Article

Revisiting Sovereignty in the Age of Cyber Warfare: Legal, Ethical and Geopolitical Dimensions

Journal of Liberal Arts and Interdisciplinary Sciences
1(1) 53–68, 2026

DOI: 10.1177/jlais.251408160
laj.tohrifoundation.com/

Priti Rana[1] and Amna Mirza[2]

Abstract

The frequency and sophistication of cyber warfare pose novel challenges to conventional ideas of sovereignty and international law. As state and non-state actors leverage cyber capabilities to launch attacks, the legal frameworks that have long regulated the use of force and state sovereignty are being challenged. This article discusses the changing dynamic between sovereignty and international law in the context of cyber warfare, highlighting the necessity for a reimagined approach to meet the fast-paced technological developments. Based on international case studies, including the 2007 cyberattack on Estonia and the current cyber tensions between the USA and Russia, this research investigates how states are attempting to navigate the intricacies of cyber sovereignty in a connected digital world. It also looks at the lacunae in current international law and the issues of attribution, proportionality and protection of civilian infrastructure. The article also identifies national legal systems and the need for international collaboration to construct a harmonious legal structure to combat cyber threats. Considering the accelerated pace of technological advancements, the article makes the case for creating international treaties and norms that give states responsibility and accountability in cyber warfare clearly. Ethical aspects involving human rights, digital infrastructure and privacy are also touched upon. Finally, this will advocate for drastic reforms in interdisciplinary reflections on law, ethics and global power to guarantee that sovereignty can be properly protected against advanced cyber threats.

Keywords

Cyber warfare, sovereignty, international law, cyber security, attribution, digital infrastructure, international cooperation, global power

[1]Faculty of Law, University of Delhi, India
[2]SPM College, University of Delhi, India

Corresponding author:
Amna Mirza, C-121, Defence Colony, Lajpat Nagar, Delhi 110024, India.
E-mail: amna.mirza786@gmail.com

Introduction

The idea of sovereignty has historically been defined as the supreme power of a state over its own territorial boundaries, untainted by interference from outside entities. In the past, sovereignty was based on the physical, geographical sphere where states had exclusive jurisdiction over their land, their people and their resources. But since the 21st century, the emergence of digital technologies and cyber warfare has threatened the very essence of this old concept, compelling international law to deal with new, transborder aspects of conflict.

However, cyber warfare, defined by the application of digital attacks against critical systems with the aim of disrupting, damaging or obtaining unauthorized access to them, has become a central threat to national security. As opposed to traditional warfare, which is fought on the tangible domain of borders, cyber warfare exists in the intangible realm of cyberspace a networked, virtual geography without borders. The simultaneous attack, aimed at the country's cyber infrastructure, caused widespread disruptions in government services, banking and media. This event proved that cyber warfare has the capability to disable a country's economy and administration without ever entering its territory. Subsequent years have seen other nations, such as the USA, Russia and China, pursuing similar actions, proving further the global reach of cyber warfare (Schmitt, 2013). Yet, despite the growing prevalence of cyber threats, international legal norms continue to be shaped by an outdated understanding of sovereignty that prioritizes physical borders and territorial integrity.

Furthermore, ongoing international law, which includes treaties such as the United Nations Charter and the Geneva Conventions, has struggled to provide clear guidelines for regulating cyber warfare. Although the UN Charter codifies the doctrine of sovereignty and non-intervention in the internal affairs of a state, these provisions were drafted when warfare was characterized by physical, armed conflicts. The Geneva Conventions, which afford critical protections during armed conflict, also do not capture the complexities of cyber warfare, especially the issues of attribution, responsibility and the protection of civilians in the virtual environment (Schmitt, 2013). Therefore, the need to redefine sovereignty within the context of cyber warfare is urgent, with international law following the pace of this fast-developing threat. Through the study of the sophistication of cyberattacks, the problems of attribution and the potential of international cooperation in countering cyber threats, this article shall contend that a revaluation of sovereignty and new international legal standards are needed at once. These new structures would not only preserve state sovereignty in the information era but also keep countries in a better position to counter the shifting threats of cyber warfare.

The Evolution of Sovereignty in the Digital Age

The conventional understanding of sovereignty has been radically changed in the last century, especially with the advent of globalization, technological advancement and the growing influence of digital platforms in domestic and global politics. Sovereignty, which was originally understood in physical and territorial terms, is now challenged by new forces as cyberspace becomes a theatre of power,

influence and conflict. Traditionally, sovereignty was understood as an absolute, undivided right of states over their territory and population to the exclusion of outside interference. Based on the Treaty of Westphalia (1648), which created the contemporary international system of statehood, sovereignty has been a pillar in international relations and law (Osiander, 2001). The Westphalian framework established well-defined borders, with stress laid upon territorial integrity and non-interference in internal matters. In this system, states were taken to be the main actors within the international realm, capable of enforcing laws, upholding order and protecting themselves within their territorial boundaries.

Furthermore, as the process of globalization gained momentum towards the end of the 20th and early 21st centuries, the concept of sovereignty also started evolving. The globalization of trade, communication and migration created hazy boundaries which made it almost impossible to retain complete control over one's state. Meanwhile, technological advancements like the emergence of the internet and digital communication technology introduced new venues for power and influence, subjecting states to dilemmas in exercising sovereignty over cyberspace. Cyberspace has radically reshaped the topology of sovereignty by making the world borderless and connected. The introduction of the internet has facilitated the quick dissemination of information, business and ideas but, in the process, has opened new vulnerabilities. Cyberattacks can attack infrastructure, disrupt political processes and even influence public opinion, all without physical presence. This has resulted in a point where state sovereignty is no longer limited to the physical space of territory but must extend to the digital space as well, giving rise to a complicated, multidimensional landscape for international law (Kello, 2017).

In addition, this article categorized an interdisciplinary approach of how cyber warfare is reshaping the meaning of sovereignty in today's interconnected world. Its originality lies in coordinating three distinct yet interrelated domains; therefore, it can be understood as the notions of law, ethics and international politics to move beyond a purely legal or technological reading of the issue. It adopts a qualitative and analytical approach, drawing from international legal instruments such as the UN Charter and the Tallinn Manual, as well as ethical theories of responsibility and justice. It also integrates perspectives from global power relations to understand how states negotiate control and accountability in cyberspace. However, rather than relying on statistical data, the research uses doctrinal and comparative analysis to interpret principles, case studies and moral implications, aiming to provide a holistic and human-centred understanding of sovereignty in the digital age.

Literature Review

The new and developing field of cyber warfare has posed essential questions regarding the interface between sovereignty and international law. The expanding use of cyber weapons in statecraft, war and terrorism has highlighted essential gaps in the prevailing international legal structures that have hitherto regulated conventional warfare. This review of the literature examines several scholarly views on the implications of cyber warfare for sovereignty and international law,

examining the intricacies and challenges that have arisen as the digital world becomes a stage for geopolitical rivalry.

The *Challenge to Traditional Sovereignty* has been the foundation of international law, based on the Westphalian system that prioritizes territorial integrity and the sanctity of national borders (Keohane, 2002). But the advent of cyber warfare contradicts this conventional perception since cyberspace has no borders. According to scholars, cyber threats, by definition, erode the territorial components of sovereignty since they cross national borders and frequently come from outside jurisdictions, thus making them hard to assign (Krasner, 2001). This transnational extension of cyberattacks makes sovereignty a critical concept that needs to be reassessed in an environment where action and reaction can take place simultaneously in the world. As Keohane (2002) posits, the states need to redefine their definitions of sovereignty to accommodate the realities of the virtual world, where internal and external threats become intertwined. The *Tallinn Manual* is perhaps the most influential academic effort to transpose international law to cyber warfare. It offers a critical examination of the application of established legal principles, including the law of armed conflict, to cyber operations (Schmitt, 2013). The manual has played a critical role in structuring the discourse on cyber war and sovereignty in that it has sought to address how the principles of war apply to the digital world. Yet, the Tallinn Manual is not binding in law, and its application is contentious. Its critics say that while it is helpful to have guidelines, it does not go as far as providing tangible solutions to the urgent issues of cyber warfare. Kello (2017) contends that as useful as the manual is, however, the fact that it is founded on pre-existing models means that it does not adequately deal with one of the most special challenges that cyber warfare presents, including the problem of attributing effects and the constantly changing nature of cyber threats. The doctrine of proportionality, which is at the heart of international humanitarian law, is key to controlling the application of force in both traditional warfare and cyber warfare. As it applies in the case of cyber warfare, proportionality makes it mandatory that a response to a cyberattack should be as the scale and extent of the initial attack (Schmitt, 2013). Yet, since numerous cyberattacks go unnoticed and might not be promptly felt, following this principle would become extremely daunting. Experts reason that identifying responses proportionate to cyberattacks implies reevaluating the measurement of damage and influence in cyberspace. Tikk (2015) implies that proportionality needs to be understood more subtly, in terms of its direct and indirect effects, including lasting economic or political implications that will not necessarily be immediately apparent.

The Imperative of Multilateral Legal Responses: As cyberspace is transnational, it is increasingly felt that unilateral legal measures for cyber warfare may not be adequate to meet the international nature of cyber threats. Scholars call for a multilateral solution to cyber warfare, in which global cyber norms are shaped and enforced through international cooperation (Mueller, 2010). Since cyberspace transcends any single state, collective action by states must be taken to prevent the escalation of cyber conflicts and create stability in the virtual space. Held and McGrew (2007) stress that international institutions, including the United Nations,

must take a leading role in governing cyber activities so that states come together to establish binding agreements on cyber defence, offence and the conduct of cyber warfare. The *Future of Cyber Sovereignty and International Law*: As the international community continues to come to terms with the reality of cyber warfare, there is also a developing understanding that the very notion of sovereignty needs to change. There has been the development of the idea of 'cyber sovereignty', where countries define control over their virtual spaces, but this must be reconciled with global cooperation (Krasner, 2001). The dilemma is how to balance states' urge to manage their virtual borders and the necessity for joint action in confronting cyber threats that tend to transcend national borders.

Global Power and Cyber Warfare

Traditional international law, based on state sovereignty and territorial integrity, has been gradually adapting to increased global complexities in challenges, particularly in the wake of sophisticated modern technological warfare. Cyber warfare has been a highly challenging issue for international legal processes since it has no conventional description or definition for warfare and associated legal implications. Unlike classical forms of war, cyber war frequently employs non-kinetic techniques that may disrupt essential infrastructure, inflict economic harm and impede political structures without territorial borders being crossed (Schmitt, 2013). The new form of conflict has raised serious issues regarding the application of existing international law to cyber operations, particularly about sovereignty, responsibility of states and the use of force.

Sovereignty, which is one of the fundamental principles of international law, holds that states possess absolute authority in their own territory without interference from outside. Cyberattacks undermine this principle since they can be launched across borders without the direct intervention of state actors. Cyberattacks may come from non-state actors or state-sponsored actors, making it difficult to define accountability and enforcing sovereignty (Tikk, 2010). This change in conflict has compelled a reconsideration of the classical definition of sovereignty in international law. Traditional sovereignty implies authority over a defined space, yet cyber warfare poses the question as to whether states can be considered to have sovereignty over their digital networks (Shackelford, 2014). Others feel that new definitions and rules must be developed to recognize the intangible character of cyber operations that do not easily fit into the existing international legal order (Klabbers, 2013). However, the use of the ban on the use of force, enshrined under Article 2(4) of the UN Charter, is yet another area of disagreement. In conventional war, the employment of force is evident, whereby physical violence occurs between military units. This uncertainty has raised questions about whether cyberattacks should be regarded as a use of force in international law and, if they can be, what requirements need to be fulfilled so that an action of cyber warfare would activate self-defence (Schmitt, 2017).

The Tallinn Manual, which is a code of guidelines on cyber warfare law established by NATO, gives some indication on this matter, stating that a cyberattack

will be an act of force if it results in 'significant harm' to a state, including damage to essential infrastructure or disruption of critical services (Schmitt, 2013). Still, the guide also emphasizes the necessity of a case-by-case approach since the benchmark for deciding if a cyberattack would amount to a use of force is uncertain and extremely dependent on context (Shackelford, 2017). State responsibility is yet another principal matter in cyber warfare. Conventional concepts of state responsibility in international law centre around the activities of state agents, but the use of anonymity in cyber operations makes this paradigmatic approach challenging. In most instances, it might be challenging to point to a state or actor responsible for a cyberattack because the actors may have used proxies, false flags or other methods to obscure the origin of the attack (Nakashima, 2018). This transparency problem presents immense challenges in identifying at what point a state can be held responsible for cyberattacks, particularly in cases where non-state actors, like hackers or terrorist organizations, are implicated. But these efforts are usually not globally coordinated, and there arises a patchwork approach to cybersecurity and law. Whereas international law establishes a basic framework for the control of conventional modes of warfare, cyber warfare raises new issues and challenges. Sovereignty, the meaning of the use of force, state responsibility and international cooperation all need to be reassessed in the wake of the emergence of cyber operations.

Global Case Studies on Cyber Warfare

Cyber warfare has become a major geopolitical instrument, with nations using cyber operations to gain strategic benefits. Analysing significant cyber wars assists in comprehending how international law, sovereignty and security paradigms are being challenged. The following case studies present major incidents that have influenced global debate on cyber warfare and its legal aspects. These international case studies illustrate the critical necessity for global legal mechanisms to regulate cyber war.

The Estonia Cyber Attacks (2007): A Wake-up Call for Cybersecurity

In 2007, Estonia was the first country to face a massive cyberattack that disabled its virtual infrastructure. After a political row regarding the removal of a Second World War memorial, Estonian government sites, banks and media were bombarded with Distributed Denial-of-Service (DDoS) attacks. While the attacks were generally ascribed to Russian interests, no definitive evidence of state actions existed (Ottis, 2008). The Estonian government replied by firming up its cybersecurity policy and calling for global cooperation. NATO then went ahead to create the Cooperative Cyber Defence Centre of Excellence in Tallinn, reflecting the growing seriousness of cyber warfare as a security threat (Tikk, 2010). This incident was criticized as to whether or not such acts qualify as acts of war according to international law since no actual physical force was employed.

Stuxnet (2010): Cyber Weapons in Military Operations

Stuxnet, a highly advanced malware that was found in 2010, was the first known instance of a cyber weapon inflicting physical damage. It was supposedly created by the USA and Israel and was aimed at Iran's nuclear enrichment plants, crippling close to 1,000 centrifuges at the Natanz plant (Zetter, 2014). The cyberattack brought with it crucial legal and ethical concerns: Is cyber sabotage against key infrastructure an act of war? How does international law control cyber weapons use? Iran condemned the attack as a breach of its sovereignty, yet since there were no clear international legal norms, no official charges were made against the suspected states. Stuxnet established a precedent for state-sponsored cyber activities as an instrument of foreign policy (Lindsay, 2015).

China–India Cyber Conflicts: Espionage and Cyber Sovereignty

India and China have experienced increased cyber tensions, especially following military border skirmishes. Chinese Advanced Persistent Threat (APT) actors have been associated with cyber espionage against Indian government institutions, defence agencies and infrastructure (Singh, 2021). One of the most important features of China's cyber policy is the 'Great Firewall', which strictly controls internet access and advances cyber sovereignty, with the state exerting control over online spaces. India has an open internet policy but has countered cyber threats by blocking Chinese apps and increasing cybersecurity efforts (Chaudhary, 2020). This tension serves to exacerbate the intersection of national sovereignty and cybersecurity, illustrating how norms in cybersecurity vary across democratic and authoritarian regimes. The absence of global agreement on cybersecurity governance makes diplomatic attempts at controlling such tensions challenging (Weber, 2022).

Proposals for Redefining Sovereignty and International Law in Cyber Warfare

The development of cyber warfare has highlighted the insufficiency of current international legal regimes in responding to state sovereignty, responsibility and conflict resolution. Conventional legal tools like the UN Charter (1945) and the Geneva Conventions mainly regulate physical warfare and territorial integrity but do not fully consider the virtual battlefields where contemporary conflicts increasingly take place. Considering the borderless environment of cyberspace, states are still in a legal limbo in which cyber aggressions are consistently answered with uneven measures, and attribution continues to be an important problem. This calls for a serious re-examination of sovereignty in cyberspace and the establishment

of clear-cut legal frameworks to regulate state actions in this environment. One of the greatest anxieties about redefining sovereignty in cyberspace is the development of cyber sovereignty norms in international law. Sovereignty in the digital world is still contentious, with some calling for total dominance over digital infrastructure and others for an open and globally connected internet. China and Russia have always advocated for a cyber sovereignty model that enables states to have complete control over their internal internet, limiting outside influences in the interest of national security. This model, however, is directly opposed to the principle of Western democracies focusing on internet freedom, information flow across borders and multilateral management of cyberspace. Closing this ideological gap is required to build a feasible international legal system. A definition of what represents a breach in cyber sovereignty is required, which should be spelled out clearly through law, specifically in instances involving election interference, cyber espionage or state-sanctioned cyberattacks. There are also insufficient answers to queries on how such threats should legally be responded to by states and whether cyber war warrants military responses. Tools such as the Tallinn Manual 2.0 offer non-binding advice, but what is needed most urgently now are binding international treaties that create accountability and state responsibility in cyberspace.

Whereas one of the key components of cyber sovereignty is international cooperation, current initiatives are still very much fragmented and have no enforcement power. The United Nations Group of Governmental Experts (UN GGE) and instruments such as the Paris Call for Trust and Security in Cyberspace emphasize cooperation but, being non-binding, have state compliance neither uniform nor compulsory. In the absence of binding measures, cyber conflicts are substantially unregulated and open to escalation without definite penalties. To answer this, the establishment of an international cyber tribunal could offer a stage for states to settle cyber grievances through law instead of reprisal. Intelligence-sharing treaties between states with allied relationships could enhance cyber defences against state-aided attacks. Regional cybersecurity architectures, like that of NATO's Cyber Defence Pledge, could be used as an example for extended multilateral treaties to secure collective security within cyberspace. Creating a *Cyber Sovereignty Accord* within the United Nations, establishing norms and proportional reactions to cyberattacks, would be a crucial step towards global stability.

Perhaps the most legally unclear element of cyber warfare is the categorization of cyberattacks in international law. Today, cyberattacks are not globally accepted as acts of war unless they cause extensive physical damage or loss of life. This legal classification gap provides a loophole through which states can practice cyber aggression without fear of conventional military counterattack. It is important to create a clear legal framework that distinguishes between cyber espionage, cyber sabotage and large-scale cyber warfare in order to establish appropriate responses. Cyber espionage, which is the collection of intelligence by unauthorized digital access, is generally handled as a diplomatic transgression and not an act of war. Cyber sabotage, for example, against financial institutions or government databases, is a more serious violation of sovereignty and must be considered an act of aggression. Large-scale cyber warfare, where attacks disable national

infrastructure or threaten civilian lives, must be explicitly defined under Article 51 of the UN Charter as an armed attack, thus warranting state self-defence actions. By defining these legal thresholds, the states can create proportional responses that avoid unnecessary escalation and provide accountability for cyber aggression.

Another essential issue is the absence of an all-encompassing international treaty that regulates cyber warfare. Although the Budapest Convention on Cybercrime deals with cybercriminal behaviour, it does not adequately regulate state-sponsored cyber action. In contrast to nuclear and chemical warfare, which are controlled by stringent treaties like the Nuclear Non-Proliferation Treaty, there is yet no global treaty that governs cyber warfare. Establishing a Global Cybersecurity Treaty within the United Nations would create much-needed legal ground for states to manoeuvre in cyber conflict. The treaty should consist of agreements on cyber arms control, limiting the employment of offensive cyber weapons against civilian infrastructure like hospitals, power grids and financial systems. It should also have a cyber non-aggression agreement prohibiting attacks on digital infrastructure that is key to humanitarian activities. For enforceability, a body for monitoring cybersecurity under the UN could exist to probe cyber breaches and sanction offenders. Without such legally enforceable agreements, cyber warfare will remain in an arena where attackers operate with impunity, further destabilizing international security. One of the most contentious areas in cyber warfare law is the issue of countermeasures and deterrence. Numerous states have started taking active cyber defence measures in which they respond to cyberattacks through offensive cyber action. But international law today does not clarify the legality of such countermeasures, which makes state responses uncertain. The lack of regulation has brought about an environment where powerful states justify retaliatory cyber measures under the mantle of self-defence, which increases the threat of uncontrolled escalation. Existing legal doctrines are inadequate in confronting the phenomenon of cyber war, with such doctrines lacking full accountability, responsibility of states and response models. A redesigned legal framework addressing cyber sovereignty conventions, enhancing multilateral cooperation, setting transparent lines for classifying cyber warfare, creating robust cyber security treaties and controlling countermoves is essential to ensure cyberspace stability. Without an active strategy of legal reform, the international community can create a vacuum that would allow cyber conflicts to develop into a normless space where non-state and state actors act without limit. As the following section discusses, ethical and human rights issues in cyber warfare further complicate the discourse on sovereignty, especially concerning privacy, digital freedom and humanitarian law.

Ethical and Human Rights Implications in Cyber Warfare

The potential for cyber warfare has brought far-reaching ethical and human rights issues, especially in relation to privacy, online freedom and the humanitarian effect of cyber warfare. In contrast to traditional warfare, where the law of armed

conflict governs actions by states and safeguards civilians, cyber warfare exists in a legal and ethical area where the effect on human rights tends to be disregarded. The increasing trend of using cyber operations for the purpose of spying, monitoring and cyberattacks has serious issues related to infringements of universal rights such as the right to privacy, the freedom of speech and information access. Cyber warfare as an instrument of national power is crucial in analysing the ethical dimensions, and it requires the formulation of a legal norm that protects the rights of humanity in cyberspace. One of the most urgent ethical issues in cyber war is the wholesale invasion of privacy by state-led surveillance and cyber espionage. Governments across the globe have increasingly used cyber means to intercept communications, monitor online activities and harvest personal information in the name of national security. The emergence of mass surveillance initiatives, including the PRISM programme by the US National Security Agency (Greenwald, 2013), has brought to light the degree to which intelligence agencies of states abuse online platforms to maintain secret surveillance, sometimes in the absence of judicial review. Although these are justified by states as required for national security and counterterror measures, they pose severe ethical concerns over the reconciliation of security and civil liberties. Both the European Court of Human Rights and the United Nations have continued to assert time and again that mass surveillance campaigns are against Article 17 right to privacy as provided in the International Covenant on Civil and Political Rights. Ethically, therefore, the issue is whether the state can resort to mass surveillance without compromising the values of a democratic society as well as human rights. There is an increasing need for global legal frameworks imposing limits on state surveillance, ensuring that intelligence gathering respects principles of necessity and proportionality.

Apart from issues of privacy, cyber warfare is also extremely consequential for freedom of expression and information access. Authoritarian states have increasingly used cyber technologies to manage digital spaces, censor online material and repress political opposition. China's 'Great Firewall' is a classic case of how governments control cyberspace to limit access to international information and track citizens' online activities (Deibert, 2018). Likewise, in times of political unrest, governments in nations like Iran and Myanmar have shut down the internet to suppress opposition movements, essentially curtailing citizens' capacity to communicate and mobilize protests. These state-imposed restrictions directly violate Article 19 of the Universal Declaration of Human Rights, which promises freedom of expression and the right to receive information. The ethical dilemma is how to define the degree to which states can control digital spaces without violating basic freedoms. The global community needs to respond to this problem by implementing laws that limit the misapplication of cyber technologies for political persecution while taking into consideration the necessity for cybersecurity. Cyber warfare also inflicts enormous threats upon critical infrastructure, which in turn threatens civilian populations. In contrast to conventional military attacks, cyberattacks against vital services such as healthcare systems, power infrastructure and financial institutions have indirect but crippling humanitarian consequences. Cyber warfare, however, obfuscates the line between civilian and military targets, such that these legal protections cannot effectively be applied. To

counteract this, international legal frameworks must provide clear directives that ban cyber operations against civilian infrastructure and entail accountability measures for violations.

Furthermore, the psychological and social effects of cyber warfare pose significant ethical considerations. Unlike traditional warfare, where damage is palpable and immediate, the impact of cyberattacks is intangible yet just as disruptive. Cyber warfare has the potential to influence public opinion, disseminate fake news and destroy democratic institutions' trust. The 2016 US Presidential Election meddling, which was blamed on Russian cyber activities, illustrated how campaigns of disinformation have the potential to demote public confidence in electoral processes and democratic leadership (Benkler et al., 2018). Likewise, deepfake technology and AI-powered propaganda campaigns have heightened the anxiety regarding the moral implications of cyber manipulation. The test for international law is how to devise tools that fight disinformation without suppressing freedom of speech and political discourse. Governments and tech companies must work together to enact solutions that boost digital literacy, fact-checking programmes and protections against algorithmic manipulation. The human rights and ethical concerns of cyber warfare emphasize the necessity to establish an international legal framework that balances security needs with inherent freedoms. States have exploited cyber technologies in ways that endanger individual rights and democratic values due to the lack of distinct legal norms. In the future, the global community has to create binding international agreements governing state surveillance, defending digital rights, protecting civilian infrastructure and establishing ethical norms for cyber activities. Mechanisms for accountability, such as international courts and human rights monitoring institutions, must also be fortified to deal with breaches of cyber ethics. As cyber war develops, the legal and ethical arguments around it will determine the future of international security and human rights in the digital era.

Recommendations and Future Directions

As cyber war continues to evolve, it becomes increasingly clear that the current structures of international law and conventional concepts of sovereignty are insufficient in responding to the challenges brought about by cyber wars. The speedy development of technology, the emerging prominence of state-sponsored cyber actions and the increasingly prominent position of non-state actors within cyber warfare have created a need to revisit the definition of sovereignty in the digital age. In the future, the global community needs to introduce sound legal frameworks, improve international governance institutions and create new norms that promote stability, security and the safeguarding of digital rights in cyberspace. One of the most urgent concerns in redefining sovereignty in the cyber environment is establishing legal norms that regulate state behaviour in cyber warfare. *The Tallinn Manual*, a non-binding legal document formulated by an international team of experts, offers a key foundation for the application of international humanitarian law to cyber operations (Schmitt, 2017). But the manual is very

limited in that it is not legally binding and does not enjoy universal acceptance among states. Whereas some nations believe that current international law is adequate to govern cyber warfare, others highlight the importance of new treaties specifically addressing cyber wars (Hathaway et al., 2012). The challenge is to find international agreement on legal principles governing cyber aggression, holding states accountable for cyberattacks and the conditions under which cyber operations are an act of war. In the absence of clear legal guidance, states will continue to use cyber warfare as a strategic means with impunity. The future of cyber governance hinges on whether the states can resolve these differences and agree on a cooperative system balancing national sovereignty and global cyber stability needs. A solution is the creation of a specialist international cyber security agency, comparable to the International Atomic Energy Agency, which observes cyber threats, settles disputes and ensures observance of norms agreed upon. The future of sovereignty in the cyber realm also poses challenges about the coexistence of national security and virtual liberties. The growing militarization of the cyber domain has contributed to the proliferation of state surveillance initiatives, censorship of the internet and the enactment of cybersecurity legislation that frequently erodes the rights of individuals (Deibert, 2020). One of the biggest challenges to defining sovereignty in cyberspace is the problem of attribution the challenge of attributing perpetrators of cyberattacks with certainty. In contrast to conventional warfare, where the origin of an attack tends to be apparent, cyber operations may be carried out anonymously, and it may not be easy to hold aggressors responsible (Rid & Buchanan, 2015). This attributability sets a risky precedent, as states and non-states can carry out cyberattacks with little chance of retaliation. Future legal systems should include mechanisms of cyber attribution, including international collaboration on digital forensics, standardized attribution protocols and the establishment of impartial investigative organizations that evaluate cyber incidents (Lindsay, 2020). Enhanced attribution capacities will be necessary in preventing cyber aggression and making states accountable for hostile cyber operations. Besides legal structures, future debates on sovereignty in cyberspace need to consider the role of private corporations in determining digital governance. The establishment of international regulatory regimes that make corporations answerable for protecting data, disinformation and cybersecurity incidents will be imperative in having a fair and secure digital world. In the end, the destiny of sovereignty and international law in cyberspace will be in the hands of states' willingness to cooperate and evolve according to the realities of the digital era. Although national security interests and geopolitical competitions tend to hold back progress, the growing gravity of cyber threats calls for immediate action. Lack of well-defined legal norms has brought about a space in which states, non-state actors and private enterprises exercise limited responsibility, resulting in increased instability in the cyber sphere. In the future, the international community must take precedence to ensure the crafting of legally binding accords governing cyber warfare, securing digital rights and establishing a system for cyber attribution and dispute resolution. The digital age has fundamentally altered the concept of sovereignty and international law must evolve accordingly to ensure security, stability and justice in the cyber domain.

Recommendations for the Scope of Future

Technological development proceeds at an unrivalled pace, and along with it, new challenges face the conventional state of sovereignty and international law. The advent of technologies such as artificial intelligence (AI), internet of things (IoT) and 5G networks has had a critical influence on cyber warfare and on the concept of sovereignty in the cyber world. These technologies have blurred state and non-state actor distinctions in cyber warfare, and it has become challenging for conventional legal norms to catch up. For example, AI and machine learning technologies can be applied to automate cyberattacks, thus accelerating the pace, scope and complexity of these operations. These technologies test the concept of 'attribution' because they complicate tracing the origin of an attack. When the infrastructure of a state is hit by an AI-powered cyberattack, it is challenging to attribute the attack to a given nation-state, making it difficult to apply conventional international law principles, including the law of armed conflict and the principles of sovereignty. Additionally, the mass production of IoT devices has raised alarms regarding data privacy and digital sovereignty. The connectivity of devices across personal, public and military domains has made them as likely targets for cyberattacks. The issues necessitate the creation of international standards and agreements to mitigate the application of such technologies under the umbrella of cyber warfare and ensure that states have control over their critical infrastructure. Therefore, the accelerated technological progress demands that sovereignty in the modern era be reassessed, challenging the international community to formulate new paradigms that can respond to the risks and challenges posed by such innovations. Legal academics and cybersecurity specialists must collaborate in offering recommendations that ensure sovereignty is protected as well as enhance international cooperation in cyberspace.

National Responses and Legal Frameworks

As a reaction to the increasing danger of cyber warfare, states have begun to establish their own national legal frameworks for dealing with these issues, even though the success of these efforts is highly varied. For example, the USA has developed an all-encompassing cybersecurity framework through the Cybersecurity Act of 2015 and its amendments, which seek to safeguard critical national infrastructure, enable information sharing between the private sector and government and upgrade the country's cyber defence. Yet, while these measures are strong at a national level, they do not always take into account the global nature of cyber warfare and international cooperation. In the same way, China has adopted a strong approach to cybersecurity with its Cybersecurity Law, which came into effect in 2017, to defend its cyberspace sovereignty. Conversely, European nations have taken a more collaborative stance through measures such as the *General Data Protection Regulation* (*GDPR*), which regulates data protection and privacy in the European Union. Although the *GDPR* is more concerned with data protection than cyber warfare, it demonstrates Europe's dedication to promoting digital sovereignty while safeguarding

individual rights and encouraging international cooperation on cybersecurity matters. The variation in national approaches underscores the difficulty of reconciling sovereignty with the necessity of international cooperation in confronting cyber threats. While each nation's legal system addresses its own national security issues, there is minimal consistency in the treatment of cyber warfare under international law. This fragmentation requires the development of more integrated international legal frameworks that not only harmonize domestic laws but also foster increased cooperation in preventing, countering and responding to cyberattacks. Additionally, certain countries have moved to strengthen cyber defence by setting up national cyber agencies, including the UK's National Cyber Security Centre and India's Computer Emergency Response Team (CERT-In). These agencies are of critical importance in tracking and dealing with cyber threats, but their usefulness is based on cross-border cooperation since cyber threats are transnational by their very nature. Thus, although national frameworks are important, they need to be integrated with international law so that there can be a more coordinated and consolidated response to cyber warfare. In summary, national legal structures are an essential component of tackling cyber threats but cannot be stand-alone.

Limitations

This research analysis is primarily conceptual and qualitative in nature. It does not include quantitative data, state-level policy surveys or cybersecurity datasets. The focus has been on interpreting existing legal and ethical frameworks rather than measuring their practical outcomes. Future research could build upon this work by integrating empirical evidence, cross-regional comparisons and field-based policy studies to strengthen the link between theory and state practice. While this study aims to offer a holistic and interdisciplinary understanding of sovereignty in the age of cyber warfare, certain limitations remain. Moreover, the discussion focuses largely on global and state-level dynamics, leaving limited space for regional or non-state perspectives, such as the role of private corporations, tech industries and civil society. The rapid evolution of cyber technologies and shifting geopolitical alignments also means that some conclusions may require future reevaluation. These limitations do not weaken the study's contribution but rather highlight areas where further interdisciplinary research integrating law, ethics, computer science and international relations can offer more grounded and policy-relevant insights.

Ending Comments: A Call for Global Reform

The swift growth of cyberspace and the advent of cyber warfare have radically questioned traditional concepts of state sovereignty and the application of international law. As states increasingly conduct cyber operations, the global community stands at a juncture where conventional legal structures are inadequate to meet the challenges and threats of the digital environment. Against this backdrop, the need

to rethink and redefine sovereignty in the cyber warfare age for the sake of global stability, security and human rights becomes paramount.

A key element of this redefinition is that a new, overall international legal framework addressing cyber warfare, state behaviour in cyberspace and digital infrastructure protection needs to be formulated. Existing legal tools, like the Tallinn Manual, offer some direction but are not legally binding and are not globally accepted. These new legal frameworks should place special emphasis on protecting civilians and civilian infrastructure from cyber aggression and hold responsible those who partake in aggressive cyber activities. International cooperation cannot be overemphasized. Cyber threats know no borders, and one country cannot adequately deal with these threats separately. Diplomatic discussion and multilateralism are necessary in establishing a joint environment whereby states exchange information, learn best practices and collaborate in joint cyber defence efforts. Only through global cooperation will the international community be able to create a cooperative system of dealing with cyber threats without infringing on national sovereignty. In addition, the changing nature of cyber warfare demands a harmonious balance between national security and human rights. As governments increase control over their digital systems, the international community must make sure that efforts undertaken in the name of cybersecurity do not compromise fundamental human rights. Cyber sovereignty, as important for national security as it is, must not be at the expense of personal freedoms. Looking to the future, it is important to recognize that the age of the computer has fundamentally changed the idea of sovereignty. Finally, the imperative for reform in international law to address the realities of cyber warfare is pressing. As the world of cyberspace becomes increasingly critical, the world community needs to move fast in establishing a cyber law that equilibrates national interests and international cooperation as well as guarantees the basic human rights of persons in cyberspace. Redefined sovereignty in cyber warfare is not only about catching up with advancing technology but also about guaranteeing that justice, peace and stability principles prevail in the information age.

Global governance in the future in the virtual world rests on states' willingness to work together, come up with innovations and build legal structures safeguarding both sovereignty and human dignity in an interdependent world.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The authors received no financial support for the research, authorship and/or publication of this article.

References

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.

Deibert, R. J. (2018). *Reset: Reclaiming the internet for civil society*. House of Anansi Press.

Deibert, R. J. (2020). The road to digital unfreedom: Seven challenges to democracy in the digital age. *Journal of Democracy*, *31*(1), 25–39.

Greenwald, G. (2013). *No place to hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, *100*(4), 817–885.

Held, D., & McGrew, A. (2007). *Globalization/anti-globalization: Beyond the great divide* (2nd ed.). Polity Press.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Keohane, R. O. (2002). *Power and governance in a partially globalized world*. Routledge.

Klabbers, J. (2013). *International law*. Cambridge University Press.

Krasner, S. D. (2001). *Sovereignty: Organized hypocrisy*. Princeton University Press.

Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security*, *39*(3), 7–47.

Mueller, M. (2010). *Networks and states: The global politics of internet governance*. MIT Press.

Nakashima, E. (2018). Russian military was behind 'NotPetya' cyberattack. *The Washington Post*.

Osiander, A. (2001). Sovereignty, international relations, and the Westphalian myth. *International Organization*, *55*(2), 251–287.

Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37.

Schmitt, M. N. (2013). The international law of cyber warfare. In M. E. O' Connell (Ed.), *International law and the use of force: A case-based approach* (pp. 257–279). Cambridge University Press.

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Shackelford, S. J. (2014). *Managing cyber attacks in international law, business, and relations*. Cambridge University Press.

Shackelford, S. J. (2017). *International cybersecurity law*. Edward Elgar Publishing.

Tikk, E. (2010). *International cyber incidents: Legal perspectives*. NATO Cooperative Cyber Defence Centre of Excellence.

Tikk, E. (2015). *International law and cyber operations*. NATO Cooperative Cyber Defence Centre of Excellence.

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