International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 25-05-2025, Accepted: 24-06-2025, Published: 25-07-2025
Volume 11, Issue 7, 2025, Page No. 90-99

International law jurisdiction in cyberspace: Navigating legal frontiers in the digital domain

Simar Sharma
Department of Law OP Jindal Global University Jindal Global Law School, Sonipat, Haryana, India

Abstract
The lack of effective international legal instruments in cyberspace has been heavily debated in theoretical and policymaking discussions, as the complexity of cyberspace make it impossible for participants to reach agreements, let alone create agreeable enforceable law. This paper delves into finding the relevant sources of international law applicable to cyberspace and the possibilities of encapsulating the complex dimension of the digital domain within a legal framework by comparing to existing sources and legal regimes and perusing over future possibilities of a codified law. This paper shall explore the spheres of customary law and state practice as well as the international conventions on cybersecurity in an attempt to mark the boundaries of international law and its jurisdiction over the digital realm.

Keywords: Jurisdiction, cyberspace, budapest convention, regulation of cyberspace, international law, un cybercrime treaty

Introduction

The 21st century has seen the growth of international law in various spectrums of the world incorporating the development of the changing times. One of the largest developments seen in the 21st century is the development of cyberspace, and with it, cybersecurity is increasingly taking centre stage in various aspects including world economy, geopolitics, international security and law. With this development, defence mechanisms, communications, as well as security measures of nation states have been revolutionized. However, with the fast growth of cyber technology, the need for a robust legal framework adjudicating on matters of cyberspace has also risen. International law is traditionally developed to regulate relations between nation states and hence faces various obstacles in making laws that can adopt to the intricacies of cyberspace.

In 2012, the U.N. Group of Governmental Experts (GGE), which is composed of representatives from 15 States, reiterated the U.S. conclusion that international law, and in particular the U.N. Charter, applies to State activity in cyberspace. However, the lack of borders in the domain of cyberspace and its dynamic spatio-temporal nature allows it to operate outside the confines of traditional territorial jurisdiction used in regulating the criminal as well as civil laws in international disputes. The application of legal norms and principles as well as the question of jurisdiction has become a recurring subject for scrutiny and debate in various platforms. Apart from a few exceptions, international law does not yet have specific rules tailor made for the regulation of cyberspace. Apart from its extraterritorial aspect, the technology is also novel and dynamic, hence for a long time, there were doubts on whether international law could even apply to cyberspace at all.

With this paper, I aim to delve into the evolving jurisprudence of international law in cyberspace to explore and navigate through the complexities of regulating the digital domain. This paper shall explore the question of jurisdiction in cyberspace, the application of key legal principles and the various sources of law regulating cyber security and the digital realm. This paper shall address the evolving threats and challenges of cyberspace and also look into the existing legal framework revolving around this domain. With the help of scholarly articles, precedents, legal principles and global discussions I aim to advance the cause of international law and global security in the digital age.

What is Cyberspace

Before diving into the complexities of outlining the jurisdiction of cyberspace it is important to understand what cyberspace is as well as how principles of jurisdiction are applied. Cyberspace is the environment in which communication done over computer networks occurs and almost everyone is connected to it in one way or another. Cyberspace has been in or dictionaries for over two decades, being redefined and modified over the years. But in simpler words, it represents the new age medium of communication that takes place in an intangible state. It is a borderless phenomenon which defies the physically marked geographic territories. Cyberspace can cut through distance by allowing people to connect virtually regardless of the physical distance between them. This creates a crucial gap in applying the principles of jurisdiction to the cyberspace.

Moreover, cyberspace has provided the world with a space where everyone and everything is connected. Cyberspace is made up of interconnected physical systems with a variety of linkages inside the physical sphere. This characteristic of cyberspace makes it all the more difficult and complex to understand. Individuals and companies may own some physical systems and interconnections, but cyberspace cannot be owned collectively. This is exacerbated by cross-jurisdictional boundaries and attribution issues, which have challenging theological, legal, and practical repercussions [1].

Jurisdictional Principles and Cyberspace

There are broadly six generally accepted principles of jurisdiction under international law. These include subjective territoriality, objective territoriality, nationality, protective principle, passive nationality and universality.

Territoriality is considered to be the preferred basis for jurisdiction. Subjective territoriality is the direct principle where, if an activity takes place within the territory of a

nation state, then that nation state has to jurisdiction to prescribe the rule. Objective territoriality on the other hand is invoked when an activity takes place outside the territory of a nation state, but the primary effect is within that state. Apart from territoriality, nationality also forms a basis for jurisdiction where the nation state asserts the right to prescribe the rule based on the nationality of the person doing the act. Passive nationality asserts jurisdiction on the basis of the victim's nationality. The protective principle is mainly invoked where the victim is the sovereign itself. The Protective principle stipulates that a sovereign may penalise conduct in other territories if it perceives a threat by such conduct. The final basis of jurisdiction is universality. Universal interest jurisdiction gives a right to any sovereign to capture and punish offenders in relation to certain universally declared crimes. These have extended to most jus cogens such as slavery, genocide, etc [2].

Analysing international conflicts of law typically involves weighing opposing governments' interests to determine whether or not there is jurisdiction to prescribe. While subjective territoriality typically takes precedence over other interests, a strong state interest in safeguarding its citizens may override a weak state interest in punishing the crime on its own territory. These principles cannot be applied as is to cyberspace due to the borderless and intangible nature of cyberspace.

For law in cyberspace, there are two kinds of actors, the uploader (one who puts information into cyberspace) and the downloader (the one who takes out information from cyberspace). International actors have often attempted to apply territoriality principle to establish jurisdiction over cyberspace activities. Article 22(1) of the Convention on Cybercrime of 2001, by the Council of Europe aimed to attribute jurisdiction to offences committed within the territory of the nation state. However, determining whether or not an offence in cyberspace has been committed within a particular state's territory is not a simple task [3]. Hence the territoriality principle is often rejected in the aspect of cyberspace.

After territoriality, nationality of the offender is a major basis for establishing jurisdiction over cyberspace acts. An example of this is in the Netherlands' provisions for specific cybercrimes like forgery, child pornography, etc. Under these laws, offences committed abroad by its nationals are punishable in the State [4]. Nationality of the victim can also be considered to be a deciding factor for jurisdiction. However, this can lead to similar results as territoriality principle would where countries could claim jurisdiction over content related offences since one of the affected parties is their national.

The Protective principle when applied to cyberspace allows States to assert their jurisdiction over acts that have a significant impact on their national security regardless of where the crimes originate. This principle underlines the need for national security in the cyber realm where physical boundaries are often defied. For example, Tanzania's Cybercrimes Act of 2015 outlines that any act committed by the use of any system within the State or which is directed against the State's infrastructure can be prosecuted under its laws, regardless of the offender's location [5].

For a few limited and specific offences, States can also assert universal jurisdiction. For specific cybercrimes, various states have framed provisions for universal jurisdiction, like in Belgium and Germany the circulation or distribution of child pornography can be prosecuted with universal jurisdiction [6].

Legal Frameworks in Cyberspace

Every legal framework in international law can be rooted back to its source of law. Article 38 of the ICJ statute lays down 4 main sources of international law; (1) international convention or treaties , whether general or particular, establishing rules expressly recognized by the contesting states; (2) international custom, as evidence of a general practice accepted as law; (3) the general principles of law recognized by civilized nations; (4) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law [7]. These sources form the basis of every law, regulation or legal framework found in the realm of international law, and so would similarly also form the basis for the regulation of cyberspace. The question then arises on the applicability of these sources to the digital domain.

Customary international law develops from state practice and opinion juris. Only when there is a general and consistent practice of nation states which is followed out of a sense of a legal obligation is it considered to be legally binding. Without consensus there can be no international law even in cases which may seem to be straightforward. Treaties on the other hand serve as formal binding agreements on all nations that are parties to them or have ratified them. General principles, form the bedrock of any legal framework and form the base of universal standards. These principles play an important role in helping bridge the gaps left by customary law or conventions.

Customary Law

Despite what many people think, international law is not primarily established through treaties. International law combines historical practices, traditions, and formal agreements between governments. Customary international law takes precedence over treaties and conventions in emerging legal areas. Customary international law stems from governments' continuous behaviour, which is motivated by a sense of legal obligation. When this happens, customary law becomes legally binding on nation-states.

While there does exists a framework of customary law reflecting an extensive and practically uniform conduct of nation states, this framework cannot directly be applied to the cyberspace as the actions and the effect of those actions available to both state as well as non-state actors in cyberspace don't coincide with the traditional principles of governance. In such absence of a structured legal regime, it is important to use the existing framework for conventional laws and use what can be applied to the cyberspace.

The creation of cyberspace led to the creation of not only new actions but also a new sphere where these actions took place. To establish state practice, a few known examples can be used. One of the first ever cyber-attacks took place in the Soviet Union in 1982, when a trans-Siberian pipeline explosion was caused by a computer malware that the CIA implanted in the Canadian software, allegedly expecting it to be stolen by Soviet agents. However, due to the embarrassment that would have to be suffered by USSR for stealing the software, the facts were concealed, and USA was never publicly accused [8]. Another significant incident was in 2010 when Google reported that their systems were

hacked into by Chinese hackers who had stolen their intellectual property. It was later found that more than 20 other companies had also been targeted by these hackers [9]. The second incident in 2010 revolved around Stuxnet, a computer worm that replicated from computers using the Windows operating system. This worm was found on various computer systems around the globe and was seen to target a supervisory control and data acquisition system created by Siemens. The target was speculated to be one of Iran's power plants, but the Iranian government never accepted these speculations [10].

Such major incidents that have occurred since the Siberian pipeline incident pave the way for setting precedent for what nation states count as acceptable cyber actions. No particular international legal body has been set up for collecting and analysing evidence to determine the intent of another state's cyber activity. When a state is made aware of a cyber intrusion, it must make a choice whether to declare it an attack or merely an espionage [11]. International law functions under its separate set of rules established by consent. The law of war, for example, is analysed fundamentally on the basis of the effects of the action. The intent of the actor acting against another state is practically irrelevant for international law analysis. Leading back to the current regime regulating activities in the cyber space. However, the distinct nature of cyberspace makes it difficult to frame a clear distinction between intrusions for reasons of collection and those of a more severe nature.

In a general sense, cyberspace can be considered to be a permissive regime where very little is prohibited. States can prohibit cyber activities with the help of their national laws, but in the international regime, activity cannot be prohibited in the cyberspace unless it appears above the level of a use of force. Aggressive cyber activities that lead to kinetic effects like damage or injury can be covered by law under the use of force and armed attacks. Although determining what would constitute as a kinetic effect is another debated topic that would be covered later in this paper.

Treaties and Conventions

Treaties and conventions form another prominent part of the sources of international law under article 38 of the ICJ statute. While these form a codified source of law, most treaties are only binding on States that are a party to the treaty. It is crucial to have a treaty or a convention regulating and penalizing cybercrime to tackle the growing rate as well as to help improve coordination and cooperation between nation states.

Budapest Convention

The Council of Europe's (CoE) Cybercrime Convention, also known as the Budapest Convention, is the only legally binding international multilateral convention on the domain of cyberspace [12]. It was open for signature by member states as well as the non-member states who took part in its development in 2001 and finally came into force in 2004. The Convention sought to provide a comprehensive response from the outset, addressing concerns about substantive offences, procedural procedures, and international coordination.

This Convention aims to harmonise national legislation, enhance cybercrime investigation tools, and strengthen international collaboration. It also advises signatories on the national-level measures required to combat cybercrime, such as revisions and additions to substantive and criminal procedural laws. The Convention also provides signatories with instructions on mutual aid and serves as a mutual legal assistance treaty for states that do not have one with the nation seeking assistance. Another significant feature is that it recognizes the crucial role of cooperation between states and private actors in combating cybercrime as well as the need to safeguard legitimate interests in both the use and the development of ICT.

This convention is the first international treaty on crimes committed through the medium of computer networks. It deals mainly with child pornography, violations of network security, copyright infringements, and computer related frauds and also lays down procedural laws regarding collection of evidence, search and seizure of stored computer data, real time collection of traffic data and the interception of content data. The potential inclusion of additional content-related offences, such the dissemination of racist propaganda over computer networks, was deliberated by the committee that drafted the Convention. However, the committee was unable to agree on criminalising such action. Although there was widespread agreement for making this a criminal offence, some delegations raised concerns about its impact on free expression [13].

The Budapest convention established its boundaries of jurisdiction to be restricted to when the crime was either committed in its territory, on board a ship or plane of the party or by one of its nationals [14]. Moreover the convention laid down principles of international cooperation which included provisions for extradition and mutual assistance. The main aim of the convention as it stated in its preamble, was to pursue a common criminal policy for the protection of the society at large against cybercrime by adopting proper legislation and promoting cooperation among nation states. It aimed to improve the means to tackle computer related crimes by establishing a common minimum standard of relevant offences. This Convention was the first step in codification of laws in the dynamic area of cyberspace. In 2003, some State parties ratified the Budapest Convention to include a protocol criminalizing acts of a racist or xenophobic nature committed through computer systems [15].

UN on Cybercrime

Since May 2021, member states of the UN have been in negotiations for an international treaty to counter cybercrime. The UN passed a resolution in December 2019 which led to the establishment of an open-ended ad hoc committee with the task of developing a comprehensive international convention to counter cybercrime while taking into account the existing international instruments and ongoing efforts at national as well as global levels [16]. The Ad hoc committee met a total of 6 times for negotiations, but as of yet no concrete decision has been arrived at. 5 years gave past, and negotiations are still pursuant with the members not able to arrive at an acceptable consensus. When the representatives gathered for the concluding session in February 2024, the decision was again postponed to a later date. The meetings addressed all relevant aspects of the treaty, ranging from international cooperation to preventive measures as well as the implementation of. The main areas of dispute in the convention are the possible scope of the treaty, addressing gaps in state capacity, human

rights safeguards [17]. It was proving difficult to decide whether the treaty should cover all possible criminal acts that can take place through computer networks, or whether it should be limited to core cyber-dependant crimes and few cyber-enabled crimes that have been dramatically transformed by digitalisation like child sexual abuse and exploitation. While it would provide for a limited scope, advocating states argued that an all-inclusive treaty would be more at risk of being abused or misinterpreted. While the treaty could become the most significant global legal framework in the digital realm as the first ever binding UN convention on cyberspace, without a clearly defined scope and sufficient safeguards, it could backfire and become a danger to human rights and global governance as a whole. There are various concerns that need to be addressed in the proposed treaty such as its failure to incorporate protections for whistleblowers, activists, security researchers, etc. Moreover, it does not have enough references to state obligations under international human rights law

The reconvened concluding session of the United Nations (UN) Ad Hoc Committee (AHC), meeting in New York on August 8, 2024, reached agreement on the "Draft United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes [18]. Reaching such consensus on an extremely complex matter of cyberspace is a crucial achievement.

Regional Conventions

Over the course of the negotiations for a universal convention on international norms for the regulation of cyberspace, various regional frameworks have come into play.

In 2014, the African Union adopted a legal framework in its Convention on Cyber Security and Personal Data Protection also known as the Malabo Convention [19]. However the convention only came into effect in June 2023, when ratified the Convention completing the requirement of 15 ratifications in May 2023 [20]. The convention covers a vast variety of issues related to cyberspace activities. It criminalizes a wide range of cyber activities like identity theft, hacking, fraud, etc., while also laying down provisions for prosecution and other procedural aspects. The Convention also recognizes the Right to privacy and provides framework for the protection of personal data. It also reinforces the principles of fair lawful and non-fraudulence in the collection of personal data. It also emphasizes on right to information, right to access to such information as well as the right to object to every individual whose personal data is being collected. The Convention underlines the need of international collaboration in combatting cybercrime and safeguarding personal information. African countries, for example, must work together and with other countries to share information, provide mutual legal help, and extradite people [21]. Any business operating in Africa is required to comply with the provisions of the Malabo Convention. The main objective behind the convention is to address the need for a harmonized legislation on cyberspace in the African Union by establishing an efficient mechanism in each member state to combat violations caused by activities occurring in cyberspace.

The Arab League also introduced the Arab Convention on Combating Information Technology Offences in 2010 [22], whose primary objectives were not limited to cybercrime and cybersecurity but also further included information security (INFOSEC) of member states and national control over systems and content. Although the convention's provisions are helpful, they are not enough for an efficient regime because they restrict investigative activities, lack a unified strategy, and require cooperation from several law enforcement networks.

Initiatives pertaining to cybersecurity at ASEAN (Association of Soth East Asian States) arose in response to the widespread and disruptive character of cybercrimes in the area. At the 17th ASEAN Summit in 2010, the leaders of ASEAN adopted the Master Plan for ASEAN Connectivity. A strong and long-term plan to strengthen the region's institutional, interpersonal, and physical ties is achieved through the Master Plan. The Plan's "physical connectivity" component covers energy, transportation, and information and communications technology (ICT). The goal of this plan, which falls under strategy 6, is to hasten the growth of ICT services and infrastructure across all ASEAN member states [23].

The Master Plan on ASEAN Connectivity 2025 adopted in 2016 seeks to add value by complementing and synergizing the ASEAN Community Blueprints 2025 [24]. First and foremost, the Cyber ASEAN Framework is unique among current frameworks for evaluating cyber-capacity since it was created by Southeast Asians for Southeast Asia. Three guiding principles—local context and ownership, agency and autonomy, and public-private-people partnerships—are what give it its meaning and purpose. ASEAN also has other initiatives working to mitigate cyber risks and threats and regulate cyberspace activities.

Various laws and directives in relation to cyberspace have also been developed and implemented by some regional organizations. A case in point is the Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime of 2012 [25]. States in the SADC might use this law as a guide for creating substantive and procedural cybercrime laws. States are not required to cooperate legally because it is a model law. The SADC Protocol on Mutual Legal Assistance in Criminal Matters and the SADC Protocol on Extradition can be used by states that have cybercrime laws or are developing them to help coordinate and cooperate on international cybercrime investigations [26].

Sovereignty in Cyberspace

The Declaration of Principles adopted in 2003 at the World Summit on the Information Society stated that the policy authority for public policy concerns related to the internet is the sovereign right of the states [27].

Sovereignty is one of the primary concepts of statehood and presents itself as a bundle of rights and attributes possessed by a state in its territory to its exclusive use as well as in relations with other states [28]. The extending of national sovereignty to cyberspace is known as cybersovereignty. It is the dominance and autonomy that a state has over cyber infrastructure, entities, behaviour, and pertinent data and information within its borders based on its national sovereignty. Sovereignty encompasses both rights and responsibilities, whether in the real world or online. Countries must respect the fundamental principles and

general rules of international law and sincerely carry out their due obligations as outlined in international law while enjoying the rights derived from sovereignty in cyberspace, made more necessary by the interconnectedness and interdependence of nations in cyberspace

Territorial sovereignty encompasses a state's rights in regard to its land, aerial space, territorial sea and other maritime zones. Applicability of territorial sovereignty to cyberspace is a heavily debated topic since conventionally, violation of territorial sovereignty involves some sort of a physical intrusion across physical boundaries. Cyberactivity on the other hand, usually operate on an intangible, virtual dimension and interactions in the digital domain are mostly deterritorialized. The cyberspace does also consist of a physical domain, over which a state can exercise territorial sovereignty, like where the hard drives and infrastructures are stored [29].

While applying principles of sovereignty to the cyberspace it is crucial to accept the reality that in the online world, states constantly transit though each other's portals, frequently without specific consent, particularly state intelligence organisations. State cyber activity can 'access' other nations' territory in a number of ways, including for 'virtuous' goals such as the immediate defeat of a terrorist attack, without other states' knowledge, at least in real time. Under an open-ended view to sovereignty, such as that of the 'pure sovereigntist', state sovereignty would be theoretically in continual breach, with transgressions occurring with no response from governments. This would result in a higher risk of confrontation and escalation; hence it is expected of the states to maintain a wider concept of sovereignty when it comes to the cyberspace. Nonetheless, since an open-ended definition is also risky, it is important for international law to be applied objectively, but the absence of specified laws categorizing violations, increases the risk of subjective interpretation by states.

The Tallinn Manual 2.0 explored the possibility of identifying criteria for infringements of state sovereignty by referencing to a hierarchy of scenarios. This included physical damage or injury, loss of functionality of cyber infrastructure and activity below loss of functionality [30]. But in a practical view, physical injury as a result of cyber activity is much less common than the effects listed below it. This approach still faced the challenge of where to establish a *de minimis* threshold. Certain states advocated that while defining criteria, the harm caused should not be measured only in quantitative but also qualitative terms. So, while the principle of sovereignty does apply to a state's cyber activities, as it applies in the non-cyber context, the violation of sovereignty does not mirror the conventional laws of the non-cyber world.

Cyber Warfare and Law of Armed Conflict

In 2009, the NATO Cooperative Cyber Defence Centre of Excellence launched the Tallin Manual project. This project was the first of its kind and conducted a deep study on the application of international law in governing the activity in cyberspace [31]. The Tallin Manual was developed in two phases with the first release in 2013 and the release of the Tallin Manual 2.0 in 2017 [32].

Cyber warfare refers to warfare conducted in the cyberspace with a globally connected digital network. Under article 2(4) of the UN Charter, all member states are prohibited from the use of force against any other state [33]. Hence, it is dependent on the extent to which can cyber operations qualify as "force" within the meaning of article 2(4). According to the ICJ, the prohibition under Article 2(4) applies to any use of force irrespective of the weapons used [34]. Hence use of cyber operations as a tool to cause destruction or damage would amount to "force" under this definition. However, there is no specific threshold at which cyber activity would amount to an internationally wrongful threat or use of force.

It is also important to note that Article 2(4) of the UN Charter is solely directed to states and forbids the use of force in "international relations" between them. This means that any use or threat of force must be lawfully attributable to a state and directed against one or more other states. International law holds a state responsible for activities undertaken by individuals or entities operating on its behalf or with its authorization or endorsement. These individuals or entities are referred to as "state agents". Non-state actors are individuals or entities who do not operate on behalf of a state or have inadequate ties to the state to engage in international legal obligation. Hence, the use of force by individual hackers or other non-state actors while may be relevant under International Humanitarian Law, it is not prohibited under article 2(4). However, the international reactions to the 2007 attacks on Estonia showed that nations would not stand by and do nothing when states or non-state actors used the Internet as a weapon to undermine the sovereignty of its allies [35].

Article 51 of the UN charter permits the inherent right of an individual or group to self-defence in case of an armed attack. While the scope is narrower than Article 2(4), it does exceed Article 2(4)'s scope by including all armed attacks against a state irrespective of whether it was carried out by a non-state actor. However, this interpretation remains highly debated and hence does not depict a uniform consensus. Either way, qualifying a state-sponsored cyber operation as a "armed attack" allows the injured state to take self-defence action without violating UN Charter restrictions, including the use of military force within and outside the cyber domain. Attempts to apply the concept of "armed attack" to cyber operations face challenges in identifying the precise level that constitutes a threat or use of "force" under article 2(4) of the UN Charter.

The scale and impacts assessment are unavoidably context-specific, it must be stressed. In their Common African Position, the 55 member states of the African Union (AU) stated that deciding whether a cyber operation is large enough and has enough impact to be considered a use of force "should be undertaken on a case-by-case basis [36]. Accordingly, the experts in the Tallinn Manual concurred that when "its scale and effects are comparable to non-cyber operations rising to the level of a use of force [37], a cyber operation is at least a use of force [38].

Role of Non – State Actors

Today, governments, corporations, academic institutions, and civil society are recognised as the four primary stakeholders in cyberspace. All of the United Nations' member states have these stakeholders, however each one plays a different role in each of those nations. Of these four, governments are primarily in charge of establishing cyberspace regulations and utilising cyber technologies for public purposes inside their borders. Governments have an interest in and a duty to ensure successful international

collaboration in the interconnected global cyber environment. Businesses have a significant influence on how governments create national cyber policy and approach international collaboration on cyber challenges worldwide because of their emphasis on innovation and the use of cyber technology that they have trademarked or copyrighted.

Academic institutions are crucial to research and development, developing and conceptualising theories about cyberspace, and frequently collaborating with corporations to disseminate the outcomes of their endeavours. With a particular emphasis on the human element, both individually and collectively, civil society examines the effects of government, corporate, and academic activity in cyberspace. By emphasising the advantages and disadvantages of cyberspace, each of the four stakeholders contributes to raising awareness of cyber concerns from their unique points of view.

Non-state actors (NSAs) have played a bigger and more significant part in world affairs since the end of the Cold War; this trend is probably going to continue even as globalisation slows down. More capability and resources accessible outside governments, a more polarised and contentious global environment, and less flexible state institutions are all contributing to NSAs' increased influence in a variety of international spheres. These entities hold considerable economic, political, or social power on a national and even global scale, despite without having the same advantages and rights as politically autonomous players. NSAs with this kind of power have historically operated as separate actors with a distinct organisational structure, but more and more diffuse collectives and even individuals without a formal operational network or hierarchy are exerting influence on a larger scale and in a wider range of ways. Non-state actors have flourished in cyberspace due to its distinctive characteristics, such as its borderless nature, inherent interconnectedness, anonymity it provides, and accessibility. As a result, cyberspace has further enabled non-state actors to act independently of states in the international arena.

Moreover, in certain fields, the involvement of private sector proves to be essential, such as digital taxation, privacy, controls on social media content, etc. Internet governance has been the domain of a multistakeholder community. The members of the multistakeholders community increasingly expect to play a similar role in questions of international cybersecurity. Conversely, most governments had been content to leave internet governance to civil society and corporations, but now, as governance affects their economies and safety, some want a more prominent or even guiding role in the digital world. This confluence - it could even be described as a collision - over roles and responsibilities is complicated by China and Russia's differing visions for security, data governance, and sovereignty. The tensions between multistakeholders and government and between democracy and authoritarian views of digital governance complicate the discussions of the role of the private sector [39].

Various organizations in the American region have seen to engage in various public-private partnerships in cases of cybersecurity. The United States founded the largest multinational cyber cooperation in the world, known as the international Counter Ransomware Initiative (CRI)7 [40]. The CRI increases everyone's ability to combat ransomware, creates policy strategies to fight ransomware and upends the ransomware ecosystem. In order to prevent and stop ransomware and increase resilience against malevolent cyber actors, the International Counter Ransomware Task Force (ICRTF) unites operational, law enforcement, and policy organisations from all over the world. Despite being primarily an intergovernmental platform, it is gradually bringing together government organisations and business partners for more disruptive and defensive actions.

Through cutting-edge features and training, public-private cooperation can support the development of a strategic partnership and enhance national digital security. The PPP between Google Singapore and the Singapore Cyber Security Agency involves the development of a security feature in Google Play Protect that will prohibit hazardous apps and increase mobile security [41]. Additionally, the Agency formed independent collaborations with Google and Microsoft on cybersecurity and national cyber defence. Understanding that multistakeholder collaboration is essential in cyberspace, the collaborations will support capacity-building initiatives, exchanges on critical and emerging technologies like artificial intelligence, joint operations to combat cybercrime and malicious cyber activity, and the sharing of cyber threat intelligence.

Challenges in Incorporating PPPS on Cybercrime

While Public-Private Partnerships provide significant benefits in framing regulations, there are various challenges in fostering effective PPPs. Lack of trust is one such key challenge. Trust affects the promptness and manner in which requests are handled. Lack of trust can make it more difficult to share incident data, threat intelligence, best practices, and essential information, which in turn makes it more difficult to effectively combat cyberthreats. If there are worries about data protection, regulatory compliance, or reputational harm, the private sector may be hesitant to work with government organisations. Similarly, worries about data security, possible misuse of given information, and the possibility of reputational harm may make government institutions reluctant to provide sensitive information [42].

Establishing and maintaining PPPs may be difficult if collaborating organisations lack motivation, coordination, and alignment. Diverse stakeholder groups and actors have different goals, passions, and methods. While the commercial sector may concentrate on operational efficiency, intellectual property protection, and upholding customer trust, government organisations may prioritise defence and security goals. Programs and projects that overlap or compete can squander resources, fragment current efforts, irritate partners, overburden reporting or communication channels, and ultimately impede effective collaboration [43]. Various other challenges such as conflicting regulatory and legislative frameworks, lack of an efficient rule of law, or limited resources also cause hurdles in forming efficient and workable PPPs.

However, with proper mechanisms and efforts, these hurdles can be overcome. When stakeholders and governments actively participate, lead by example, produce outcomes, and encourage transparency, trust between them can be enhanced. Through encouraging interpersonal cooperation, face-to-face interactions, and shared ownership, PPPs must establish reliable networks that enable meaningful engagement and transparent communication. The greatest

methods for fostering trust between partners have been identified as frequent meetings, lively conversations, cooperative activities, and modern information-sharing platforms. Guided and equitable partnerships which are sensitive to the particular needs and concerns of marginalised or under-represented groups can be developed through including diverse groups. In order to guarantee that solutions are customised to the unique requirements and circumstances of the community, inclusivity should also include local organisations' involvement, boosting their local ownership, efficacy, and sustainability.

Human Rights in the Digital Realm

Human Rights form a part of general principles of law and are required to be maintained by all governing bodies in any situation. The UDHR (United Nations' Universal Declaration of Human Rights) along with the ICCPR (International Covenant on Civil and Political Rights) guarantee basic human rights and freedoms including freedom of expression, freedom of speech, the right to privacy, freedom of opinion, and freedom of association. Technological advancements in data surveillance, personal data control, and knowledge identification and organisation have led to the transfer of the topic of anonymity into the political arena. On the one hand, this has been accomplished through database management, and on the other hand, through the creation of postulates like "the right to anonymity" or "protection of privacy" through political actions.

One of the main challenges in governing the cyberspace is the possibility of violating human rights in the process. Investigations into crimes in the digital world can be highly invasive and threaten the right to privacy. The interception and collection of traffic data, the search and seizure of personal data and mishandling of such sensitive data by law enforcement agencies, all pose a risk of violating the privacy of the ones being investigated.

This issue was also one of the main concerns raised in the ad hoc committee of the UN [44]. While most of the member states agreed about the importance of taking human rights into consideration, others argued that the treaty is not a human rights treaty and hence consideration for human rights should be kept to a minimum. Advocates for human rights wanted the treaty to refer specific rights in its framework while the other states felt that a single article in the opening chapter would suffice [45]. Maintaining a balance between the obligations of the states under international human rights law and codifying a legal framework for global cybersecurity poses as an obstacle for the UN convention.

In various reports, GCEs (Group of Government Experts), who were tasked by the UN General Assembly to conduct research and report on existing as well as potential threats to cybersecurity have emphasized that all efforts made by states in pursuance of cybersecurity, work in adherence with respect for human rights and fundamental freedoms laid out in the UDHR as well as other such instruments.

Scope of International Cooperation

In order to improve confidence and security in the information society, the International Telecommunications Union (ITU), a United Nations organisation that is regarded as the "premier global platform by means of which stakeholders work towards an agreement on a broad range of issues pertaining to the future course of the ICT industry introduced the Global Cybersecurity Agenda.

India has also made several efforts in contributing to the international cooperation in regulating cyberspace. With an emphasis on a safe and welcoming cyberspace for sustainable development, India sponsored the Fifth Global Conference on Cyberspace in 2017. Promoting inclusivity and human rights in global cyber policy, defending the current state of an open, interoperable, and unrestricted cyberspace, establishing political commitment for capacity building initiatives to help countries and address the digital divide, and developing security solutions in a balanced manner that appropriately acknowledges the role of the private sector and technical community were the goals of the conference [46].

Harmonised national substantive cybercrime laws that criminalise cybercrime and national procedural cyber laws that establish the norms of evidence and criminal procedure are essential for international collaboration. Where necessary, harmonising bilateral, regional, and multilateral cybercrime instruments can also promote international cooperation. In order for regional and multinational cybercrime instruments to become legally binding, they must also be ratified or admitted. As long as dual criminality—that is, a provision in treaties requiring the accused action to be illegal in collaborating countries—exists, bilateral, regional, and multilateral treaties on cybercrime can enhance international collaboration. Cybercrime safe havens are established where offenders are shielded from prosecution in the absence of dual criminality and unified legislation. This was seen in the now-famous Love Bug virus case of 2000, in which the inventor and distributor were unable to face legal action since, at the time of the incident, their actions were not deemed criminal in the Philippines [47].

However, even in the absence of a rigorous interpretation of the dual criminality requirement, international cooperation might still be feasible.

The scope of cooperation on digital evidence that should be included in the treaty, which is related to human rights protection, has yet to be agreed upon. One alternative for the committee is a greater scope for cooperation on digital evidence, including for 'serious crimes' in general, which could be complemented with a narrow criminalization chapter and an agreement on how more crimes could be added to the treaty in the future. Enhancing the scope of electronic evidence cooperation to a broader and more ambiguous range of offences may introduce inherent human rights issues. General principles and Jus Cogens have also set universal standards for human rights that must be adhered to by any and all regulations around the globe.

The compromise presented in the Chair's offer includes Article 59(3), which partially reflects Canada's widely supported proposal to clarify Article 3's scope and prevent any misinterpretation of the treaty that could conflict with member states' broader obligations and responsibilities. Canada's proposal was a welcome call to uphold human rights while also reminding civil society actors of the risks

posed by this deal. As member states were unable to agree on the language, a notion that appeared to gather traction to include another provision, reflecting New Zealand's proposal for Article 37(15) - a non-discrimination clause for reasons of rejection. The advantage of this clause is that the reasons for refusal would apply to the entire chapter on foreign cooperation [48].

Way Forward

In my opinion, with the growth and development in technology, it is the need of the hour to come up with a legal framework to regulate the digital domain. The Budapest convention and the Tallin manual among other conventions constitute the first major step forward on this road, but a UN treaty will pave the way for legality and jurisprudence in the cyberspace.

While a new treaty is likely to be a powerful instrument in the global battle against cybercrime, it needs to be compatible with existing international processes and networks that function in similar environments. Even if member countries agree on a 'package deal', there is broad worry about the treaty's possible negative impact on internet rights and safety. The debate on the implications on regulating activities in cyberspace from the perspective of privacy, national security, sovereignty and autonomy has made it quite difficult for stakeholders in the international legal realm to reach a consensus.

The UN treaties combating transnational organised crime and corruption, which were unanimously approved by nearly all member countries, are essential components of current global responses against transnational crime. Many states propose incorporating and altering articles from previous agreements into the cybercrime treaty. More substantial debates arise over existing cybercrime instruments. For more than 20 years, the Council of Europe's Budapest Convention has endeavoured to define cybercrime and how law enforcement agencies should work together. Many states based their legislation on the conference. The UN treaty remains a muddled combination of both, which may explain why member countries had struggled for so many years to reach an agreement.

However, not all countries have ratified it. Some countries, such as Russia, have constantly contended that the Budapest Convention is not globally significant and undermines concepts such as state sovereignty and non-interference. This prompted them to advocate the resolution establishing the AHC, which was approved against objections from numerous Western states and civil society representatives. State proposals in the treaty process have also cited provisions from regional documents, such as the African Union's Convention on Cybersecurity and Personal Data Protection [49].

The consensus on the UN treaty on cybercrime is a huge milestone in the jurisprudence of international law in the regulation of cyberspace. However, it is also essential for the treaty to now be efficiently imposed on all member states and provide guidance for the states to form their own national and regional regulatory frameworks. By December 2024, significant decisions on the pact must be made. Notwithstanding its flaws, the draft convention was accepted as a compromise in the AHC and will be put to a vote in the current GA. Since nations had already approved the draft resolution during the AHC's reconvened closing session, the treaty's adoption is viewed as a formality. Additionally, a treaty is one of the few ways to show that UN multilateralism can heal state differences. However, considering the consequences of the treaty, its ratification could lead to long-term issues, influencing the vote and action of UN member states.

Conclusion

Globalization has dramatically increased expansion of cyberspace, which has brought new perspectives, both positive and negative, to interactions in communications, commerce and global relations. This paper sought to answer the critical question: How can the instruments found in international law best regulate the cyber-space environment and at the same time respect sovereignty, security and human rights? From jurisdictional analysis of principles, legal systems and new threats and risks, it is quite evident that much progress has been made but much more needs to be done in managing this complex virtual space.

Cyberspace is intrusive and nebulous thus making it hard to regulate directly with territorial jurisdiction and enforcement strategies. While concepts such as nationality and protective jurisdiction have been practiced, they cannot adequately address the cross-border nature and decentralization of cyberspace operations. The weakness of the current frameworks like the Budapest Convention proves that a standardized approach to cyber governance is required within the international community and should embrace the development of further problems ahead.

This problem is founded in the conflict between sovereignty and international cooperation. Sovereignty is an important principle of international law that now emerges as a problem in cyberspace as networks extend beyond state boundaries and yet remain invisible. Although the state must not relinquish ownership and management of their cyberphysical systems, integration and dependencies of cyberspace require collective processes to protect assets and deter nefarious actions.

As important as the promotion of the state sovereignty in cyberspace governance, there is the need to protect human rights as well. The right to privacy, freedom of speech and the right to be equal continue to be threatened by surveillance, hacking and unfair and racists algorithms. A legal context that will protect such rights in light of cybercrime and national security is crucial to uphold the public's confidence in the digital environment as well as to defend basic rights.

As highlighted above cyberspace remains dynamic, where citizens, civil society, organizations, and particularly the non-state actors exert significant control over cyberspace. It is for these reasons that the stakeholder voices presented here underscore the importance of coordinated multistakeholder governance processes that allow for the drawing on various sources of knowledge and capabilities. There is still lack of the matter how mutually successful combined governance can be if it had purposeful public trust, coordinative accountability, and correct interaction between private sector and state agencies as well as regional conventions and new forms of cooperation.

The study emphasizes that only a solid multilateral convention with substrates that accords with existing initiatives, takes into account customary procedures, and responds to new challenges, can be the way forward. Any such treaty must offer adequate layers of security on the digital front as well as fair Internet connectivity on the one

hand while at the same time being versatile sufficient to adapt to generally emerging trends in technology on the other. The Persistent attempts of the United Nations in their attempt to come up with a global cybercrime convention is worrisome but the current states have been in a difficult position due to highly conflicting state interests and there are still deficits of capacity, enforcement, and human rights protection.

Therefore, the regulation of cyberspace with reference to international law is a need as it is a deep challenge. The answers to the research question are that a meaningful and coherent structure of legal regulation should be established to address sovereignty, security, and human rights and create a climate of cooperation and fairness based on the digital transformations. With the ever-changing advances in technology, the international community must continue to work toward the goal of protecting cyberspace as an open society environment that would embrace innovation, cooperation, democracy, freedom, security, and justice.

References

1. Peter Ladis Kumar Gaurav, Nilesh K Modi. Cyber Space and Its Governance, 2020, 22–23.
2. Darrel C. Menthe. Jurisdiction in Cyberspace: A Theory of International Spaces. Mich. Telecomm. Tech. L. Rev,1998:4(69):71–73.
3. Susan W. Brenner Bert-Jaap Koops. Approaches to Cybercrime Jurisdiction. J. High Tech. L,2004:4(1):10.
4. Wetboek van Strafrecht (Dutch CC). Tanzania, 2015. Cybercrimes Act.
5. Susan W. Brenner Bert-Jaap Koops. Approaches to Cybercrime Jurisdiction. J. High Tech. L,2004:4(1):28.
6. Statute of the International Court of Justice, art, 38, 1.
7. Davis P. The Farewell Dossier: A Look Back at The Cold War Spy Code Named Farewell. Paul Davis on Crime, 2013.
8. Nakashima E. Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say - The Washington Post. Washington Post, 2013. https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html accessed 12 May 2024.
9. Zetter K. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Wired, 3 November 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ accessed, 2024.
10. Brown G, Poellet K. The Customary International Law of Cyberspace. Strategic Studies Quarterly,2012:6(3):133.
11. Convention on Cybercrime (ETS No. 185) (Budapest convention).
12. Explanatory Report, Convention on Cybercrime, opened for signature 23 November 2001, ETS 185 entered into force, 2004. ('Convention Explanatory Report').
13. Convention on Cybercrime (ETS No. 185) (Budapest convention) Art. 22.
14. ETS. Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems, 2003, 189.
15. Wilkinson I. What Is the UN Cybercrime Treaty and Why Does It Matter? | Chatham House – International Affairs Think Tank. Chatham House. https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter accessed, 2024.
16. Wilkinson I. What Is the UN Cybercrime Treaty and Why Does It Matter? | Chatham House – International Affairs Think Tank. Chatham House. https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter accessed, 2024.
17. Council of Europe. United Nations Treaty on Cybercrime Agreed by the Ad Hoc Committee. Cybercrime, 2024. https://www.coe.int/en/web/cybercrime/-/united-nations-treaty-on-cybercrime-agreed-by-the-ad-hoc-committee accessed, 2024.
18. African Union Convention on Cyber Security and Personal Data Protection, 2014. (EX.CL/846 (XXV).
19. Sheik S. Au Convention on Cyber Security and Personal Data Protection: Malabo Convention. Michalsons, 2023. https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281#:~:text=and%20stored%20securely.-,Cooperation,mutual%20legal%20assistance%2C%20and%20extradition. Accessed, 2024.
20. African Union Convention on Cyber Security and Personal Data Protection, 2014. (EX.CL/846 (XXV).
21. Gastorn Kennedy. Relevance of International Law in Combatting Cybercrimes: Current Issues and AALCO's Approach. Presentation at the 4th World Internet Conference, Wuzhen Summit) International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes, 2017, Wuzhen, China.
22. ASEAN's Perspective on Cyber security. ASEAN-India Conference on Cyber Security in New Delhi, India.
23. Association of South East Asian Nations, 2015.
24. Master plan on ASEAN Connectivity 2025, The ASEAN Secretariat, Jakarta, 2016, 20.
25. SADC Model Law on Computer Crime and Cybercrime of, 2012.
26. Katharina.kiener-Manu. Cybercrime Module 3 Key Issues: International and Regional Instruments. Cybercrime Module 3 Key Issues: International and Regional Instruments. https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html accessed, 2024.
27. Chinese Academy of Social Sciences and Cybersecurity Association of China. Sovereignty in cyberspace: Theory and practice. https://news.whu.edu.cn/__local/2/C8/10/626E74BC31FF85C4DCCFC8745F6_352641B6_40029.pdf accessed December, 2024.
28. Corfu Channel Case (United Kingdom v. Albania); Separate Opinion, 1949, ICJ Rep 43.

29. Moynihan H. 2. the Application of Sovereignty in Cyberspace | Chatham House – International Affairs Think Tank. Chatham House, 17 December 2020. https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace accessed, 2024.
30. Schmitt MN. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd edn, Cambridge University Press, 2017, 11–29.
31. Schmitt M, Pakkam AS. Cyberspace and the Jus ad Bellum: The State of Play. INT'L L. STUD,2024:103:194.
32. Schmitt MN. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd edn, Cambridge University Press, 2017, 11–29.
33. UN Charter, Art. 2(4).
34. International Court of Justice. Legality of the Threat or Use of Nuclear Weapons, advisory opinion, 1996: 39; and Ian Brownlie, International Law and the Use of Force by States, 1963:362: 431.
35. Herzog S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security,2011:4(2):49–60. [suspicious link removed].
36. African Union Peace and Security Council. Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, at, 2024, 7.
37. Schmitt MN. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd edn, Cambridge University Press, 2017.
38. Schmitt M, Pakkam AS. Cyberspace and the Jus ad Bellum: The State of Play. INT'L L. STUD,2024:103:194.
39. Lewis J. Private Actors' Roles in International Cybersecurity Agreements – Unlearned Lessons. CDR,2022:7(1):33-33.
40. International Counter Ransomware Initiative. https://counter-ransomware.org.
41. Zulhusni M. Google and the Cyber Security Agency of Singapore Forge A Strategic Alliance. Tech Wire Asia, 2024. https://techwireasia.com/2024/02/google-singapore-teams-up-with-csa-for-enhanced-mobile-security/ accessed 26 December, 2024.
42. Public-private partnerships on Cybercrime. https://www.unodc.org/documents/NGO/PDF/CSU-CyberCrime-240807-WEB.pdf accessed, 2024.
43. Id.
44. Brookbanks D. A Dream Deferred or a near Miss? UN Committee Postpones Decision on Cybercrime Convention. Global Initiative, 2024. https://globalinitiative.net/analysis/un-committee-postpones-decision-cybercrime-convention/ accessed, 2024.
45. Wilkinson I. What Is the UN Cybercrime Treaty and Why Does It Matter? | Chatham House – International Affairs Think Tank. Chatham House. https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter accessed, 2024.
46. Amb (Retd) Asoke Mukerji. Distinguished lectures details. https://www.mea.gov.in/distinguished-lectures-detail.htm?743 accessed, 2024.
47. White G. Love Bug's Creator Tracked down to Repair Shop in Manila. BBC News, 3 May 2020. https://www.bbc.com/news/technology-52458765 accessed, 2024.
48. Brookbanks D. A Dream Deferred or a near Miss? UN Committee Postpones Decision on Cybercrime Convention. Global Initiative, 2024. https://globalinitiative.net/analysis/un-committee-postpones-decision-cybercrime-convention/ accessed, 2024.
49. African Union Convention on Cyber Security and Personal Data Protection, 2014. (EX.CL/846 (XXV).