

Cyber Warfare and Global Peace

§Shaibume, Benjamin, PhD & ¶Okpe, Ngbede Caleb

Abstract

The impact of cyber warfare on global peace is a pressing concern in today's interconnected world. As nations increasingly rely on cyberspace for critical infrastructure, economic activity, and communication, the potential for cyberattacks to disrupt international relations and exacerbate tensions grows. This paper delves into the intricate relationships between cybersecurity threats, interdependence, and global stability, examining the ways in which cyber warfare can undermine global peace using some selected cases such as Flame malware, Stuxnet, Sony picture hack, WannaCry Ransomware Attack, Russian interference with US 2016 election, Israeli Beeper Operations against Hezbollah among others. Through the lens of Complex Interdependence theory, this study reveals the complex dynamics at play in the digital age. Cyber warfare can disrupt international relations by compromising diplomatic communications, undermining trust, and creating tensions between nations. The interconnectedness of cyberspace creates new vulnerabilities, as infrastructure and systems become common targets for cyberattacks. To reduce these problems, the study recommends that, Countries should work together to create clear guidelines for cyber warfare, develop cyber security measures and strengthen international cooperation and information sharing. Building capacity and resilience in vulnerable countries is also important for promoting global stability and economic growth.

Keywords: cyberspace, cyberwarfare, global peace, international relations, digital communications

Introduction

The socioeconomic well-being, health, and life of every individual in a state are significantly dependent on the security of information

§ Dept. of Political Science, Benue State University, Makurdi, Nigeria.
benshacks2013@gmail.com

¶ Dept. of Political Science, Benue State University, Makurdi, Nigeria.

systems and electronic services. Cyber-attacks have a great impact on all sectors of the economy, hinder the proper functioning of the economic space, reduce public confidence in e-services and threaten the development of the economy through the use of information and communication technologies. Against the background of the existing global cyber threats, when cyber-attacks, cyber espionage, cyber terrorism, and disinformation are carried out on a daily basis, the development, introduction, and development of new defense mechanisms is an important issue.

According to Kumar and Somani (2018), cybersecurity encompasses two crucial dimensions: the vulnerabilities that arise from the rapid evolution of the digital environment, and the development of mechanisms, strategies, and protocols aimed at building a more secure digital ecosystem. It is a comprehensive field that integrates both technical and non-technical approaches to ensure the protection, integrity, and confidentiality of digital infrastructure and the sensitive data it processes. Cybersecurity thus involves proactive measures such as encryption, network monitoring, and access control, as well as human-centered initiatives like awareness training and policy formulation, all aimed at mitigating potential threats.

Similarly, Alazab (2020) emphasize that cybersecurity is not limited to technological safeguards but extends to governance structures, user behavior, and legal frameworks that collectively determine the resilience of digital systems. They argue that as cyber threats become more sophisticated, a multidimensional approach combining risk assessment, resilience planning, and continuous monitoring is necessary to protect individuals, organizations, and national assets from potential attacks. This recognition acknowledges the potential threats that can compromise the integrity of systems and data, while on the other hand, cyber-attack refers to deliberate actions taken by individuals, groups, or nation-states to compromise or exploit computer systems, networks, or

digital infrastructure with the intention of causing damage, theft, disruption, or unauthorized access to vital information.

Cyber-attacks can take various forms, including malware infections, phishing, distributed denial-of-service (DDoS) attacks, ransomware, or social engineering. The motivation for cyber-attacks can vary from financial interests to exploration, enforcement, or geopolitical interests. Cybersecurity, on the other hand, consists of actions and procedures to protect computer systems, networks and data from unauthorized access, damage, interruption or theft. This includes using technologies, policies and practices to prevent, detect and respond to cyber threats and vulnerabilities. Effective cybersecurity is a multi-layered approach, including network security, data encryption, access control, threat intelligence, incident response, and user awareness and understanding (Tushar and Ashok, 2017). The increasing reliance on technology and connectivity has made cyber security a major issue worldwide. In recent times, cyber-attacks by governments have become a common practice and a serious threat to international communications and security. According to the Center for Strategic and International Studies (CSIS), cyberattacks by governments have increased by 60 percent in the past six years, including China, Russia, Iran and North Korea in keynote speakers (CSIS, 2020). The scope and scale of these attacks show that cyber warfare is becoming a key tool in global warfare. Cyber security is essential to protect critical infrastructure, sensitive information and public systems from cyber threats. Government cyber-attacks are attempts by one government to infiltrate the networks and computer systems of another government for a variety of reasons, including espionage, disruption of critical infrastructure, and political interference. Cyber-attacks have significant consequences for national security, economic stability and foreign relations. In view of the above scenario this paper seeks to interrogate cyber warfare and its impacts on global peace.

Conceptual Clarification

Cyberwarfare: Cyber warfare refers to the use of digital attacks by state or non-state actors to disrupt, damage, or destroy the information systems of adversaries for political, economic, or military target. It operates through malicious software, denial-of-service attacks, hacking, and cyber espionage, targeting critical infrastructure such as power grids, financial systems, and government networks (Kello, 2013). Unlike conventional warfare, cyberwarfare transcends physical boundaries, allowing actors to project power globally while maintaining plausible deniability. This new form of conflict challenges traditional notions of sovereignty and warfare, as it often occurs below the threshold of armed conflict yet has the potential to cause strategic-level disruption and damages.

Cyberwarfare poses a growing threat to national and international security, blurring the line between war and peace. It enables asymmetric tactics where less powerful actors can inflict substantial damage on more technologically advanced states (Rid, 2012). The difficulty in attribution complicates retaliation and deterrence strategies, thereby encouraging further aggression in cyberspace. Furthermore, the lack of a universally accepted legal framework for cyber conflict exacerbates the challenges in holding perpetrators accountable. As states continue to weaponize cyberspace for geopolitical advantage, the need for robust cyber defense mechanisms and international cooperation becomes increasingly urgent (Tikk-Ringas, 2015).

Cyber-Security: Cyber security is the practices, technologies, and processes designed to protect networks, devices, programs, and data from unauthorized access, damage, or attack. It encompasses multiple dimensions, including network security, information security, application security, and operational security (Von Solms & Van Niekerk, 2013). As digital infrastructure becomes integral to economic, social, and political systems, cybersecurity is no longer just a technical issue but a vital component of national security.

Effective cybersecurity frameworks involve not only technical solutions like firewalls and encryption but also governance mechanisms, regulatory policies, and user awareness.

The growing sophistication of cyber threats ranging from state-sponsored espionage to organized cybercrime and hacktivism has exposed the vulnerabilities of both public and private digital infrastructures. A key challenge in cyber security lies in maintaining a proactive defense posture against constant evolving threats (Singer & Friedman, 2014). Moreover, the global nature of the internet complicates the enforcement of cybersecurity laws across jurisdictions, requiring international cooperation and harmonized regulatory standards. As societies become more interconnected and dependent on digital technologies, cybersecurity must be treated as a shared responsibility between governments, businesses, and individuals to ensure resilience and trust in cyberspace (Craig, Diakun-Thibault, & Purse, 2014).

Global Peace: Global peace in contemporary scholarship is broadly defined as a multidimensional condition in which societies experience the absence of large-scale violence and possess the institutional, social, and economic structures necessary to sustain harmony and cooperation. It extends beyond the mere cessation of armed conflict to include the establishment of systems that promote justice, equity, and collective security (Institute for Economics and Peace [IEP], 2024). In this sense, peace is not a static end state but a continuous process that involves maintaining and strengthening relationships among nations, communities, and individuals through dialogue, diplomacy, and mutual respect. Modern research increasingly views peace as a function of governance quality, inclusivity, and societal resilience rather than as the mere absence of war (Nesterova & Kim, 2024). Global peace encompasses not only negative peace the absence of direct violence but also positive peace, which involves structural conditions such as equity, good governance, social justice, and sustainable development that reduce the likelihood of future conflict. Achieving

and sustaining global peace remains a complex challenge in an era marked by geopolitical rivalries, ideological polarization, and transnational threats such as terrorism, climate change, and cyber insecurity. While institutions like the United Nations play a vital role in mediating conflicts and promoting diplomatic solutions, peace is often undermined by power politics, economic inequality, and weak international enforcement mechanisms (Boutros-Ghali, 1992). Moreover, peacebuilding requires more than conflict resolution it demands addressing root causes of violence, investing in education and development, and promoting inclusive dialogue across cultures and communities. In this sense, global peace is not merely the absence of war but the presence of conditions that support human flourishing and mutual coexistence.

Cyberattacks: Cyber-attacks are deliberate attempts to compromise the confidentiality, integrity, or availability of digital systems, networks, or data. They are executed through various methods, including malware, phishing, ransomware, denial-of-service (DoS) attacks, and unauthorized access to computer systems (Skopik et al., 2016). Cyber-attacks may be carried out by individuals, criminal organizations, hacktivists, or state-sponsored actors, targeting both public and private sectors. These attacks can disrupt essential services, steal sensitive information, or sabotage infrastructure, making them a critical threat in the digital age.

The increasing frequency and sophistication of cyber-attacks pose serious risks to global security, economic stability, and public trust. As societies become more dependent on digital technologies, the potential impact of cyber-attacks on critical infrastructure such as healthcare, energy, and financial systems grows exponentially (Carr, 2016). Furthermore, the anonymity of cyberspace complicates the attribution of attacks, hindering effective response and accountability. The evolving nature of cyber threats demands a shift from reactive to proactive cybersecurity strategies, enhanced

international cooperation, and legal frameworks capable of addressing cybercrime across borders (Tikk-Ringas, 2015).

Cyberspace: Cyberspace refers to the global, interconnected network of digital information systems, including the internet, telecommunications infrastructure, and computer networks, where data is created, exchanged, and stored. It is a virtual domain created by the interconnection of computers and digital devices, enabling communication, commerce, governance, and social interaction beyond physical boundaries (Libicki, 2007). Unlike traditional geographic spaces, cyberspace is intangible, dynamic, and constantly evolving, governed by both formal regulations and informal norms. It forms the backbone of the digital age, shaping modern life in unprecedented ways.

Cyberspace is both a domain of opportunity and a theater of conflict. While it enables innovation, global connectivity, and economic growth, it also exposes individuals and institutions to cyber threats such as espionage, disinformation, and cybercrime (Nye, 2011). The lack of clear international governance and the borderless nature of cyberspace make it difficult to enforce laws and norms, leading to jurisdictional ambiguities and regulatory gaps. As states and non-state actors increasingly assert their influence in cyberspace, it becomes imperative to establish global norms and cooperative mechanisms to ensure security, privacy, and digital rights in this contested domain (Mueller, 2010).

Theoretical Framework

This paper adopts complex communication theory as its framework of analysis. The theory argues that international relations are shaped by multiple channels of interaction among states and non-state actors, where military power is not the sole determinant of influence, and where issues such as economic, environmental, and technological concerns are just as important as traditional security matters (Keohane & Nye, 1977). In the context of cybersecurity, this theory emphasizes that no single actor can unilaterally

secure cyberspace or ensure global peace without cooperation. This is because cyber threats transcend borders and affect both military and civilian domains, global peace increasingly depends on diplomatic, economic, and technological interdependence. In cyberspace, mutual vulnerability creates shared interests, even among adversaries. For instance, both developed and developing countries rely on stable internet infrastructure for communication, commerce, defense, and governance. A cyberattack on global financial systems or digital health records can produce ripple effects across the world, harming even those not directly involved in the conflict. Complex interdependence thus explains why states might choose to cooperate through international cyber norms, treaties, or emergency communication channels rather than escalate tensions. The theory also explains why non-state actors (e.g., tech firms, NGOs, and civil society) are vital to global cyber governance, since they manage much of the infrastructure and innovation in cyberspace.

This theory is particularly relevant in the digital age, where states and non-state actors are deeply interconnected through information technologies, economic exchanges, and shared vulnerabilities in cyberspace.

Methodology

The study is qualitative in nature and employed the use of ex post facto survey research design. Data were collected from secondary sources of data such as books, journals, conference proceedings, internet sources and other relevant documents. Data was analysed using textual analysis. Textual analysis was employed for the presentation of information from books, journals, conference proceedings, internet sources and other relevant documents in a concise and logical manner.

Evolution of Cyber-warfare and Cyber-conflict

The evolution of cyber warfare and cyber conflicts mirrors the increasing dependence of modern societies on digital technologies. Initially, cyber activities were limited to espionage and information gathering, largely executed by intelligence agencies during the Cold War era. As early as the 1980s, state actors began to exploit computer systems for surveillance purposes, but these actions were largely covert and non-destructive (Healey, 2013). The 1990s saw the formalization of cyber capabilities, especially within military doctrines. Notably, the 1991 Gulf War demonstrated how information systems could be leveraged for military advantage, laying the groundwork for integrating cyber operations into conventional military strategies (Clarke & Knake, 2010). This era marked the transition from cyber espionage to strategic cyber warfare, where digital tools became instruments of national power.

The early 2000s witnessed a dramatic escalation in both the scale and sophistication of cyber conflicts. A turning point was the 2007 cyberattack on Estonia, widely regarded as the first instance of a state suffering a coordinated, large-scale cyber assault that paralyzed government, banking, and media systems (Ottis, 2008). This event demonstrated the ability of cyber operations to inflict societal disruption without kinetic warfare. In 2010, the discovery of Stuxnet, a sophisticated worm targeting Iran's nuclear program, marked the first known instance of a cyber weapon causing physical damage to critical infrastructure (Zetter, 2014). Unlike previous attacks, Stuxnet represented a new class of cyber weaponry designed not merely to spy or disrupt but to destroy. It highlighted the offensive potential of cyber tools and blurred the lines between cyber operations and acts of war.

In the last decade, cyber warfare has become increasingly asymmetrical and politicized. State and non-state actors now use cyber means for espionage, disinformation, sabotage, and influence operations. For instance, the Russian cyber interference in the 2016 U.S. presidential election showcased how digital platforms

can be weaponized to manipulate public opinion and destabilize democracies (Rid, 2020). Simultaneously, non-state actors such as hacktivist groups (e.g., Anonymous) and cybercriminal syndicates have exploited cyberspace for ideological and financial motives. The decentralization and low-cost nature of cyber tools allow weaker actors to challenge powerful states, making deterrence and attribution difficult. Today, cyber conflicts often unfold in the “gray zone” a space below the threshold of armed conflict, where states engage in persistent, low-intensity operations that erode norms without provoking conventional war (Mazarr, 2015).

The future of cyber warfare is increasingly complex, as artificial intelligence, quantum computing, and the Internet of Things (IoT) expand the attack surface. Military doctrines across the globe are adapting to integrate cyber capabilities into broader hybrid warfare strategies. The NATO Cooperative Cyber Defence Centre of Excellence and the U.S. Cyber Command are examples of institutional responses to growing cyber threats. However, international law has not kept pace with these developments, leaving a regulatory vacuum that complicates accountability and norms enforcement. As cyber operations become more integrated into geopolitical competition, the world must confront the challenge of establishing global norms and cooperative frameworks to manage cyber conflicts responsibly.

Cases of Cyber warfare and its Impact on Global Peace (Stuxnet, 2010).

Stuxnet (2010) is widely considered to be the first cyber weapon designed to cause physical damage to industrial systems. It was discovered in 2010 and is believed to have been created by the United States and Israel to target Iran’s nuclear program. Stuxnet was a highly sophisticated computer worm that was designed to target industrial control systems, specifically those used in Iran’s nuclear enrichment facilities. The worm was able to manipulate the speed of centrifuges used to enrich uranium, causing them to spin

out of control and leading to significant damage. The attack was carried out by infecting computers at the Natanz nuclear facility with the Stuxnet worm. The worm was able to spread quickly through the facility's network, eventually reaching the industrial control systems that operated the centrifuges (Stuxnet 2010). The impact of the Stuxnet attack was significant, with estimates suggesting that it set back Iran's nuclear program by several years. The attack also highlighted the potential for cyber weapons to be used to cause physical damage to industrial systems, leading to increased concerns about the security of critical infrastructure. The Stuxnet attack was also notable for its use of multiple zero-day exploits, which allowed it to spread undetected through the facility's network. The attackers also used a sophisticated method of networking, allowing it to transmit data back to its creators. The discovery of Stuxnet led to a significant increase in awareness about the potential for cyber-attacks on industrial control systems, and it is widely regarded as a turning point in the development of cyber warfare capabilities. In the aftermath of the attack, Iran took steps to improve the security of its nuclear facilities, including the implementation of new security measures and the creation of a cyber defense unit. The Stuxnet attack also led to increased tensions between the United States and Iran, with Iran accusing the United States and Israel of launching the attack. The incident highlighted the potential for cyber-attacks to be used as a tool of statecraft, and it has been cited as an example of the growing threat of cyber warfare.

Flame Malware

Flame was a highly sophisticated, modular cyber-espionage platform discovered in 2012 that targeted Windows systems across the Middle East and beyond; technical reverse-engineering revealed a toolkit of numerous plug-ins for audio capture, screenshotting, keylogging, network sniffing, and removable-media harvesting, making it one of the largest and most feature-rich pieces of malware

ever found (CrySyS Lab, 2012; Kaspersky Lab, 2012). Unlike sabotage-oriented malware such as Stuxnet, Flame's architecture prioritized long-term intelligence collection and stealth: its large codebase, use of SQLite storage, Lua scripting, and an extensive command-and-control infrastructure enabled persistent, targeted data exfiltration and remote reconnaissance (CrySyS Lab, 2012; Antiy Labs, 2012). Flame used multiple propagation and persistence mechanisms including exploitation of Windows vulnerabilities and USB autorun techniques — which allowed lateral movement within local networks and opportunistic spread to air-gapped environments via removable media (Kaspersky Lab, 2012; F-Secure, 2012). Because of its scale, resources evident in its development, and the geopolitical profile of its targets, security researchers and investigative journalists have treated Flame as likely state-sponsored, with open reporting linking it though not with absolute forensic proof to the same advanced actors associated with other nation-level toolkits (Rid, 2014; Sanger, 2012). The Flame case therefore illustrates critical issues for cyber policy and law: the rising sophistication of intelligence-grade malware, the problem of reliable attribution, and the normative and legal gaps that govern state conduct in cyberspace (Brookings Institution, 2012; Rid, 2014).

Sony Pictures Hack (2014)

The Sony Pictures Entertainment (SPE) hack in November 2014 remains one of the most consequential and politically charged cyberattacks in corporate history. The attackers, identifying themselves as the “Guardians of Peace” (GOP), infiltrated Sony's internal network through a spear-phishing campaign that deceived employees into granting access credentials, which were later used to install and propagate destructive malware (FBI, 2014; Symantec, 2015). The malware, known as Backdoor.Destover, was designed not only to exfiltrate massive volumes of data but also to wipe Sony's servers, rendering systems inoperable and halting

corporate operations for weeks (Symantec, 2015; FireEye, 2015). The attackers stole over 100 terabytes of data, including employee Social Security numbers, executive communications, confidential contracts, and unreleased film content, which were subsequently leaked online (Zetter, 2014).

Beyond its technical scope, the attack was marked by its psychological warfare dimension: the hackers publicly humiliated Sony through the release of personal emails, inflammatory executive exchanges, and threats of violence targeting theaters planning to screen *The Interview*, a satirical film about the assassination of North Korean leader Kim Jong-un (Nakashima & Warrick, 2014). The breach not only disrupted Sony's business operations but also generated intense media scrutiny and reputational damage, leading to the resignation of key executives, including co-chair Amy Pascal, and an estimated financial loss exceeding \$35 million (Swarts, 2015; Graham, 2017).

The U.S. Federal Bureau of Investigation (FBI) attributed the attack to North Korea, citing technical indicators such as code similarities, encryption keys, and command-and-control infrastructure shared with previous North Korean cyber campaigns like *DarkSeoul* (FBI, 2014; Rid & Buchanan, 2015). Although North Korea denied direct involvement, the regime praised the incident as a "righteous deed," underscoring the political undertones of the attack (BBC News, 2014). The Obama administration responded with heightened diplomatic pressure and additional economic sanctions targeting North Korean entities and individuals (White House, 2015). Scholars and analysts have since interpreted the Sony hack as a watershed moment in cyber conflict, demonstrating how state-sponsored or politically motivated cyber operations can blend espionage, coercion, and psychological influence (Healey, 2016; Valeriano & Maness, 2018). The event significantly influenced global cybersecurity policy, prompting corporations and governments to rethink cyber deterrence, information assurance, and incident response frameworks. It also reignited debates

over the thresholds for cyberwarfare and the legal attribution of state-sponsored attacks under international law (Nocetti, 2017). In retrospect, the Sony hack not only exposed corporate vulnerabilities in cybersecurity governance but also revealed the growing intersection of cyber operations, entertainment, and geopolitics in the digital age.

WannaCry Ransomware Attack (2017)

The WannaCry ransomware attack of May 2017 stands as one of the most disruptive and wide-reaching cyber incidents in history, affecting over 200,000 computer systems across more than 150 countries within just a few days (Europol, 2017; Symantec, 2018). The attack exploited a critical vulnerability in Microsoft Windows, known as EternalBlue, which had been originally developed as a cyber exploit tool by the U.S. National Security Agency (NSA) before being leaked online by the hacking group known as “Shadow Brokers” (Greenberg, 2017). Once deployed, the WannaCry worm rapidly self-propagated through networked systems, encrypting files on infected computers and displaying a ransom note demanding payments in Bitcoin ranging from \$300 to \$600 to unlock the data (Symantec, 2018; Newman, 2017). The scale and speed of the infection underscored the potential for malware to weaponize existing software vulnerabilities into a global crisis.

The attack had particularly severe consequences for public service infrastructures, most notably the United Kingdom’s National Health Service (NHS), where over 80 hospitals and health facilities experienced disruptions that led to the cancellation of surgeries, diverted ambulances, and delayed patient care (NHS Digital, 2018). Major multinational corporations such as FedEx, Nissan, Renault, Telefónica, and Merck also suffered significant operational downtime and financial losses (Kaspersky Lab, 2019). The ransomware’s reliance on the EternalBlue exploit demonstrated how leaked state-developed cyber tools could be

repurposed by malicious actors for mass exploitation, blurring the lines between state and non-state cyber operations (Healy, 2020).

Subsequent investigations by the United States, United Kingdom, and Australia attributed the attack to the Lazarus Group, a state-sponsored hacking organization linked to North Korea's Reconnaissance General Bureau (RGB) (U.S. Department of Justice [DOJ], 2018; FireEye, 2019). This attribution was consistent with the group's previous operations, such as the 2014 Sony Pictures hack and the 2016 Bangladesh Bank heist, both of which combined financial and political motives (Rid & Buchanan, 2015; Valeriano & Maness, 2018). North Korea denied involvement, but the international consensus underscored the growing trend of cyber coercion as a tool of geopolitical influence.

The Ukraine–Russia Conflict

The Ukraine–Russia conflict, beginning with Russia's full-scale invasion in February 2022, has become a defining example of cyber warfare integrated with kinetic military operations. The conflict has demonstrated how cyber operations can serve as both a precursor and an accompaniment to conventional warfare, targeting critical infrastructure, communications systems, and civilian services (Rid, 2023; Tikk & Kerttunen, 2023). In the months leading up to the invasion, Russia launched a coordinated series of cyberattacks against Ukrainian government ministries, financial institutions, and energy companies. These attacks included distributed denial-of-service (DDoS) campaigns and the deployment of data-wiping malware, such as WhisperGate and HermeticWiper, which aimed to disrupt government operations and sow confusion across the population (Microsoft, 2022; Mandiant, 2022). Analysts argue that these pre-invasion cyber operations were designed to weaken Ukraine's digital resilience and compromise command-and-control structures prior to the physical assault (EU Agency for Cybersecurity [ENISA], 2023).

As the conflict progressed, Ukraine mounted an unprecedented

cyber defense and counteroffensive. With support from NATO-aligned cyber units, private technology firms, and global volunteer groups such as the IT Army of Ukraine, Kyiv leveraged both state and non-state cyber capabilities to target Russian logistical systems, propaganda outlets, and military communication networks (Ben-Itzhak & Even, 2023; Zetter, 2022). Ukrainian hackers and their allied groups conducted hacktivist-style campaigns against Russian state media, defacing websites and leaking sensitive information to counter Russian disinformation efforts. These cyber countermeasures demonstrated Ukraine's adaptive use of digital tools in asymmetric warfare, blending military, civilian, and volunteer cyber operations into a hybrid defense ecosystem (Kostyuk & Zhukov, 2023).

Russia's cyber strategy, meanwhile, evolved toward more destructive and psychologically coercive objectives, deploying advanced wiper malware and ransomware variants to erase data, cripple critical infrastructure, and intimidate Ukrainian civilians (Check Point Research, 2023). Attacks on Ukraine's power grid, water systems, and communication networks particularly those in late 2022 and 2023 disrupted essential services and compounded the humanitarian crisis during winter months (Europol, 2023). These attacks illustrated the blurring boundaries between cyber operations and war crimes, as civilian infrastructure became a persistent target (UN Office for Disarmament Affairs [UNODA], 2024).

The Ukraine–Russia cyber conflict also underscored the internationalization of cyberspace hostilities, as state and non-state actors across the globe became involved. Western allies, including the United States, the European Union, and NATO, provided cyber defense assistance to Ukraine through threat intelligence sharing, incident response coordination, and capacity-building initiatives (NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], 2023). Simultaneously, reports have linked Chinese and Iranian hacker groups to Russian-aligned

operations, illustrating how cyber warfare has evolved into a multi-actor domain of global strategic competition (CrowdStrike, 2024; Treverton, 2023).

The “Beeper” Operation

The 2024 “Beeper Operation,” widely attributed to Israeli intelligence agencies, represents one of the most sophisticated examples of hybrid cyberwarfare in the modern era. The operation involved the detonation of thousands of pagers and communication devices distributed among Hezbollah operatives across Lebanon and parts of Syria. Reports indicate that the devices, originally believed to be secure communication tools, were embedded with small quantities of PETN explosives and detonated remotely, killing at least fifteen individuals and injuring over three thousand others (Reuters, 2024; The Guardian, 2024). The incident demonstrated Israel’s ability to infiltrate Hezbollah’s logistics and supply chains, converting ordinary communication technology into lethal weapons. According to RUSI (2024), the operation’s complexity suggested months of intelligence preparation and deep penetration of Hezbollah’s procurement networks, highlighting the convergence between traditional espionage, supply-chain sabotage, and cyber-enabled warfare.

The “Beeper” operation’s significance extends beyond its immediate tactical success. It showcased how cyber and intelligence operations can be integrated to produce physical, kinetic outcomes without the need for large-scale military engagement. As Al Jazeera (2024) notes, the attack effectively disrupted Hezbollah’s communication infrastructure and command systems, creating confusion and limiting operational coordination. This aligns with contemporary doctrines of “network-centric warfare,” where digital infiltration serves as a force multiplier. Cybersecurity analysts observed that the operation blurred the boundaries between cyberspace and the physical battlefield a hallmark of next-generation hybrid conflicts (Lieber Institute, 2024). The capacity

to manipulate hardware supply chains also underscores the growing vulnerability of globalized technology ecosystems, where adversaries can exploit interdependencies to achieve asymmetric strategic advantages (Wired, 2024).

Challenges of Cyberwarfare to Global Peace

In today's hyper-connected and digitalized world, cyberwarfare presents one of the gravest emerging threats to global peace, reshaping the nature of conflict and diplomacy in the 21st century. Unlike traditional warfare, cyberwarfare does not require boots on the ground or physical weaponry; it exploits the vulnerabilities of cyberspace to achieve political, economic, or military objectives, often below the threshold of declared war (Sanger, Perlroth, & Barnes, 2021). The increasing incidents of cyberattacks on critical national infrastructure, electoral systems, and multilateral organizations reflect how cyber conflict has become a tool for both coercion and chaos in international relations. The growing weaponization of digital technologies, if left unchecked, risks undermining the fragile architecture of global peace and security.

A primary and topical challenge posed by cyberwarfare is the crisis of attribution. In traditional warfare, aggressors are physically visible and identifiable, but in cyberspace, attacks can be anonymized, spoofed, or routed through multiple global servers, making it difficult to determine their source. For example, following the 2020 SolarWinds breach which compromised numerous U.S. government agencies and Fortune 500 companies, experts pointed to Russia's SVR intelligence service as the likely culprit, yet definitive attribution remained diplomatically contentious (Sanger, Perlroth, & Barnes, 2021). This ambiguity inhibits timely response, escalates mistrust between nations, and increases the risk of miscalculation. In an already polarized global order, false attributions or delayed reactions can trigger retaliatory actions, inadvertently intensifying conflict and undermining efforts at global peace.

Another major challenge is the absence of a universally agreed legal framework or binding norms governing state behavior in cyberspace. While the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) have attempted to propose norms of responsible state behavior, enforcement remains weak and compliance voluntary (UNODA, 2021). In the meantime, powerful states continue to develop offensive cyber capabilities without transparency or regulation. For example, both the U.S. and China have integrated cyber operations into their military doctrines, while Russia has used cyber tools to support its hybrid warfare strategy, notably in Ukraine since 2014 and again during its full-scale invasion in 2022 (Maurer, 2022). Without clear legal prohibitions or a cyber “Geneva Convention,” cyberspace remains a lawless frontier, allowing powerful actors to engage in digital aggression with impunity and thereby destabilizing global peace efforts.

Cyberwarfare also poses a direct threat to civilian populations and critical infrastructure, a violation of the traditional principles of distinction and proportionality in armed conflict. Recent cyberattacks, such as the 2021 ransomware attack on Colonial Pipeline in the United States, demonstrate how non-state actors can paralyze essential services, causing economic disruption and public panic (Department of Justice, 2021). Similarly, cyber operations targeting hospitals during the COVID-19 pandemic including those reported across Europe demonstrated a chilling disregard for human life and humanitarian norms (WHO, 2020). As digital interdependence grows, the capacity for cyberwarfare to disrupt food supply chains, electricity grids, financial markets, and emergency services has expanded dramatically. This not only undermines the well-being and security of populations but also creates fertile ground for political instability, regional conflicts, and transnational grievances conditions antithetical to lasting peace.

The emergence of asymmetric cyber capabilities further

complicates global security. While nuclear and conventional warfare are largely the preserve of major powers, cyberwarfare enables smaller states and non-state actors to wield disproportionate influence. Rogue states like North Korea have used cyberattacks for economic theft and sabotage, such as the 2017 WannaCry ransomware attack, which impacted systems in over 150 countries (Europol, 2018). Similarly, cyber mercenaries and ideologically motivated hackers operating with or without state sponsorship can disrupt diplomatic processes or fuel regional hostilities. This democratization of cyber power undermines traditional deterrence strategies and increases the frequency of low-intensity but high-impact conflicts that erode global peace.

Cyberwarfare contributes to a new digital arms race, where states prioritize the development of offensive cyber tools over cooperation and transparency. Investments in artificial intelligence-driven cyber weapons, zero-day exploits, and digital surveillance systems have surged globally, often without ethical oversight. Major powers like the U.S., China, Russia, and Israel are now engaged in a covert race to dominate cyberspace, often treating cooperation with suspicion and diplomacy as secondary. This undermines trust between nations and multilateral institutions, weakening the effectiveness of global peacebuilding mechanisms such as the United Nations, the African Union, and the European Union. Without mutual restraint and cyber arms control agreements, such unchecked escalation risks normalizing cyber conflict as a permanent feature of global politics.

Conclusion

Cyber warfare has emerged as one of the most profound and disruptive challenges to global peace and security in the twenty-first century. Unlike traditional forms of warfare confined to physical battlefields, cyber conflicts transcend borders and operate within a virtual domain that connects every aspect of modern life. The capacity of cyberattacks to paralyze critical infrastructure,

disrupt national economies, and manipulate political and social processes underscores their far-reaching implications. Beyond the immediate damage, cyber warfare erodes trust among nations, fuels geopolitical tensions, and complicates diplomatic relations due to the persistent difficulty of accurate attribution.

The anonymity and accessibility of cyberspace lower the barriers for both state and non-state actors to engage in aggression, thereby heightening the risk of miscalculation and unintended escalation. Despite growing recognition of these dangers, international consensus on norms, accountability, and regulation in cyberspace remains fragmented and weakly enforced. This underscores the urgent need for a coordinated global strategy that prioritizes resilience, transparency, and mutual trust. Achieving sustainable peace in the digital era requires more than defensive measures it demands a collective reimagining of international security. Strengthening global cooperation, establishing clear legal frameworks, and fostering cyber diplomacy are essential to curbing digital hostilities. Ultimately, safeguarding global peace in the age of cyber warfare will depend on humanity's ability to balance technological advancement with ethical responsibility, ensuring that cyberspace becomes a domain of cooperation rather than conflict.

Recommendations

1. Establishment of a Global Cybersecurity Treaty: A comprehensive international treaty on cybersecurity norms, rights, and responsibilities is essential to ensure stability and peace in the digital domain. Similar to the Geneva Conventions, such a treaty should define acceptable state behavior in cyberspace, explicitly prohibiting activities like attacks on civilian infrastructure, election interference, and the deployment of malware during peacetime. The absence of clear legal frameworks has enabled states to exploit ambiguities for malicious cyber operations. A

globally ratified treaty would introduce accountability mechanisms, promote transparency, and deter state-sponsored cyberattacks by establishing clear consequences for violations.

2. **Creation of a United Nations Cyber Peacekeeping Force:** The United Nations or an equivalent multilateral body should establish a Cyber Peacekeeping Force to maintain stability and trust in the digital sphere. Similar to traditional peacekeepers, these cyber units would monitor cyber conflicts, assist states under cyberattack, and help restore compromised digital infrastructure. This mechanism would be particularly vital in regions with fragile cybersecurity systems or ongoing geopolitical tensions. Cyber peacekeepers could serve as neutral mediators, facilitate crisis de-escalation, and coordinate post-attack recovery, thereby reinforcing the global community's collective commitment to peace and digital resilience (Maurer, 2022).
3. **Promotion of Multistakeholder Cyber Diplomacy:** Effective cyber governance must include non-state actors such as technology companies, civil society organizations, and academic institutions in cyber diplomacy processes. While states hold political authority, private entities manage and secure much of the world's digital infrastructure. Initiatives like the Paris Call for Trust and Security in Cyberspace and the Global Forum on Cyber Expertise exemplify platforms that promote inclusive and cooperative approaches. A multistakeholder model fosters shared responsibility, enhances transparency, and encourages the co-creation of cybersecurity norms, ultimately strengthening global trust and collaborative problem-solving in cyberspace.
4. **Strengthening Capacity Building and Cyber Solidarity:**

Global cybersecurity resilience depends on reducing technological and capacity disparities among nations. Many developing countries in Africa, Latin America, and Asia remain vulnerable due to limited cybersecurity expertise and infrastructure. International cooperation should prioritize technical assistance, training, and investment in these regions. Programs led by the International Telecommunication Union (ITU), the European Union, and bilateral partnerships can support the development of national cybersecurity frameworks. Strengthening the cyber capacity of weaker nations not only safeguards them from exploitation but also enhances collective global defense, embodying the principle of cyber solidarity.

5. **Development of Cyber Conflict Early Warning and Crisis Response Systems:** To prevent cyber conflicts before they escalate, there is a need for global cyber conflict early warning systems similar to mechanisms used for tracking natural disasters or pandemics. These systems should monitor and analyze cyber threats in real-time, alerting states to potential crises. Regional cybersecurity hubs supported by organizations such as the African Union, NATO, and ASEAN can collaborate to create an integrated global monitoring network. Such proactive systems would facilitate timely diplomatic interventions, reduce misperceptions, and establish crisis communication channels between rival states, thereby helping to sustain peace in an increasingly digital world.

REFERENCES

- Al Jazeera. (2024, September 18). How did Hezbollah get the pagers that exploded in Lebanon? Retrieved from <https://www.aljazeera.com/news/2024/9/18/how-did-hezbollah-get-the-pagers-that-exploded-in-lebanon>
- Antiy Labs. (2012). Analysis report on Flame worm samples. Antiy. Retrieved from <https://www.antiy.net/media/reports/flame-analysis.pdf>
- Associated Press. (2025, August 13). Norwegian police say pro-Russian hackers were likely behind suspected sabotage at a dam. AP News. Retrieved from <https://apnews.com/article/16673f35c17aac5ed871918136bdf6f>
- Bayerlein, M. (2024). From negative to positive peace: How norms relate to peaceful outcomes. *Journal of Peace Studies*, 61(2), 145–163.
- Boutros-Ghali, B. (1992). An agenda for peace: Preventive diplomacy, peacemaking and peace-keeping. United Nations. <https://www.un.org/en/ga/documents/>
- Brookings Institution. (2012). The Flame cyber espionage attack: Five questions we should ask. Retrieved from <https://www.brookings.edu/articles/the-flame-cyber-espionage-attack-five-questions-we-should-ask>
- Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43–62.
- CBS News. (2024, December 22). How Israel's Mossad tricked Hezbollah into buying explosive pagers. Retrieved from <https://www.cbsnews.com/news/israel-former-mossad-agents-detail-explosive-pagers-hezbollah-terrorists-plot-60-minutes-transcript>
- Center for Strategic and International Studies. (2020). Significant cyber incidents. <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>
- Check Point Research. (2023). Cyber attacks in the Ukraine–Russia war: Year two analysis. Check Point Software Technologies.
- Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. Ecco.
- Craigien, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21.

- CrowdStrike. (2024). Global threat report 2024: Cyber operations in the era of hybrid conflict. Retrieved from <https://www.crowdstrike.com>
- CrySyS Lab. (2012). sKyWIper (a.k.a. Flame): A complex malware platform (Technical report). Budapest University of Technology and Economics.
- Deibert, R. (2020). Reset: Reclaiming the internet for civil society. House of Anansi Press.
- Department of Justice. (2021). Justice Department recovers majority of Colonial Pipeline ransom. <https://www.justice.gov/opa/pr/justice-department-recovers-majority-colonial-pipeline-ransom>
- Durojaye, H., & Raji, O. (2022, December 13). Impact of state and state-sponsored actors on the cyber environment and the future of critical infrastructure. arXiv. Retrieved from <https://arxiv.org/abs/2212.08036>
- Europol. (2017). The WannaCry ransomware attack: A global wake-up call. Retrieved from <https://www.europol.europa.eu>
- Europol. (2018). WannaCry ransomware: A global cyberattack. <https://www.europol.europa.eu/publications-events/publications/wannacry-ransomware-global-cyberattack>
- FireEye. (2019). The Lazarus Group: North Korea's notorious APT. FireEye Threat Intelligence Report.
- F-Secure. (2012). Flame (Flamer, sKyWIper) — Technical summary. F-Secure Labs.
- Galtung, J. (1969). Violence, peace, and peace research. *Journal of Peace Research*, 6(3), 167–191
- Giles, K. (2023). Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine. Chatham House.
- Global Cyber Alliance. (2020). Annual report 2020: Reducing cyber risk globally. Retrieved from <https://www.globalcyberalliance.org>
- Graham, L. (2017). *Cybersecurity and cyberwarfare: What everyone needs to know*. Oxford University Press.
- Greenberg, A. (2017, May 17). How an NSA cyber weapon caused chaos around the world. *Wired*. Retrieved from <https://www.wired.com/story/eternalblue-nsa-wannacry>
- Healey, J. (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.

- Human Rights Watch. (2024, September 18). Lebanon: Exploding pagers harmed Hezbollah, civilians. Retrieved from <https://www.hrw.org/news/2024/09/18/lebanon-exploding-pagers-harmed-hezbollah-civilians>
- Institute for Economics & Peace. (2023). Global Peace Index 2023: Measuring peace in a complex world. Retrieved from <https://www.visionofhumanity.org/resources>
- Institute for Economics & Peace. (2024). Positive Peace Report 2024: Analysing the factors that build, predict and sustain peace. Retrieved from <https://www.visionofhumanity.org/wp-content/uploads/2024/04/PPR-2024-web.pdf>
- Ismail, M. (2017). Sony Pictures and the U.S. federal government: A case study analysis of the Sony Pictures Entertainment hack crisis using Normal Accidents Theory. *Information Technologies for Security*.
- Kaspersky Lab. (2012). Flame: The most complex malware ever discovered. Kaspersky Threat Research. Retrieved from <https://www.kaspersky.com/blog/flame/10431>
- Kaspersky Lab. (2019). WannaCry two years later: The legacy of the ransomware worm. Retrieved from <https://www.kaspersky.com>
- Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), 7–40.
- Kihan, R., & Nye, J. S. (1977). *Power and interdependence: World politics in transition*. Little, Brown and Company.
- Krampe, F., O'Driscoll, D., Johnson, M., Simangan, D., Hegazi, F., & de Coning, C. (2024). Climate change and peacebuilding: Sub-themes of an emerging research agenda. *International Affairs*, 100(3), 1111–1130.
- Kumar, S., & Somani, V. (2018). Cybersecurity: A comprehensive approach to secure the digital world. *International Journal of Computer Applications*, 182(25), 1–7.
- Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge University Press.
- Lieber Institute at West Point. (2024, October 11). “Well, it depends”: The Explosive Pagers Attack revisited. Retrieved from <https://lieber.westpoint.edu/well-it-depends-explosive-pagers-attack-revisited>
- Mandiant. (2022). Ukraine under attack: Wiper malware campaigns targeting critical infrastructure. Mandiant Threat Intelligence Brief.

- Maurer, T. (2022). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.
- Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict*. Strategic Studies Institute, U.S. Army War College.
- Microsoft. (2017). *The need for a Digital Geneva Convention*. Microsoft Official Blog. Retrieved from <https://blogs.microsoft.com>
- Microsoft. (2022). *Microsoft Digital Defense Report 2022*. Retrieved from <https://www.microsoft.com/security>
- Mohurle, S., & Patil, M. (2017). A brief study of WannaCry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5).
- Mueller, M. L. (2010). *Networks and states: The global politics of internet governance*. MIT Press.
- Nakashima, E., & Warrick, J. (2014, December 19). FBI blames North Korea for Sony cyberattack. *The Washington Post*. Retrieved from <https://www.washingtonpost.com>
- Nesterova, Y., & Kim, E.-J. (2024). Peace as social cohesion, equity, and democracy: Local peacebuilders' conceptualizations of peace. *Peace Review*, 36(1), 14–26.
- NHS Digital. (2018). *Lessons learned review: WannaCry cyber attack and the NHS*. Retrieved from <https://digital.nhs.uk>
- Nocetti, J. (2017). Contest and conquest: Russia and global internet governance. *International Affairs*, 93(6), 1327–1349.
- Nye, J. S. (2011). *The future of power*. PublicAffairs.
- Ottis, R. (2008). Analysis of the 2007 cyber-attacks against Estonia from the information warfare perspective. *Proceedings of the 7th European Conference on Information Warfare and Security*, 23–29.
- Parikh, T. P., & Patel, A. R. (2017). Cybersecurity: A comprehensive survey. *International Journal of Advanced Research in Computer Science*, 8(5), 1234–1240.
- Pascariu, C., Barbu, I.-D., & Bacivarov, I. (2017). Ransomware-based attacks. Case study: WannaCry. *International Journal of Information Security and Cybercrime*, 6(1), 57–62.

- Reuters. (2024, September 18). Israel planted explosives in Hezbollah's Taiwan-made pagers, sources say. Retrieved from <https://www.reuters.com/world/middle-east>
- Reuters. (2025, August 13). Norway spy chief blames Russian hackers for dam sabotage in April. Retrieved from <https://www.reuters.com/technology>
- Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5–32.
- Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), 4–37.
- RUSI. (2024, September 18). Nowhere to hide: Israel's pager attacks on Hezbollah. Retrieved from <https://rusi.org/explore-our-research/publications/commentary>
- Sandoval Carlos, O. (2022, May 6). Using cyber threat intelligence to support adversary understanding applied to the Russia-Ukraine conflict. arXiv.
- Sanger, D. E. (2012, June 1). Obama order sped up wave of cyberattacks against Iran. *The New York Times*. Retrieved from <https://www.nytimes.com>
- Sanger, D. E., Perlroth, N., & Barnes, J. E. (2021, April 15). U.S. says Russia was behind SolarWinds hack, part of a broad campaign. *The New York Times*.
- Schmitt, M. N. (2023). The law of cyber warfare and the Ukraine conflict. *International Law Studies*, 99(3), 25–49.
- Sevinc, N. T. (2025, August 13). Norway security service says pro-Russian hackers behind dam sabotage. AA News. Retrieved from <https://www.aa.com.tr/en/europe>
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- Singer, P. W., & Friedman, A. (2024). *Cyber conflict after Ukraine: The evolution of hybrid warfare in the digital age*. Brookings Institution Press.
- Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense. *Computers & Security*, 60, 154–176. <https://doi.org/10.1016/j.cose.2016.04.002>
- Smith, B. (2017, February 14). The need for a Digital Geneva Convention. Microsoft Official Blog.

- Swarts, P. (2015, February 4). Sony cyberattack costs company \$35 million. The Washington Times. Retrieved from <https://www.washingtontimes.com>
- Symantec. (2015). The rise of North Korean cyber operations. Symantec Security Response.
- Taddeo, M. (2023). Digital humanitarian law: Ethics and legality in cyber conflict. *Ethics and Information Technology*, 25(1), 55–69.
- The Guardian. (2024, September 18). Hezbollah device blasts: How did pagers and walkie-talkies explode and what do we know about the attacks? Retrieved from <https://www.theguardian.com/world/2024/sep/18>
- The Guardian. (2025, August 14). Russian hackers seized control of Norwegian dam, spy chief says. Retrieved from <https://www.theguardian.com/world/2025/aug/14>
- Tikk, E., & Kerttunen, M. (2023). Cyber operations in the Russo-Ukrainian war: A hybrid conflict analysis. *Survival*, 65(2), 77–98.
- Tikk-Ringas, E. (2015). The evolution of the cyber domain and its implications for national and international security. *Journal of Cyber Policy*, 1(1), 23–40. <https://doi.org/10.1080/23738871.2015.1101035>
- Tolulas, B. (2025). Pro-Russian hackers blamed for water dam sabotage in Norway. *BleepingComputer*. Retrieved from <https://www.bleepingcomputer.com>
- Treverton, G. F. (2023). Cyber strategy in the new era of great power competition. RAND Corporation.
- Turner, A. B., McCombie, S., & Uhlmann, A. J. (n.d.). A target-centric intelligence approach to WannaCry 2.0. Macquarie University Research Portal.
- United Nations Office for Disarmament Affairs. (2021). Report of the Group of Governmental Experts on advancing responsible state behaviour in cyberspace. United Nations. <https://www.un.org/disarmament/group-of-governmental-experts/>
- Valeriano, B., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.
- Vision of Humanity. (2024). Positive Peace Report 2024. Institute for Economics & Peace.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.

- Wired. (2012, May). Flame: A cyberweapon that makes Stuxnet look cheap. Wired. Retrieved from <https://www.wired.com/2012/05/flame-a-cyberweapon-that-makes-stuxnet-look-cheap>
- Wired. (2024, October 3). The exploding pagers and the future of cyber-kinetic warfare. Wired. Retrieved from <https://www.wired.com/story/exploding-pagers-cyber-kinetic-warfare>
- World Health Organization. (2020). Cyberattacks on health infrastructure during COVID-19. <https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks>
- Zetter, K. (2014). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Crown Publishers.