber espionage, infrastructure attacks, and misinformation campaigns, therefore fostering a climate whereby digital wars may spiral out of control.[14]

Although various initiatives—such as the Budapest Convention on Cybercrime and the United Nations' attempts to create cyber norms—have been undertaken to solve this problem, worldwide cybersecurity collaboration remains disjointed. Enforcing universal rules is challenging since different nations see cyber sovereignty, intelligence collecting, and state-sponsored cyber operations differently. But the risk of unchecked cyber escalation rises without international coordination. Nations have to endeavour to create enforceable worldwide rules, enhance cross-border threat intelligence sharing, and create diplomatic channels for cyber conflict resolution if we are to stop cyber wars from spiralling into actual crises.

Future of Cyber Warfare – What Lies Ahead in the Next Decade of Digital Conflicts?

Driven by developments in artificial intelligence, quantum computing, and increasing digitisation of vital infrastructure, the next decade will probably see cyberwarfare change in several important ways. AI-powered cyber operations will grow more autonomous and hacks will be more exact and challenging to find. Once completely developed, quantum computing could make current encryption techniques outdated, so countries would have to reassess their cybersecurity plans. Furthermore, the spread of the Internet of Things (IoT) will bring fresh vulnerabilities since billions of linked devices provide a larger target for cybercrime and state actors.

[14] Reinhold, Thomas, and Christian Reuter. "Artificial Intelligence and Cyber Weapons." In *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*, pp. 335-349. Wiesbaden: Springer Fachmedien Wiesbaden, 2024.

With hybrid conflicts—where cyberattacks support conventional military operations—cyberwarfare is likewise projected to grow increasingly entwined. The Russia-Ukraine conflict has shown how concurrently with land fighting cyber operations may affect supply lines, infrastructure, and communication networks. Preemptive cyber operations meant to undermine rivals before physical hostilities start could rise as more countries acquire offensive cyber capabilities. Like in the Cold War, the next years will also test the efficacy of cyber deterrence strategies—that is, if the prospect of reprisals can stop major cyberattacks.

Conclusion – Are We Prepared for a Full-Scale Cyber War?

Though most countries still lack readiness for a full-scale cyberwar, knowledge of cyberthreats is expanding. Although companies and governments have enhanced cybersecurity policies, the fast development of cyberthreats implies that defensive capabilities usually follow behind offensive developments. Many nations lack the tools, trained workforce, and strategy frameworks needed to successfully offset state-sponsored cyber attacks.

Disruption of vital services such electrical grids, banking systems, healthcare networks, and communication infrastructure could result from a full-scale cyberwar. Unlike conventional warfare, in which harm is limited to battle areas, cyberwarfare might affect world economies and civilian populations much beyond the targeted objectives. The question is not whether cyberwarfare will intensify but rather how ready countries are to lessen its effects. Cyber resilience, international cooperation, and adaptive security measures must be given top priority going forward to make sure cyberspace does not turn into the new arena of combat unchecked worldwide.