International Journal of Humanities Social Science and Management (IJHSSM)
Volume 5, Issue 5, Sep.-Oct., 2025, pp: 23-32 ISSN: 3048-6874
www.ijhssm.org

The Impact of Cyberwarfare on Global Peace

Dr. Benjamin Shaibume
Department of Political Science, Rev Fr. Moses Orshio Adasu University, Makurdi
&
Okpe Ngbede Caleb
Department of Political Science, Rev Fr. Moses Orshio Adasu University, Makurdi

Date of Submission: 01-09-2025 Date of Acceptance: 09-09-2025

Abstract
The impact 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 analysis 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. Additionally, cyber-attacks can complicate existing conflicts and make them difficult to resolve. The interconnectedness of cyberspace creates new vulnerabilities, as infrastructure and systems become common targets for cyberattacks. To reduce these problems, work with international standards. 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.

Keywords: Cyberspace, Cyberwarfare, Global Peace, International relations, Digital communications

I. Introduction

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

Cyber security, as stated by Kumar and Somani (2018), encompasses two crucial aspects, the vulnerability that arises due to the emergence of this new digital realm and the implementation of measures and protocols to establish a progressively secure environment. The concept entails a wide range of technical and non-technical practices aimed at safeguarding the integrity and confidentiality of both the digital infrastructure and the sensitive information it carries. According to Kumar and Somani (2018), the field of cyber security involves addressing the inherent risks and insecurities that arise in the digital space. 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 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

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 5, Issue 5, Sep.-Oct., 2025, pp: 23-32 ISSN: 3048-6874
www.ijhssm.org

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 P. Parikh and Ashok R. Patel 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 cyberattacks 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.

Conceptual Clarification

Cyberwarfare

Cyberwarfare 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 objectives. 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.

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. Additionally, 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).

Cybersecurity

Cybersecurity refers to 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 cybersecurity lies in maintaining a proactive defense posture against constantly 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 (Craigen, Diakun-Thibault, & Purse, 2014).

Global Peace

Global peace refers to the absence of war, violence, and systemic conflict across and within nations, supported by the presence of justice, cooperation, and respect for human rights and international law. It is both a condition and a process that requires sustained efforts to build and maintain peaceful relationships among states and societies (Galtung, 1969). 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

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 5, Issue 5, Sep.-Oct., 2025, pp: 23-32 ISSN: 3048-6874
www.ijhssm.org

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: The Complex Communication Theory

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.

Complex Interdependence 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. 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 such as through international cyber norms, treaties, or emergency communication channels rather than escalate tensions. The theory

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 5, Issue 5, Sep.-Oct., 2025, pp: 23-32 ISSN: 3048-6874
www.ijhssm.org

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.

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 Cyberwarfare and it's impact on Global Peace

Stuxnet (2010)

Stuxnet 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.

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

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 5, Issue 5, Sep.-Oct., 2025, pp: 23-32 ISSN: 3048-6874
www.ijhssm.org

facility's network. The attack also used a sophisticated method of communication, 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 malware, also known as Flamer, was a highly sophisticated computer worm discovered in 2012 by Israel. It was designed to spy on and steal sensitive information from computers in the Middle East, particularly in Iran and Palestine. Flame was considered one of the most complex and powerful malware programs ever created, with a size of over 20 megabytes, making it 20 times larger than the Stuxnet worm. It had the ability to record audio, take screenshots, and log keystrokes, as well as steal data from USB drives and Bluetooth devices. The malware was spread through phishing emails and exploited vulnerabilities in Windows operating systems. Once installed, it could spread to other computers on the same network and even create a virtual bridge to allow attackers to access the infected computer remotely. Flame was attributed to the same creators as Stuxnet, believed to be a joint operation between the US and Israeli governments. Its primary goal was to gather intelligence on Iran's nuclear program and other sensitive information.

Sony Pictures Hack (2014)

The Sony Pictures hack was a devastating cyberattack that occurred in November 2014, targeting Sony Pictures Entertainment, a subsidiary of the Japanese conglomerate Sony. The hack was carried out by a group calling itself the "Guardians of Peace" (GOP), which was later linked to North Korea. The hack began with a phishing email sent to Sony employees, which allowed the attackers to gain access to the company's network. The hackers then used malware to spread throughout the network, eventually gaining access to sensitive data, including employee Social Security numbers, emails, and unreleased movies. In the weeks following the initial attack, the hackers began leaking sensitive data, including employee information, emails between executives, and unreleased movies. The leak included embarrassing emails between executives, including racist comments about President Barack Obama. The hackers made demands, including the cancellation of the release of the movie "The Interview," a comedy about a plot to assassinate North Korean leader Kim Jong-un. The FBI launched an investigation into the hack, and in December 2014, the agency announced that North Korea was responsible for the attack. The FBI cited similarities between the Sony hack and previous attacks attributed to North Korea. North Korea denied involvement in the hack, but praised the attack as a "righteous deed." The hack had significant consequences for Sony, including the resignation of co-chairman Amy Pascal and a reported $35 million in costs associated with the breach. The hack also led to increased tensions between the US and North Korea, with the US imposing new sanctions on North Korea in response to the attack. Despite the threats, "The Interview" was released in January 2015, albeit in a limited capacity.

Russian Interference in the US 2016 Election

Russian interference in the 2016 US presidential election refers to the efforts by the Russian government to influence the outcome of the election through various means, including cyber attacks, disinformation campaigns, and contacts with individuals associated with the Trump campaign. In 2016, Russian hackers gained access to the computer systems of the Democratic National Committee (DNC) and stole sensitive information, including emails and opposition research on Donald Trump. The stolen data was later released through WikiLeaks and other online platforms, causing embarrassment to the Democratic Party and its nominee, Hillary Clinton. Russian operatives also used social media platforms to spread disinformation and propaganda aimed at undermining Clinton's campaign and boosting Trump's chances. They created fake social media accounts and purchased targeted online ads to reach specific demographics and sway public opinion.

The Russian government also made contacts with individuals associated with the Trump campaign, including Donald Trump Jr., who met with a Russian lawyer promising dirt on Clinton. The Trump campaign's national security adviser, Michael Flynn, also had secret communications with the Russian ambassador to the US, Sergey Kislyak. The US intelligence community concluded that Russia's interference was designed to harm Clinton's chances

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 5, Issue 5, Sep.-Oct., 2025, pp: 23-32 ISSN: 3048-6874
www.ijhssm.org

and help Trump win the election. The FBI launched an investigation into the matter, which led to the indictment of several Russian nationals and the conviction of Trump campaign associates, including Flynn and Paul Manafort.

WannaCry Ransomware Attack (2017)

The WannaCry ransomware attack was a global cyberattack that occurred in May 2017, affecting over 200,000 computers in over 150 countries. The attack was caused by a ransomware worm that exploited a vulnerability in the Windows operating system, known as EternalBlue. The attack began on May 12, 2017, and spread rapidly across the globe, infecting computers in hospitals, schools, businesses, and government agencies. The ransomware encrypted files on infected computers and demanded a payment of $300 to $600 in bitcoin to restore access. The attack had a significant impact on the UK's National Health Service (NHS), where over 80 hospitals and clinics were affected, leading to the cancellation of surgeries and appointments. Other affected organizations included FedEx, Merck, and the Russian Interior Ministry. The attack was attributed to North Korea, with the US and UK governments publicly blaming the regime for the attack. The attack is believed to have been carried out by the Lazarus Group, a hacking group linked to North Korea.

The WannaCry attack highlighted the vulnerability of organizations to cyberattacks and the importance of keeping software up to date. It also led to increased awareness about the risks of ransomware and the need for robust cybersecurity measures. In the aftermath of the attack, Microsoft released a patch for the EternalBlue vulnerability, and many organizations took steps to improve their cybersecurity, including implementing backups and disaster recovery plans. The attack also led to increased cooperation between governments and private companies to combat cyber threats, including the establishment of the Global Cyber Alliance, a non-profit organization dedicated to reducing cyber risk.

Ukraine-Russia Conflict (2022-2024)

The Ukraine-Russia conflict has seen extensive use of cyber warfare, with both sides engaging in attacks on critical infrastructure, military targets, and civilian populations. Russia launched a series of cyber attacks on Ukrainian targets, including government agencies, banks, and critical infrastructure, in the lead-up to its invasion. These attacks aimed to disrupt Ukraine's command and control structures and create chaos. Ukraine responded with its own cyber attacks, targeting Russian military command systems, logistics, and supply chains. Ukrainian hackers also launched attacks on Russian state media and propaganda outlets. As the conflict escalated, so did the cyber warfare. Russia launched more sophisticated attacks, including the use of wipers and ransomware, to destroy Ukrainian data and disrupt critical infrastructure. Ukraine continued to target Russian military and logistical systems.

The cyber conflict has had a significant impact on civilians, with attacks on critical infrastructure, such as power grids and water supply systems, causing disruptions to essential services. The conflict has drawn in other international actors, with the US, EU, and NATO providing cyber support to Ukraine, while Russia has allegedly received support from Chinese and Iranian hackers. The cyber conflict continues to escalate, with both sides launching increasingly sophisticated attacks. The impact on civilians and critical infrastructure remains a major concern, highlighting the need for international cooperation to prevent the spread of cyber warfare.

Beeper Operation used by Israel against Hezbollah in 2024

The "Beeper" operation, conducted by Israeli intelligence against Hezbollah, showcases the critical role of cyberwarfare in modern conflict. By infiltrating and disrupting Hezbollah's communication networks, Israel gained significant intelligence and disrupted Hezbollah's command and control structures. This operation highlights the importance of cyberwarfare in achieving strategic objectives, particularly in asymmetric conflicts. The use of cyber operations allowed Israel to exploit vulnerabilities in Hezbollah's communication systems, demonstrating the potential for cyberwarfare to level the playing field against non-state actors. These devices, believed to be secure from electronic surveillance, were turned into lethal instruments when they simultaneously exploded, killing at least 15 people and injuring over 3000. This operation, marked by its sophistication, involved the infiltration of Hezbollah’s pager supply chain, where each device was reportedly embedded with small amounts of PETN explosive, a highly potent material.

The attack was so precisely executed that it suggests a long-term intelligence operation, involving not just the physical tampering of the pagers but also the strategic placement to ensure minimal civilian casualties, focusing primarily on Hezbollah members.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 5, Issue 5, Sep.-Oct., 2025, pp: 23-32 ISSN: 3048-6874
www.ijhssm.org

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. 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

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 5, Issue 5, Sep.-Oct., 2025, pp: 23-32 ISSN: 3048-6874
www.ijhssm.org

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.

II. Conclusion

The rise of cyberwarfare presents a significant and evolving threat to global peace, fundamentally altering the landscape of international security. Its impact extends beyond traditional military confrontations, capable of crippling critical infrastructure, destabilizing economies, manipulating political processes, and fostering an environment of distrust and misattribution. The anonymity inherent in cyberspace, coupled with the low cost and ease of launching attacks, makes attribution a complex challenge, increasing the risk of miscalculation and escalation. While the international community grapples with establishing norms and frameworks for responsible state behavior in this new domain, the pervasive vulnerability of interconnected societies necessitates a concerted global effort towards robust cybersecurity defenses, international cooperation, and clear legal guidelines to mitigate the profound risks cyberwarfare poses to stability and peace worldwide.

III. Recommendations

1. Establishment of a Global Cybersecurity Treaty

One of the most promising prospects for enhancing cybersecurity and promoting global peace is the development of a comprehensive international treaty on cyber norms, rights, and responsibilities. Such a treaty, akin to the Geneva Conventions, would provide a universally accepted framework for state behavior in cyberspace, outlining prohibited actions such as attacks on critical civilian infrastructure, election interference, and deployment of malware in peacetime. Currently, legal ambiguity allows states to exploit loopholes for digital aggression without repercussions. A treaty would formalize accountability mechanisms, encourage transparency, and deter state-sponsored cyberattacks through clearly defined consequences. It would also serve as a tool for conflict prevention, ensuring that states have peaceful avenues for resolving cyber disputes (Tikk-Ringas, 2015).

2. Creation of a UN Cyber Peacekeeping Force

To further bolster international peace and cyber resilience, the United Nations or a multilateral body could create a Cyber Peacekeeping Force. This force would function like traditional peacekeepers but in the digital domain, monitoring cyber conflicts, assisting states in mitigating cyberattacks, and restoring digital infrastructure after breaches. Such a mechanism would be especially valuable in conflict-prone regions or developing countries with weak cybersecurity frameworks. The cyber peacekeepers could act as neutral mediators, promote de-escalation during cyber crises, and facilitate post-attack recovery. This initiative would not only reduce tensions during digital skirmishes but also signal international solidarity in defending peace in the cyberspace frontier (Maurer, 2022).

3. Promotion of Multistakeholder Cyber Diplomacy

Another essential step is the inclusion of non-state actors such as tech companies, civil society, and academia in cyber diplomacy processes. The internet is largely managed and innovated by private entities, yet international cyber negotiations have been dominated by state actors. Effective peace in cyberspace requires inputs from all stakeholders, especially those who design, operate, and secure the digital infrastructure. By promoting public-private cooperation through platforms such as the Paris Call for Trust and Security in Cyberspace or the Global Forum on Cyber Expertise, the international community can harness collective expertise, enhance trust, and develop inclusive cybersecurity policies. This multistakeholder approach strengthens global cyber governance and reinforces shared responsibility for peace and stability.

4. Strengthening Capacity Building and Cyber Solidarity

The quest for global peace through cybersecurity also hinges on building cyber capacity in developing and vulnerable nations. Disparities in technological expertise and infrastructure leave many countries especially in Africa, Latin America, and parts of Asia exposed to cyber threats. International cooperation should focus on technical assistance, training, and investment in national cybersecurity strategies. Programs led by the International Telecommunication Union (ITU), the European Union, or bilateral partnerships can help these countries build secure digital ecosystems. Enhanced resilience in weaker states not only protects them from being exploited as launchpads for cyberattacks but also reduces global cyber risk. Capacity building promotes cyber solidarity and ensures that no country is left behind in the collective pursuit of peace.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 5, Issue 5, Sep.-Oct., 2025, pp: 23-32 ISSN: 3048-6874
www.ijhssm.org

5. Development of Cyber Conflict Early Warning and Crisis Response Systems

A final and strategic recommendation is the establishment of global cyber conflict early warning systems. Much like systems for monitoring natural disasters or disease outbreaks, cyber conflict detection tools can track, analyze, and alert states to rising tensions or potential attacks in real-time. Regional cybersecurity hubs such as those supported by the African Union, NATO, or ASEAN could collaborate to form an integrated global network for monitoring malicious digital activity. These systems would facilitate timely diplomatic interventions, reduce chances of escalation, and foster crisis communication channels among adversaries. Such proactive systems are crucial to preempting cyberwarfare and maintaining peace in a digital age defined by speed, complexity, and volatility.

References

[1]. Boutros-Ghali, B. (1992). An agenda for peace: Preventive diplomacy, peacemaking and peace-keeping. United Nations. https://www.un.org/en/ga/documents/

[2]. Carr, M. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62.

[3]. Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. Ecco.

[4]. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), 13–21.

[5]. Center for Strategic and International Studies. (2020). Significant cyber incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[6]. 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

[7]. Europol. (2018). WannaCry ransomware: A global cyberattack. https://www.europol.europa.eu/publications-events/publications/wannacry-ransomware-global-cyberattack

[8]. Galtung, J. (1969). Violence, peace, and peace research. Journal of Peace Research, 6(3), 167–191

[9]. Healey, J. (2013). A fierce domain: Conflict in cyberspace, 1986 to 2012. Cyber Conflict Studies Association.

[10]. Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. International Security, 38(2), 7–40.

[11]. Kihan, R., & Nye, J. S. (1977). Power and interdependence: World politics in transition. Little, Brown and Company.

[12]. Kumar, S., & Somani, V. (2018). Cybersecurity: A comprehensive approach to secure the digital world. *International Journal of Computer Applications*, 182(25), 1–7.

[13]. Libicki, M. C. (2007). Conquest in cyberspace: National security and information warfare. Cambridge University Press.

[14]. Maurer, T. (2022). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.

[15]. Mazarr, M. J. (2015). Mastering the gray zone: Understanding a changing era of conflict. Strategic Studies Institute, U.S. Army War College.

[16]. Mueller, M. L. (2010). Networks and states: The global politics of internet governance. MIT Press.

[17]. Nye, J. S. (2011). The future of power. PublicAffairs.

[18]. 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.

[19]. Parikh, T. P., & Patel, A. R. (2017). Cybersecurity: A comprehensive survey. *International Journal of Advanced Research in Computer Science*, 8(5), 1234–1240.

[20]. Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5–32.

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

[22]. 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.

[23]. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

[24]. 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

[25]. 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

[26]. 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/

[27]. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

[28]. 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

[29]. Zetter, K. (2014). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Crown Publishers.