Cyber Warfare and International Law: Rethinking State Responsibility in the Digital Age

Dr. Abida Hassan[1], Dr. Saeed Ahmed Butt[2], Muhammad Sohrab Saleem[3]

[1]Assistant Professor, Deptt of Dr. Muhammad Iqbal Law School GCU Lahore, Email: dr.abidahassan@gcu.edu.pk

[2]Assistant Professor, Government College University, Lahore, Email:saeedbutt@gcu.edu.pk

[3]Independent Researcher, Advocate High Court, Research focus on International Law, Criminology and Maritime Security, msohrabsaleem@gmail.com

Abstract:

Cyber warfare has emerged as one of the most significant security challenges of the twenty-first century, transforming cyberspace into a strategic domain of international conflict. Unlike conventional warfare, cyber operations involve anonymous actors, transnational networks, and advanced technologies that complicate attribution, accountability and enforcement. These developments challenge traditional principles of state responsibility as many cyber operations remain below threshold of armed attack while causing substantial political, economic, and social harm. This article critically examines applicability of international law to cyber warfare, focusing on state responsibility under United Nations Charter, customary international law, the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), International Humanitarian Law and International Human Rights Law. Using a qualitative doctrinal and comparative methodology, it analyzes major cyber incidents, including Estonia attacks (2007), Stuxnet (2010) and SolarWinds (2020). The study argues that although existing international law provides a basic framework for regulating state conduct in cyberspace, important legal and institutional gaps persist. It concludes by recommending stronger international cooperation, improved attribution mechanisms, clearer state obligations and development of a more coherent legal regime capable of addressing the evolving challenges posed by cyber warfare in an increasingly interconnected and multipolar international system.

Keywords: Cyber Warfare, International Law, State Responsibility, Cyberspace; International Humanitarian Law, United Nations Charter, Attribution, Cybersecurity, Digital Sovereignty, International Relations.

Introduction

International security has significantly changed in twenty first century, with digitalization having accelerated to a level that has made cyberspace an integral part of governance, e-commerce, communication and national defense. Cyberspace is also a strategic environment, which, together with land, sea, air and outer space is now a theatre of competition for political, economic and military gain for states. Digital technologies have contributed to innovation and global connectivity, but have also introduced new vulnerabilities, which can be seized by both state and non-state actors. Thus, cyber domain has emerged as one of most important security issues of modern-day international system and has transformed, influenced and blurred traditional notions of conflict, sovereignty, deterrence and state responsibility. Cyber operations are different from conventional warfare, in that they are anonymous, fast, transnational and relatively inexpensive to operate. They can attack, without deployment of armed forces, critical infrastructure, military networks, financial institutions, healthcare systems, electoral processes, and public utilities. These types of operations frequently raise question of what constitutes peace and what constitutes armed conflict, what is military and what is civilian and what is domestic and what is international. Cyber operations may have serious political, economic and social consequences, even if not armed attacks per se, including disruption of critical services, loss of public trust, and economic and/or economic and political instability. There are several significant cyber incidents that highlight increasing strategic importance of cyberspace. In 2007, Estonia's government, financial systems and media networks were targeted by cyberattacks, exposing vulnerabilities of digitally dependent societies. Stuxnet, a cyber weapon that was found in 2010, showed how damaging cyber weapons could be to critical infrastructure. In recent years, SolarWinds supply-chain compromise, mass ransomware attacks and cyber operations linked to Russia-Ukraine conflict have demonstrated how cyber weapons are becoming a part of geopolitical competition and contemporary military tactics. International law, however, has been lagging behind developments of technology, even though use of these tools in warfare is becoming more significant. While United Nations Charter does not specifically mention cyber operations, underlying principles of

Charter such as prohibition on use of force, respect for sovereignty, non-intervention and inherent right of self-defence can still be applied in cyberspace.

"Policymakers (but less so IR academics) have been attuned to the imperative of trying to make sense of these technological shifts for conceptions of global security, power, and order. There are too many significant policy implications to enumerate here but protecting critical infrastructure from cyber security vulnerabilities has been one of the more enduring concerns. Connecting critical infrastructure like energy plants, financial institutions, and transport systems to a global computer network comes with many opportunities for increased efficiency and lower costs which developed states have raced to exploit. But the relatively insecure nature of the Internet also introduces a range of vulnerabilities for those systems to be penetrated, manipulated, and damaged. The potential for such interference to lead to large-scale destruction and loss of life, coupled with speculation that state or non-state actors may pursue that potential in lieu of, or in addition to, conventional kinetic force, has led to a focus on cyber security in domestic and international politics. This has manifested in a number of ways, including the development of national cyber security strategies, the establishment of dedicated cyber security military units and doctrine, and in discussions on international cooperation on cyber security at head-of-state level. States are clearly concerned about the implications of digital technology for violence and conflict in international relations." (Madeline Carr, 2017)

In same way, articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) offer a general approach to state responsibility. These rules do not apply to cyber operations, however, because it is difficult to attribute action to a specific actor and because a perpetrator could use a proxy to carry out action and because he or she can hide his or her identity in multiple jurisdictions. The main legal concern is still attribution. To establish state responsibility, it is necessary to first find technical source of a cyber operation and then to find legal link with a state. Private contractors and state-sponsored cyber networks are used by states to maintain plausible deniability and attackers often use proxy servers, botnets, false flag operations and third-party infrastructure to mask their activities. All these factors make accountability and implementation of international obligations difficult. There are also substantial challenges to IHL in cyber realm. The concepts of distinction, proportionality, military necessity and precaution are not so easy to apply in context of a close interconnection between civilian and military digital infrastructure. Cyber operations against military targets could have an unintended impact on a hospital or transportation system, financial services or an energy grid, posing significant legal and ethical issues about protecting civilians. In response to such challenges, various efforts have been made to come up with more concrete rules for application of international law to cyberspace including Tallinn Manual 2.0, United Nations Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG). These measures are still not concrete and do not clear up disputes between great powers over issues of sovereignty, attribution and legal measures for responding to cyberattacks. The rise of new technologies such as artificial intelligence, self-driving cyber systems, quantum computing and internet of things, makes legal liability even more complex. This article suggests that principles of international law still remain relevant to cyber warfare, but they need to be further elaborated, institutionalized and normatively elaborated for a better regulation, accountability and peace and security among nations in digital age. The Course Leader's introduction to Cyber Warfare is a reflection of the concept.

2. Conceptualizing Cyber Warfare: Evolution, Characteristics and Strategic Significance:

Cyber-space has become a strategic domain with a profound impact on nature of international conflict and statecraft. Digital technologies have long entered realm of governance, military use, economic systems, financial markets and communication networks and critical infrastructure over past 30 years. At the same time, this reliance on digital connectivity has opened up new avenues for development, as well as new risks that can be used by adversarial parties. Thus, cyber warfare has emerged as a non-negotiable part of national security policies, military operations and foreign policy. Cyber warfare differs from traditional warfare, which takes place on battlefield and is fought through digital networks and computer systems. It includes a wide range of attacks both offensive and defensive in nature that are intended to interfere, alter, compromise, or compromise integrity of information systems and critical infrastructure. Apart from relative cheapness of cyber capabilities, strategic significance is the speed at which they can be acquired, anonymity they can offer, their scalability and their potential to generate strong political, economic and military impacts without need for a conventional armed conflict. (Rid, 2020) The study of conceptual bases of cyber warfare is crucial for comprehending legal dimensions and developing the doctrine of state responsibility in this new contested strategic environment.

2.1. Evolution of Cyber Warfare:

The beginning of cyber warfare can be traced back to rapid expansion of computer networks in late 20th century. The common types of early cyber incidents were by individual hackers or criminal organizations and they included espionage, computer hacking and information theft. In Cold War era, there is an increasing use of digital technologies in espionage and information collection by intelligence agencies, but cyber-related activities were still mostly stealth and small in scale. Internet commerce heralded a new era in 1990's and Internet became an integral part of national economies and public administration. Digital technologies started to be embedded in military command systems, financial systems, transportation and energy systems and health systems. The more things became connected, the more cyber threats transitioned from technical issues to national security threats. Terrorist attacks of 9/11/2001 greatly influenced thinking about security by emphasizing need to consider non-traditional threats. Terrorism was primary concern of international

security policy, but a growing number of decision makers were becoming aware that economic disruption via cyber attack could be as devastating as by military action. The states thus focused on development of their offensive and defensive cyber capabilities. The attacks on Estonia in 2007 were a watershed moment in international security. This was after political conflict over relocation of Soviet era Bronze Soldier monument to Estonia, leading to coordinated DDoS attacks on communication networks, media outlets, banking systems and government institutions. While controversy over attribution continued, incident showed that cyber operations can have a significant impact on a highly digitalized society without use of any gunfire. (Ottis, 2008) Later cyber attacks proved development of sophistication of cyber warfare. In Georgia in 2008, cyber activities were incorporated into conflict alongside conventional military forces. In 2008, Russian-Georgia conflict was an example of integration of cyber capabilities into conflict. In 2010, Stuxnet malware was discovered that enabled cyber weapons to cause physical damage to industrial control systems linked to Iran's nuclear program. (Lindsay, 2013). Over past decade, there has been an exponential rise in state and state-sponsored cyber operations. Strategic importance of cyberspace has been confirmed by recent events such as SolarWinds supply-chain attack, ransomware attack on critical infrastructure, cyber interference in electoral processes and large-scale cyber operations in context of Russia–Ukraine conflict. As these occasions demonstrate, cyber warfare is not a one-off event anymore but a key component of geopolitical competition.

2.2. Defining Cyber Warfare:

There is no clear-cut definition of cyber warfare, although it is becoming increasingly significant. However, there are various interpretations of it depending on strategic, legal and operational considerations of different states, international organizations and scholars. In a broad sense, cyber warfare is the application of cyber means by a state or a state-sponsored entity to gain strategic advantage by offensive operations against another state's information systems, networks or critical infrastructure. These can be designed to affect function of government, the military, manipulate information, or affect economic stability. Cyber operations are defined as “actions using cyber capabilities to achieve objectives in or through cyberspace” in Tallinn Manual 2.0 on International Law Applicable to Cyber Operations. (Schmitt M. N., 2017) Cyber activities, if done as part of interstate hostilities or with effects similar to traditional military operations, are part of cyber warfare, although not all instances of cyber operation are warfare. (Schmitt, 2017) The cyber warfare is very different from conventional cybercrime. Typically, a cybercriminal will seek to achieve a financial objective, one of three types: money through a fraud scheme, theft of an identity or ransom. Cyber espionage is mainly about intelligence gathering but not necessarily physical or economic damage. Cyber warfare, on the other hand, is more strategic, political or military in nature, and is often carried out by the state or state-sponsored.

2.3. Characteristics of Cyber Warfare:

The nature of cyber warfare is unique in several respects in comparison with conventional warfare. An important aspect of cyber warfare is that it is hard to trace attackers. Attackers use proxy servers, botnets, encrypted communications and compromised third party systems regularly to hide their identities. False-flag operations are made to appear as though they are by another actor to deceive investigators. The anonymity poses difficulties for international law to identify origin of crime and to enable victim state to gauge its response. Attribution is an additional difficulty and an added danger of misjudgement and unintended escalation between states. Offensive cyber operations require relatively small financial investments, in comparison to conventional military capabilities. A clever programmer and advanced malware can have strategic impact, which, in turn, could take a good amount of military effort. Cyberattacks on financial institutions, transportation systems, electrical grids or communication networks could inflict massive economic damage without political price tag that accompanies traditional military response. Cyber operations happen on an incredible pace and across borders. Malicious software can reach multiple jurisdictions at once, and spread around the world in minutes. Cyber operations differ from traditional warfare in that they are not limited by geography. States can operate against far-flung opponents without boots on ground and without physical borders being crossed. In traditional deterrence, it has been assumed that an attacker can be identified and that a credible threat of retaliation can be made. In a world of cyber warfare, however, the opposite is true; since attribution of attacks is often ambiguous, this undermines logic of deterrence. Further, cyber capabilities are frequently classified and hard for states to effectively demonstrate their offensive capabilities. Contemporary societies have digital infrastructure, which is connected, civilian and military. Military operations often rely on electrical grids, satellite communications, transportation, financial institutions, healthcare facilities and telecommunications networks, which provide critical civilian services. As a result, cyber activities targeting military targets could have unintended civilian impacts, thus creating legal and humanitarian issues.

2.4. Cyber Warfare, Cyber Operations and Information Warfare:

These terms are often interchangeable, but are different facets of digital conflict. Cyber operations refer to any activity that occurs via cyberspace including espionage, surveillance, gathering of cyber-related intelligence, sabotage, and defense measures related to cyber. A vast majority of cyber operations are not of the armed conflict kind. Cyber warfare is cyber operations conducted in context of interstate conflict or military campaigns carried out with the aim of inflicting strategic effects similar to those of conventional warfare. Information warfare is more than just cyber warfare and involves propaganda, psychological operations, disinformation campaigns, opinion manipulation and manipulation through digital platforms. Information warfare has shown itself to be an effective way to affect political stability without

destroying physical infrastructure in recent elections in several democratic countries. Cyber warfare and information warfare are both a product of multi-faceted nature of today's conflict.

2.5. Cyber Warfare as a Fifth Domain of Warfare:

Throughout most of modern history, military engagements have taken place in four historical spheres of land, sea, air and most recently outer space. Cyberspace is now a domain that is commonly recognized as being fifth operational domain. Current major military powers, such as US, China, Russia, UK, France and India as well as NATO member countries have dedicated cyber commands whose primary mandate is to conduct offensive and defensive cyber operations. These institutions incorporate cyber capabilities into a holistic military planning and national defense. The definition of cyberspace as an operational domain is emblematic of a number of realities in an increasingly militarily command and control dependent world. Precision-guided weapons rely upon satellite communications and digital infrastructure. The collection of intelligence is becoming more cyber enabled. The critical infrastructure has become an attractive target when facing between states conflict. Cyber operations are oftentimes used in conjunction with, or in advance of, conventional military operations. The Cyber dimension in military doctrine reflects the importance of Cyberspace in current international relations.

2.6. Strategic Importance of Cyber Warfare in International Relations:

Cyber warfare has become an instrument of state power alongside diplomacy, economic sanctions, intelligence operations and conventional military force. It provides states with flexible options for coercion below threshold of declared war. Several factors explain its growing strategic importance like first cyber capabilities enable states to project power without physical occupation or direct military confrontation. This is particularly attractive in an era where major powers seek to avoid escalation into large-scale conventional wars. Second, cyber operations offer plausible deniability. States can employ intelligence agencies, private contractors or proxy hacker groups while avoiding explicit responsibility. Third cyber warfare has become central to strategic competition among major powers including US, China, Russia and other technologically advanced states. Competition increasingly extends beyond territorial disputes into technological dominance, digital infrastructure, artificial intelligence, semiconductor production and control of global communication networks. Fourth, cyber capabilities disproportionately empower middle powers and technologically advanced smaller states. Unlike conventional military power, cyber capabilities depend more heavily on human expertise than on large defense budgets, allowing smaller states to exert influence beyond their traditional military capacities. Finally, cyber warfare directly affects international economic stability. Global financial markets, multi-national corporations, energy systems, supply chains and digital commerce depend upon secure cyber infrastructure. Disruptions in cyberspace therefore possess immediate international economic consequences.

3. Theoretical Framework: Understanding Cyber Warfare through International Relations Theories

Cyber warfare is a key and emerging aspect of today's international politics that threatens to upend assumptions about power, sovereignty, conflict and security. In virtual domain, cyber conflicts are played out in a space without borders and between actors other than soldiers, including actors from non-state groups, multinational corporations as well as individuals and states, who have capacity to affect international stability. Hence, there does not exist any single theoretical approach that explains complexity of cyber warfare. In contrast, broader understanding of the strategic behavior of states in cyberspace can be obtained through an interdisciplinary approach, based on the main theories of International Relations (IR).

3.1. Realism and Cyber Warfare:

One of the most important theories in IR for the study of interstate competition is realism. Realism is based on works of Thucydides, Niccolò Machiavelli, Thomas Hobbes, Hans Morgenthau, later Kenneth Waltz and John Mearsheimer and considers international system as anarchic: there is no central authority to enforce international law or to ensure state security. In those circumstances, states will seek to survive by gaining as much power as possible and defend national interest. The realist view of cyberspace today is that it is yet another theatre for strategic competition between states. (Morgenthau, 1948) States have historically fought for territorial control, military dominance and economic power; it is now for technical leadership, cyber-skill and digital intelligence. Offensive cyber operations are considered tools of national power that can provide political end, at lower cost of conventional military operations. The biggest powers such as US, China, Russia and some regional powers have added cyber activities to their national security policies. Offensive cyber capabilities offer a major strategic edge, allowing states to gain intelligence on their competitors, interfere with military command and control, impact political decision making, attack critical infrastructure, affect international power dynamics and compromise economic competitiveness. A group of realists believe that cyber warfare is a continuation of the security dilemma. One state advances its cyber defense and/or gains offensive capabilities, and other states see this as a threat and respond with increased cyber capabilities. This rivalry fuels an international cyber arms race with ongoing advancements in technology and strategic distrust. Cyber operations have supported traditional military operations by disrupting government communication, energy infrastructure, satellite systems and information networks. Likewise, US-China rivalry has now seeped into cyberspace via accusations of cyber espionage, stealing technology advances and intellectual property including artificial intelligence, semiconductors and quantum computing. The explanation for why

international norms from which legal framework of cyberspace is derived are generally secondary to national security concerns is thus given in terms of realism. States are typically not keen on having laws that restrict their strategic maneuverability in cyberspace. Realism is one of the most significant theories in the field of cyber warfare. Classical Realism posits the international system as an anarchical one, forcing states to focus on self-preservation, gain as much power as possible, and protect their nations' security. Cyber is thus regarded as strategic tools that can augment national power and mitigate military vulnerabilities. (Morgenthau, 1948) The common traits of contemporary cyber operations by great powers—such as United States, China, Russia, Iran, and North Korea—correspond to realist understandings of strategic competition. Offensive cyber capabilities are now becoming more common among states, as the cyber domain allows states to collect intelligence, conduct espionage, engage in coercion, sabotage, and strategic signalling at a relatively low cost. (Libicki, 2009) In a realist view, cyber warfare is another sphere in which states struggle for relative gains. Offensive cyber capabilities allow governments to attack military command systems, critical infrastructure, financial institutions, and communication networks without necessarily entering into conventional armed conflict. (Valeriano, 2015) Examples of the cyber aspect of geopolitical competition include the cybercriminal arms race between the United States and China, Russian attempts to influence Western elections, and North Korea's cyber-financial activities. (Healey, 2013)

3.2. Liberal Institutionalism and International Cyber Governance:

While realism focuses on conflict, liberal Institutionalism sees a role for cooperation, international institutions and common interests in easing conflict. Robert Keohane and Joseph Nye among others contend that rising interdependence and cooperation among states will lead to peaceful solutions to conflicts and to creation of international norms of behavior. (Keohane, 2012) The most obvious example of complex interdependence is with cyberspace. Modern economies rely on global communication, financial and technological infrastructure, as well as digital supply chains. One major cyber-attack on a financial or communication system in one country could have far-reaching impacts in other countries. As a liberal, such interconnectedness offers opportunities for cooperation among states to establish international cyber norms and law. In recent years, international organizations such as United Nations, NATO, European Union, INTERPOL and regional organizations have made a concerted effort to develop guidelines for responsible state conduct in cyberspace. Significant institutional progress has been made such as United Nations Group of Governmental Experts (UN GGE), United Nations Open-Ended Working Group (OEWG), Budapest Convention on Cybercrime and Regional confidence-building measures by Organization for Security and Co-operation in Europe (OSCE) and by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). Liberal institutionalists argue that while cyberspace is competitive, international institutions help to minimize uncertainty by providing opportunities to talk, be transparent, share information and promote trust-building between states. But there are many hurdles in way of institutional cooperation. Development of universally binding cyber treaties remains hampered by divergent national interests, varying views on internet governance and geopolitical competition. Liberal institutionalism, on the other hand, posits that international cooperation is still possible under the conditions of anarchy–it does so with the help of institutions, legal norms and repeated interactions. (Nye, 2011) In context of cyberspace, Liberal Institutionalism highlights the need for the creation of international law principles and institutions of responsible state action. Confidence building, norm setting and dispute resolution can be achieved through the activities of various institutions, including the United Nations Group of Governmental Experts (UN GGE), the Open-Ended Working Group (OEWG), the International Telecommunication Union (ITU) and regional institutions. (Schmitt M. N., 2017)

3.3. Constructivism and Social Construction of Cyber Norms:

Constructivism is a paradigm that provides a very different approach to understanding international politics that focuses on the role of ideas, identities, norms and social interactions in influencing state behaviour. Alexander Wendt, Martha Finnemore, Peter Katzenstein and other scholars believe that international politics is not just a product of material forces. Constructivists see cyberspace as more than an environment of technology, however, as one in which rules and meaning develop as a result of interaction with other countries. There are no absolute categories of responsible state behavior, digital sovereignty, cyber aggression or acceptable cyber conduct, but rather they are continually negotiated via diplomatic practice, through international organizations, expert communities, and state interactions. This is normative process as illustrated in development of Tallinn Manual 2.0. Manual is not of binding legal force, but it is an important contribution by international legal experts to explaining the application of existing international law to conduct of cyber operations. With time, these interpretations can affect customary international law by affecting expectations of states and legal practice. Constructivism can also yield an understanding of different visions of cyberspace that states promote. In general, liberal democracies promote an open, secure and interoperable Internet that is based on human rights and freedom of expression. However, a number of states call for greater government oversight of digital data, highlighting cyber sovereignty and political stability within the state. Consequently, international legal principles and provisions pertaining to cyberspace are not only being developed through treaties, but also through evolution of state practices, diplomatic negotiations, judicial interpretations and formation of an international consensus. In addition to material power, state action is also influenced by norms, identities, beliefs and shared understandings as said by constructivist scholars. (Wendt, 1999) International principles of responsible state conduct in cyberspace continue to be in the formative stages. The shift towards concepts like cyber sovereignty, responsible disclosure, protection of civilian infrastructure and restraint in peacetime has slowly come into diplomatic practice and multilateral negotiations. (Nye, 2011) The reasons for

the varying interpretations of cyber sovereignty can be better explained with the help of constructivism. While China and Russia tend to promote greater state regulation of cyberspace, many Western democracies promote an open, interoperable and globally connected internet. (Segal, 2016) International organisations, technology firms, academic institutions and civil society are other types of norm entrepreneurs who shape cyber governance in this world through advocacy, technical standards and legal interpretation. (Finnemore, 1998)

3.4. Deterrence Theory in Cyberspace:

The principles of Deterrence Theory have always been important in military planning, especially in the nuclear era. The basic idea is simple: the best way to avoid aggression is to make it clear to potential aggressors that the benefits of attacking will be outweighed by the costs. The cyber challenge to deterrence is unique. Traditional deterrence relies on three factors: clear attribution of attacks, adversaries' rational decision-making and retaliatory capabilities. All these assumptions are undermined by cyber warfare. Firstly, attribution is technically and politically challenging. Often attackers are using proxy servers, compromised infrastructure, botnets and false flag methods. Second, cyber retaliation can have second effects as digital networks are interlinked around world. If a cyber attack occurs and it impacts another nation or civilian infrastructure, it can have unintended consequences. Third cyber threats originate from diverse actors, including intelligence agencies, criminal organizations, terrorist groups, patriotic hackers and private contractors. While problems of attribution, anonymity and proportionality differ greatly from the real world, deterrence theory has become more relevant than ever in the digital realm. (Schelling, 1966) The elements of cyber deterrence can include deterrence by denial, deterrence by punishment, resilience, attribution capabilities, and offensive retaliation. Many of these actors may not be deterred through conventional military retaliation. Modern cyber strategies increasingly rely upon these integrated approaches rather than traditional deterrence alone. Cyber operations, however, are often not of the armed attack level and deterrence is sometimes ineffective using traditional means. (Lindsay, 2013)

3.5. Cyber Sovereignty:

“Since the end of tCold War, international law has been more and more subject to challenges from states and other actors in an increasing sense and specific norms have been challenged, in application, by new realities and obstacles. (Delerue, October 2019) Cyber sovereignty has become one of the most contested concepts in contemporary international law and global governance. Traditional sovereignty refers to the exclusive authority of states over their territory and domestic affairs. In cyberspace, however, territorial boundaries become significantly less meaningful because digital communications routinely cross national jurisdictions. Different states interpret cyber sovereignty differently. One perspective argues that states possess sovereign rights over digital infrastructure, data, and cyber activities occurring within their territory. This interpretation emphasizes governmental authority to regulate internet content, digital platforms, cybersecurity and information flows. An alternative perspective emphasizes global nature of cyberspace, arguing that excessive governmental control threatens open and interconnected architecture of the Internet. Proponents advocate multi-stakeholder governance involving governments, private technology companies, civil society organizations and technical communities. The disagreement over cyber sovereignty has significant implications for international law.

3.6. Integrating International Relations Theory with State Responsibility:

Each theoretical perspective contributes unique insights into evolving doctrine of state responsibility. Realism explains why states continue developing offensive cyber capabilities despite legal uncertainty. Liberal Institutionalism highlights necessity of international cooperation and institutional governance to reduce instability in cyberspace. Constructivism demonstrates how legal norms governing cyber behavior gradually emerge through international practice and diplomatic interaction. Deterrence Theory illustrates why attribution and credible response mechanisms remain essential for maintaining international stability. Cyber Sovereignty emphasizes the continuing relevance of state authority while recognizing that digital technologies challenge traditional territorial conceptions of sovereignty. Collectively, these theories suggest that state responsibility in cyberspace cannot be understood solely through traditional legal doctrine. Rather, it reflects interaction of strategic competition, institutional development, evolving international norms, technological innovation and competing conceptions of sovereignty.

4. International Legal Framework Governing Cyber Warfare:

The swift development of cyber warfare has thrown new challenges for necessity of international law to regulate state activity in cyberspace. The dynamism of cyber warfare has posed fundamental questions about sufficiency of international law to address state activity in cyberspace. Cyber operations rarely can be described as armed attacks and they often are carried out by individuals or groups that act on behalf of other people or entities with effects that can range from data breaches to service disruptions and destruction of infrastructure. These features raise questions about sovereignty, jurisdiction, prohibition on use of force, self-defence and state responsibility.There is no complete and universally accepted international law dedicated to cyber warfare but most states and legal experts believe that existing international law applies in cyberspace. This has also been reiterated in successive reports of United Nations Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG), which confirm that principles and purposes of United Nations Charter continue to apply to cyber activities. These principles are still subject to much debate, however, about interpretation and application.

4.1. United Nations Charter and Cyber Warfare:

“One should not endanger the values that underlie societies based on the rule of law in the name of protecting the world and countries from rogue states, terrorists and cybercriminals.” The cornerstone of modern system of international law is United Nations Charter (1945). Originally drafted as long ago as before advent of cyberspace, original principles govern interstate relations whether exercised by real or virtual means of a state. Sovereign equality of all states is laid out in Article 2(1) of UN Charter (Douwe Korff, January 2019). In terms of cyber domain, sovereignty means that all states have sovereignty over networks, resources and cyber infrastructure within their territory. Cyber operations that occur in unauthorized ways and impact governmental institutions, critical infrastructure or national communication systems could accordingly be considered as violations of sovereignty. There is, however, a split in international law over whether all unauthorized cyber intrusions are an expression of sovereignty or only those that result in "substantial" adverse effects. In some countries like France and Netherlands, cyber intrusion is deemed as an attack on sovereignty if it is not destructive. Other countries have taken a more reserved stance, such as United Kingdom, which says all the time that it is not case that cyber intrusion is equivalent to violation of international law. This disagreement is a reflection of one of key legal issues facing cyber governance. The principle of non-intervention is the principle of customary international law that states may not use force to interfere in matters that are solely within another state's domestic jurisdiction.Non-intervention is the principle of customary international law that states may not forcefully intervene in matters which are solely within another state's domestic jurisdiction. Cyber operations that seek to alter an election process, to disrupt government decision-making or to attack public institutions can infringe on this principle. This can involve interference in elections by means of cyber-based disinformation campaigns, hacking governmental communication systems, manipulation of voter data, cyber operations against judicial systems and interference with national financial systems. Cyber interference can take place covertly as opposed to traditional military intervention and legal assessment can be very difficult.

The legal issue that has been discussed is the determination of whether cyber operations are a use of force under Article 2(4) of UN Charter. According to Article 2(4), territorial integrity and political independence of a state can not be interfered with by using force. The traditional definition of force was primarily military violence (destruction or armed attack). With use of cyber operations, similar strategic outcomes can be achieved without use of traditional weapons. There are three types of cyber operation: Website defacement, Distributed Denial-of-Service (DDoS) attacks, Data theft, Cyber espionage and temporary disruption of online services. The majority of legal experts maintain that these actions are not a ‘prohibited use of force'. They include disruption of banking systems, large-scale economic losses, long-term interruption of public services and significant interference with governmental functions; a prohibited use of force is a subject of intense debate. Nowadays, cyberattacks with physical impact like explosions, destruction of power plants, transportation failures or damage to military installations are perceived as being equal to conventional military attacks. Stuxnet is one of most obvious examples of a cyber operation causing physical damage against Iranian nuclear enrichment facilities. Therefore, several scholars believe that technology used is of secondary consideration and that evaluating cyber operations should be based on their impacts.

Article 51 of UN Charter provides that existence of right of individual and collective self-defence in event of armed attack. This is controversial as far as cyberspace is concerned. Among pertinent legal issues raised are those of whether a cyberattack could amount to an armed attack? What amount of harm must occur in order for armed attack requirement to be met? Is economic disruption a good enough reason for self-defense? Is cyber-attack that has been ongoing for a long time counted as an armed attack? The majority of modern legal writings point to idea that cyber operations that kill, cause physical damage or effects similar to traditional military operations might result in Article 51 being triggered. Some examples are cyber attacks that could cause a national electricity grid to malfunction, disrupt hospital system leading to deaths, or destroy nuclear facilities and disrupt military defense during an armed conflict. But operations that involve espionage, data theft or temporary services disruption are typically not considered to be armed attacks. In cases of self defence, international law stipulates that all three principles of necessity, proportionality and immediacy must be observed. The same principles of “preparedness” apply to cyber responses.

International Humanitarian Law regulates behaviour of belligerent parties, irrespective of what kind of weaponry is used in an armed conflict. The International Committee of Red Cross (ICRC) has always held that IHL applies completely to cyber operations during armed conflict. There are four key principles that are relevant in particular. Parties shall differentiate between Military Objectives, Civilian Persons and Civilian Objects. A cyber-attack on civilian hospitals, schools, banking systems, or even a water treatment plant are an example of an attack that would be an unethical violation of this principle, unless such an object became lawful military targets. It is very hard to keep civilian and military networks separate, since they are often linked together. States have an obligation to minimize incidental civilian harm even in event of an attack on legitimate military targets. Military communication systems can be attacked using cyber means and lead to unintended disruption of services of Emergency medical health systems, Air traffic control, banking networks, water supply systems and electricity grids. Proportionality is therefore a significant challenge for commanders in assessment of cyber operations. Only cyber operations necessary to legitimate military goals are allowed under military necessity. Unauthorized cyber attacks that are only meant to inflict large-scale civilian destruction are still illegal. States engaging in cyber operations have responsibility to take practicable measures to limit civilian damage. Such precautions can involve careful design of malware, verification of target, restricting propagation of malware and monitoring cyber effects ongoing. The unintended dissemination of malicious software to unauthorized recipients is an important issue under IHL.

4.2. International Human Rights Law (IHRL):

While IHL is mainly in effect in context of armed conflict, International Human Rights Law can be in force also in context of peace. The impact of cyber operations on a multitude of internationally protected rights such as Right to Privacy, Freedom of Expression, Right to Health and Right to Life is growing. Under Right to Privacy, mass cyber surveillance, unlicensed data collection and government hacking could encroach upon right to privacy as guaranteed by international human rights documents. State Internet shutdowns, Internet censorship and cyber restrictions in Freedom of Expression can affect freedom of expression and access to information. In context of Right to Health, a cyber-attack on healthcare network can disrupt critical healthcare delivery services and compromise public health. Where cyber operations cause a failure of emergency services, hospitals or essential infrastructure causing death, states could have human rights obligations, according to Right to Life. Therefore, cybersecurity policies should strike a balance between legitimate national security goals and respect for internationally accepted human rights. We should "attempt to define a middle ground between cybersecurity and human rights. Importantly, we think it is necessary to take a stance against the common conception that national security and human rights as they relate to cyberspace are always incompatible. Through rights-respecting design of cybersecurity law and policy and, very importantly, technology that is security- and rights-respecting by design, both 'camps' can be reconciled, with benefits for all." (Kavanagh, 2019)

4.3. Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA):

The main legal principles governing state responsibility are contained in Articles on Responsibility of States for Internationally Wrongful Acts adopted by International Law Commission in 2001. (Commission, 2001) While ARSIWA predates advent of cyber warfare, its tenets are still relevant. There are two key elements to define state responsibility. The cyber conduct should be legally linked to a state. Attribution can be an issue, when cyber operations are carried out by a government agency, military cyber command, an intelligence service or a state-controlled organisation or non-state actor working under direction or effective control of state. One of most difficult legal battles in cyberspace is establishing attribution, as attackers often try to hide their tracks. Responsibility is not always held even if cyber-attribution is confirmed, only when cyber conduct infringes upon an international legal obligation. These include breaches of principles of Sovereignty, non-intervention, use of force, humanitarian law and Human rights law and Treaty obligations. If responsibility is found, responsible state could be bound to make obligations such as Cessation of wrongful conduct, Guarantees of non-repetition, Reparation, Compensation, Restitution and Satisfaction.

4.4. The Tallinn Manual 2.0:

The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations is one of the more important scholarly works to have influenced cyber law and was prepared by a group of international experts under auspices of NATO's Cooperative Cyber Defence Centre of Excellence. (Schmitt M. N., 2017) Manual does not constitute legal binding documents, but it is the most extensive study of current international law on cyber operations. Manual is unanimous in that law of land is to be applied completely in cyberspace. Sovereignty remains applicable. No use of force includes cyber operations. Self-defense is possible after successful hacking of cyber weapons. In an armed conflict, IHL applies to cyber operations. States are responsible for any internationally wrongful cyber activity they are responsible for. Although Manual has had a significant impact, it has also been criticized due to some interpretations of Manual that are not in line with opinion of states on sovereignty, DoD and attribution. Although doctrinal change has occurred, there is still a lot of legal uncertainty. These include absence of widely accepted rules of attribution, unclear division between cyber espionage and the unauthorized use of force, disagreement on definition of when a cyber operation is considered a use of force, the increasing use of proxy actors and private cyber firms, use of artificial intelligence for autonomous cyber operations, rise of quantum computing and future questions regarding security of encryption, and lack of binding cyber treaties. International dialogue and law development is needed to address these issues.

5. Attribution and State Responsibility in Cyberspace: Legal Standards, Evidentiary Challenges, Proxy Actors and Emerging Approaches to Accountability

A very difficult legal question in cyber warfare is who is legally responsible for a cyber operation. When state is attacked in "conventional warfare" it can normally be easily determined since military units fight under a known command and under banner of a known state. However, in cyberspace, attackers can use a variety of tactics, including encryption, proxy servers, botnets, compromised third-party infrastructure and false-flag operations, to mask their identity. This makes it difficult to tell difference between criminal hackers, state sponsored, patriotic hackers, and official military cyber units, and/or any of them. "In an age of cyber insecurity, anxieties about the silence of States concerning the applicability of international law to peacetime cyber operations have been growing. Concerns have focused on the reluctance of States to agree cyber-specific multilateral treaties and to publicly clarify the customary international rules applicable to hostile cyber operations." (Sander, May 2019) State responsibility is a major issue in debates over this attribution problem. That an internationally wrongful act must be imputable to a state is a requirement of international law. However, traditional attribution rules are tricky in cyberspace because of its decentralized and transnational character. States are increasingly using proxy actors, private contractors, cyber militias and intelligence agencies to seek strategic goals while keeping their hands clean. As a result, current rules of war must be changed.

5.1. The Legal Concept of Attribution:

"States are rapidly approaching an international law crossroads in cyberspace. While many States, led by the United States, take the view that existing international law, including the law of armed conflict, is sufficient to cover cyberspace ("law of the horse"), such a view is being overtaken by reality." (Walker, 2015)

According to international law, attribution" is ability to determine whether or not the action of an individual or entity can legally be attributed to a state. Attribution is different to technical identification. Attribution, legal process of determining who is responsible for malicious code or who is responsible for an attack, is a process that cybersecurity experts might be able to carry out and prove a strong linkage between perpetrators and state. The responsibility of state is imposed on state only if two conditions are met: conduct must be attributable to the state under international law. The behaviour is a violation of international legal obligation. This distinction is relevant especially in cyberspace as technical evidence is insufficient to prove legal responsibility in most instances. For instance, malware coming from servers from other countries does not necessarily mean that government of that country was behind or authorized the malware. Cyber attacks often take advantage of infrastructure in other jurisdictions to hide their tracks and make it a challenge to attribute them, especially politically. "An independent international mechanism could lend credibility to attribution in the cyber realm, thereby limiting the ability of responsible States to deny involvement and facilitating collective attribution and response. Like the OPCW Technical Secretariat, such a mechanism could prove useful for State and non-State actors in certain situations.86 To be sure, such a mechanism should complement, not replace, existing attribution mechanisms and practices. Optimally, it should find ways to harness the evidence gathering and analytical wherewithal of State agencies, and the technical expertise resident in the public and private cyber security sectors." (Schmitt (. S.)

5.2. Attribution under Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA):

Articles on Responsibility of States for Internationally Wrongful Acts (2001) of International Law Commission offer main legal basis for establishing attribution. (Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, 2001) According to Article 4, conduct of any state organ is attributed to state regardless of whether organ carries out a legislative, executive, judicial, military or intelligence function. Military cyber commands, national intelligence agencies, government cybersecurity agencies and other official state institutions whose actions are carried out in their official capacity are considered to be acting on state's behalf in their cyber operations. For instance, if national cyber command attacks another nation's military infrastructure under government's consent, then operation is an act of state under international law. Article 5 further extends attribution to bodies which are not formally constituted state organs but nevertheless have powers to exercise governmental functions. These can include state owned cyber security agencies, government-contracted cyber defence organisations and Public corporations carrying out national cyber security functions. In particular, Article 8 is applicable to cyber warfare. It states that actions of non-state actors may be considered to be attributable to a state if they are performed in accordance with the instructions, direction or effective control of state. This can be key factor as many cyber operations include patriotic hacker groups, private cyber-security contractor groups, criminal groups, proxy militias and volunteer cyber units. The difficulty is in figuring out how much control is needed in order to make attribution. In Nicaragua case (1986), International Court of Justice (ICJ) used effective control standard, which required a finding of state direction and control of specific operation in question. The overarching control test as it came to be called was subsequently suggested by International Criminal Tribunal for former Yugoslavia (ICTY) in its Tadić case (1999). Though powerful, the ICJ has remained favourites of the more demanding effective control test. These standards are very controversial when applied to cyber operations, due to the lack of direct evidence of governmental instructions.

5.3. Technical Attribution versus Legal Attribution:

One of hallmarks of cyber warfare is separation of technical attribution from legal attribution. Technical attribution attempts to determine IP address, malware signatures, command and control servers, digital infrastructure, programming techniques, linguistic patterns and operational behaviour. Forensic analysis is often used by cyber security companies and intelligence agencies to pinpoint suspects. But attackers are using VPNs, Proxy servers, Compromised third-country infrastructure, Anonymous cryptocurrencies, False digital identities and Artificial intelligence assisted obfuscation are becoming more and more common. These techniques substantially diminish reliability of technical attribution. Technical evidence is not the only evidence needed for legal attributability. States are required to prove that identified actors acted on behalf of a state, there was enough control over its operation or operation was officially authorised by state. Public accusations therefore are frequently based upon a mix of technical intelligence, human intelligence, signals intelligence, diplomatic assessments and classified information. This more comprehensive manner of evidence demonstrates the complexity of legal responsibilities of the State in cyberspace. "Fact-finding provides a basis for legal and political claims. Thus, fact-finding mechanisms are especially useful in fields where legal compliance is chronically deficient, such as human rights law, where there is a special need to further legitimize norm-implementation efforts and increase deterrence, or where unique technical challenges present themselves, as in the case of unconventional weapons. Indeed, the use of the OPCW's technical facilities in connection with the Salisbury incident illustrates the benefits of fact-finding in cases requiring complex scientific analysis, as well as the growing interest of States in internationalizing attribution

processes." (Schmitt (. S.)

5.4. Evidentiary Challenges in Cyber Warfare:

Cyber operations are digital, which presents a number of obvious challenges for evidence. Cyber criminals are able to hide behind advanced technology that makes it difficult for even the most powerful intelligence agencies to identify perpetrators. A false-flag cyber operation is a malicious attack that mimics the code, language, and/or techniques of another state in order to deceive investigators. This deception makes politics more difficult and makes it harder to hold them accountable in court. Cyber operations routinely go through many jurisdictions leading to the target. The attack can include Servers in one country, Malware created in another, Financial support provided from a third and Operators in another country. This multi-national setup makes it difficult in regards to criminal investigations and interstate cooperation. A significant number of attributions are based on classified intelligence, which governments are not willing to release publicly. Accordingly, claims by victim states to attribute cyber operations to foreign governments are often met with skepticism, because it is likely that they do not disclose the identifying details of their intelligence sources when making such allegations. Today, cyber warfare is increasingly carried out by proxy actors and not official military actors. They comprise Private cybersecurity contractors, Volunteer cyber militias, nationalist hacker collectives, organised criminal groups, State-sponsored ransomware organisations and Intelligence-linked technology companies. Proxy actors bring a number of strategic benefits such as plausible deniability, lower political costs, reduced risk of military escalation, Operational flexibility and Access to specialized expertise. Their use, however, makes international legal accountability much more difficult. In same way, ongoing discussions about relationship between governments and advanced cyber organizations have been sparked by several major cyber espionage campaigns by groups like APT28 (also known as Fancy Bear), APT29 (aka Cozy Bear), APT10 and Lazarus Group.

5.5. Due Diligence Obligations:

Due diligence obligations are now increasingly recognised under international law beyond direct attribution. The principle imposes on states the obligation to take reasonable steps to ensure that their territory is not used for internationally wrongful cyber activities which affect other states. The expression "due diligence" does not mean "absolute prevention". Instead, states should: Investigate malicious cyber activities; Co-operate with international investigations; Take reasonable steps to prevent continuance of cyber operations; Strengthen domestic cybersecurity institutions and Enforce criminal laws relevant to cyber operations. Due diligence is a somewhat ambiguous concept in law, but has been increasingly acknowledged in Tallinn Manual, UN reports and practice of states. If it is determined that victim states are targets of the attack, they may take lawful measures in compliance with international law. These include diplomatic measures (formal protest), diplomatic negotiations, expulsion of diplomats and Public attribution. economic Measures include targeted sanctions, financial restrictions, export controls and Technology restrictions. Legal Measures, criminal indictments, asset seizures and International arbitration (where applicable) should be taken in this subject. For purposes of cyber counter-measures under international law, states are allowed to take reasonable countermeasures, provided they are proportionate in order to ensure compliance by responsible state. Any such measures should comply with principles of necessity, proportionality, where possible Reversibility and Respect for humanitarian obligations. Furthermore, states may exercise their inherent right of self-defense under Article 51 of UN Charter in cases of cyber operations which rise to the level of an armed attack. States and international organizations have offered several proposals to reform existing legal mechanisms and overcome their limitations. They include following such as developing international attribution mechanisms under UN auspices, enhancing intelligence sharing amongst trusted partners, establishing common evidentiary standards for cyber investigations, Promoting greater transparency about state cyber doctrines, expanding confidence building measures, negotiating a multilateral cyber convention clarifying state obligations, strengthening public-private partnerships between governments, technology companies and Encouraging capacity-building in developing states to improve cyber-resilience. All these efforts aim to mitigate uncertainty and to strengthen accountability in cyberspace.

5. Major Cyber Warfare Case Studies:Lessons for International Law & State Responsibility:

Major cyber incidents over last 20 years should be used to better understand the legal and strategic consequences of cyber warfare. The incidents highlight transformation of cyber operations from hacking to becoming instruments of statecraft that can impact military operations, affect critical infrastructure, influence domestic political processes and influence international legal discourse. The two cases have significant issues of attribution, sovereignty, prohibition on use of force, due diligence, proportionality and state responsibility. Together, they show that, although current international law concepts are still applicable, they are complex to apply in cyber-space. It discusses six key cyber incidents that include Estonia cyberattacks (2007), Russia–Georgia conflict (2008), Stuxnet (2010), SolarWinds (2020), Colonial Pipeline ransomware attack (2021).

5.2 The Estonia Cyberattacks (2007):

These attacks on Estonia in April and May 2007 have been considered the first large-scale cyber campaign against a modern state. Shortly after removal of Soviet-era Bronze Soldier from centre of Tallinn, Estonia saw an unprecedented series of Distributed Denial-of-Service (DDoS) attacks on government ministries, parliament, political parties, banks,

media and tele-communications networks. Estonia was one of most digitally connected societies in world, and consequently used electronic governance and online financial services extensively. The simultaneous assaults created chaos in public administration, online banking, emergency communications and news services for several weeks. While there was no physical destruction, attacks resulted in substantial economic losses and loss of confidence in key national institutions.

From a legal point of view, Estonia incident raised a number of questions that never got answered; although attacks were strongly suspected as being made by a foreign government, it was hard to prove it legally. The disruption was not obviously covered by the definition of an "armed attack" in Article 51 of UN Charter. NATO saw cyberspace as a new security issue and found that collective military defense mechanisms were not activated. The most important results were creation of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in 2008. The experience also directly helped develop one of the most influential interpretations of international law that applies to cyber operations: Tallinn Manual. Estonia case proved that cyber operations can pose a threat to national security without using conventional military means and changed international views on cyberspace.

5.3. Russia–Georgia Conflict (2008):

For the first time in history, Russia-Georgia conflict was a clear example of cyber operations coming into play with traditional military conflict. In August 2008, just prior to Russian army's invasion of Georgian territory, Georgian Government faced coordinated cyberattacks on Government websites, banking institutions, media organizations, communication systems and public information portals. These cyber operations affected communication of governmental authority and Georgia's ability to communicate during active military hostilities with her domestic and foreign users. In contrast to Estonia, cyber incidents were not confined to conventional military operations but rather were intertwined with Georgian conflict, marking evolution of cyber capabilities as force multipliers in a conventional military campaign. Conflict posed important legal questions: Whether cyber operations in support of armed conflict are separate violations of international law; International Humanitarian Law (IHL), cyber operations and state responsibility when cyber operations are carried out by patriotic hackers or by unofficial proxy groups. While it was difficult to definitively say who had originated the attacks, many cybersecurity experts felt that they were orchestrated with Russian military in mind. Georgia case further highlighted importance of including cyber operations within frameworks of existing military doctrines and legal frameworks to analyze armed conflict.

5.4 Stuxnet and Iranian Nuclear Program (2010):

The release of Stuxnet malware in 2010 is a pivotal moment in history of cyber warfare. The Stuxnet attack was unlike other cyberattacks that have recently targeted government agencies, banks or services: It is a program that specifically aimed to destroy uranium enrichment plant at Natanz in Iran, using industrial control systems made by Siemens. The malwares interfered with the centrifuges' operations and also fed false information into system, leading to the destruction of hundreds of centrifuges without any military action. United States and Israel have not officially taken responsibility for operation, but a lot of investigative reporting and scholarly research has pointed to a US-Israeli intelligence operation. Stuxnet had a number of implications for international legal debates. To begin with, it was a proof that Cyber Weapons can inflict physical destruction similar to a military attack. Second, it questioned the traditional understanding on use of force under Article 2(4) of UN Charter. Third, it posed challenges to questions of 'legality of preventive cyber operations' and 'Sovereignty violations', 'Proportionality' and 'State responsibility for covert cyber campaigns'. Some scholars say that Stuxnet was the first cyber operation to demonstrate that it could meet the "threshold of an unlawful use of force" due to its impact on real world that was similar to kinetic military means. The incident also spurred a global growth in cyber weapons development, prompting many states to pursue development of offensive cyber capabilities.

5.5 The SolarWinds Supply Chain Compromise (2020):

Overall, the SolarWinds attack was one of the most advanced cyber espionage operations ever detected. The attack creators gained access to SolarWinds' software updates, which are provided to governments and private sector companies around the world and are utilized by many network management tools. Multiple US federal agencies, defense contractors, Technology companies, Critical infrastructure organizations and International institutions were targeted in the attacks, which involved attackers inserting malicious code into legitimate software updates to gain unauthorized access into these organizations. The operation went undetected for months until it was discovered in last few months of 2020. In contrast to Stuxnet, SolarWinds was mostly about espionage and not physical destruction. It has therefore been debated whether there is a violation of international law with the extensive cyber espionage. The laws governing espionage have been somewhat murky for years. The existence of practice is acknowledged by many States but it is not expressly forbidden or permitted in international law in general. The United States publicly blamed operation on Russian Foreign Intelligence Service (SVR) and took diplomatic, economic and criminal action. SolarWinds showed the fragility of the world's software supply chains and the rising need for cybersecurity in public-private collaborations.

5.6 Colonial Pipeline Ransomware Attack (2021):

The Colonial Pipeline ransomware attack highlighted the increasing overlap of cybercrime, national security and

international law. In May 2021, the ransomware gang DarkSide attacked Colonial Pipeline, which is one of the biggest fuel distribution networks in United States. Panic buying, fuel shortages, and economic disruption occurred in several states in US, as pipeline operations were temporarily halted. While the attackers' motives seemed to be mainly financial, incident highlighted potential for a criminal cyber operation to produce a similar impact to a national security crisis. The US government clarified that states are responsible for keeping their land from being exploited by cybercriminals against foreign critical infrastructure. This incident prompted a rehash of due diligence duties; International cooperation in combating ransomware; State responsibility for tolerating criminal cyber organisations on its territory. The Colonial Pipeline incident also helped spur international collaboration on transnational ransomware operations.

5.7. Comparative Analysis of Case Studies:

While the circumstances of each cyber incident were different, there are some similarities to be observed. The first is that attribution is always an issue. Where governments claim to recognize responsible states, legal evidence of existence of such responsibility may still be disputed. Second, cyber operations are becoming more and more part of an overall political or military strategy rather than a stand-alone operation. Third, critical civilian infrastructure, such as banking, healthcare, telecommunications, transportation and energy systems are main targets. Fourth, private sector actors have become essential in cyber defense and cyber attribution and thus pose a threat to traditional state-based definition of international security. Fifth, current international law offers general principles that can be used in cyber operations, but it does not contain specific provisions on many aspects of operations. Last, these case studies are a proof of fact that cyber warfare is no longer a kind of exceptional security phenomenon, but a permanent part of international relations. The following lessons are important to glean from these landmark incidents. International law applies to cyberspace but there is a need for more clarity in interpretation of concepts of sovereignty, use of force and due diligence. State responsibility will rely on credible attribution, which will depend on better global cooperation on digital forensics and intelligence sharing. There needs to be a more robust legal framework for the protection of critical infrastructure, especially in healthcare, energy, financial and communication sectors. Today technology companies are more likely to have capabilities that surpass those of many governments, so public-private partnerships are becoming a staple. There is a need for more effective conflict prevention, confidence building and cyber dispute resolution mechanisms in international institutions. Cyber warfare today has become a part of the larger geopolitical contest and the need for a comprehensive international regime now has become more pressing than ever.

6. Reforming International Law for Cyber Warfare: Toward a Comprehensive Framework for State Responsibility, Global Cyber Governance and International Cooperation:

The current structure of international law has proven to be inadequate in light of swift development of cyber warfare. The principles of United Nations Charter, International Humanitarian Law, International Human Rights Law and Articles on Responsibility of States for Internationally Wrongful Acts are still relevant to cyberspace, but were formulated in a time of mostly territorial and kinetic armed conflict. The anonymous, decentralized and transnational character of cyber operations has introduced uncertainties in law on attribution, states' sovereignty, force and due diligence and accountability. In the last ten years, many international processes have tried to explain how existing legal norms should be applied in cyberspace, such as United Nations Group of Governmental Experts (UN GGE), Open-Ended Working Group (OEWG), “Tallinn Manual 2.0” regional organisations and multi stakeholder forums. Nevertheless, significant conflicts remain between leading powers in cyber sphere on several issues such as state sovereignty, internet governance, offensive cyber operations, and the legal liability.

6.1.Need for Legal Reform:

The difference between cyber warfare and classical warfare are fundamental in several aspects. Cyber operations are often carried out at a level less than armed attack. Attribution is still unclear, and technically and legally difficult. Civilian/civilian and civil/military infrastructures are becoming more interdependent. Non-state actors are also involved in significant operations. The nature of cyber threat is constantly evolving with new technologies impacting it at all times. Offensive cyber capabilities are inexpensive, easy to obtain and commonplace. These attributes are sufficient to indicate that existing legal concepts do not need to be supplanted, but must be clarified. The goal should not be to abandon the principles, but to embrace them in cyberspace.

“The goal of creating an international attribution mechanism remains viable and that such an entity would prove valuable, albeit primarily in three contexts. First, an international attribution mechanism could prove useful for States with a limited independent capacity to effectively generate accountability. This includes States that, on the one hand, are sufficiently advanced technologically so as to render them highly vulnerable to hostile cyber operations, but, on the other hand, lack the technological capability to conduct their own forensic investigations98 and access to high-quality intelligence that can support attribution to a State actor. In this context, an international attribution mechanism could help level the playing field.” (Schmitt (. S.)

6.2. Clarifying the Principle of Sovereignty in Cyberspace:

A major debate is whether cyber operations that do not result in physical destruction, do still infringe upon state

sovereignty. Existing practice suggests that there is a range of interpretations. Unauthorized penetration of governmental systems, Manipulation of digital infrastructure, and Cyber interference with governmental functions are violations of sovereignty, according to some states. Other scholars argue that only cyber operations which have a significant physical and/or functional impact on adversary are considered to violate international law. There is a need for future legal advancement to set internationally recognized criteria as to when cyber activity constitutes as a violation of a State's sovereignty. Possible factors include scale of intrusion, duration, effects on governmental functions, Impact on critical infrastructure, degree of coercion and national security consequences. More clarity in the law would lessen uncertainty and would help standardize state practice.

6.3. Establishing Clear Attribution Standards:

Attribution is a key element of effective state responsibility. Attributions also differ widely by state, and are frequently based on classified intelligence that cannot be independently verified. The standards for attribution should be accepted internationally and should include technical Evidence and intelligence Evidence. Technical Evidence deals with digital forensic, analysis, malware identification, infrastructure tracing and behavioral signatures. Intelligence Evidence deals with human intelligence, signals intelligence, open-source intelligence and satellite intelligence as applicable. Independent evaluation should identify distinction between technical and legal attribution by analyzing state control, Government authorisation, effective control of proxy actors and Official responsibility. Legal certainty would be improved if there were internationally recognised evidentiary standards in place.

“An independent professional mechanism could offer verification of individual attribution claims, assuaging the concerns of States about the reliability of the attribution determinations upon which they are being asked to take action. Moreover, since cyber-related sanction regimes like the EU’s have implications under the domestic law of the member States, such as the freezing of assets and travel restrictions, domestic courts may examine the evidence underlying the sanction decision or seek credible assurance that the fact-finding process was independent, fair, and provided those involved an opportunity to contest the findings against them.103 An international attribution mechanism could, should it offer features along these lines, help satisfy this demand. (Schmitt (. S.)

“The configuration of the international attribution mechanism must be responsive to the goal of supporting States facing capacity issues, those interested in collective attribution, and cyber-related sanctions regimes. We believe additional research is called for in order to enumerate and ascertain specific “client” preferences and expectations.” (Schmitt M. N., 2017)

6.4. Reforming the Doctrine of State Responsibility:

While ARSIWA offers a flexible structure suitable for cyber operations, there are some issues that need further clarity. A clearer international law should be established or be amended to regulate activities of patriotic hacker groups, Private cybersecurity contractors, Volunteer cyber militias and State-sponsored ransomware groups.States should not be relieved of responsibility simply because cyber operations are carried out by intermediaries under control or direction of State. Future development of law should be to be more specific on scope of due diligence requirements that would require States to take steps to prevent malicious cyber activity emanating from within their jurisdiction, investigate serious cyber incidents, cooperate internationally and protect critical infrastructure and criminalize significant cyber offenses. Such commitments would enhance accountability and in accordance with national sovereignty.

6.5. Toward an International Cyber Convention:

The most important of reform proposals is to discuss a comprehensive international treaty on cyber warfare. A treaty could clarify definitions of relevant law, provide attribution mechanisms, define offensive cyber operations, secure critical civilian infrastructure, improve international cooperation, provide confidence-building measures and improve dispute resolution processes. But it is difficult to reach such an accord in politics because of divergent national interests. There are significant differences on Internet governance, cyber sovereignty, Human rights, Offensive cyber capabilities, state surveillance and Military transparency. It is challenging to reach consensus but is still possible in framework of framework agreements and sector specific treaties in legal field.

6.6. Strengthening the Role of United Nations:

United Nations is still the most legitimate international platform for creating cyber governance. There are a number of institutional changes that could be considered. There should be greater technical expertise for Open-Ended Working Group (OEWG), more involvement from developing countries, frequent review mechanisms, and more implementation monitoring for the OEWG. The Permanent Cyber Security Forum could be a permanent international body under aegis of United Nations to be responsible for Monitoring cyber threats, facilitating dialogue supporting capacity-building, Coordinating international responses and Promoting norm development. This type of institution would be in addition to, rather than a substitute for, other mechanisms.

6.7. Confidence-Building Measures:

Improvements in nuclear and conventional arms control have made good progress with confidence building measures

(CBMs). The same could be applied to improving cyber stability. They might involve Voluntary notification of major cyber incidents, Direct communication channels between national cyber authorities, Joint cybersecurity exercises, Information sharing concerning malware threats, Cooperative incident response mechanisms and Transparency concerning national cyber doctrines. Regional mechanisms such as OSCE, ASEAN Regional Forum, African Union and Organisation of American States (OAS) have valuable roles to play in implementation of measures. While traditional military security relies on expertise of private sector, cybersecurity relies heavily on it as well. Many of world's digital infrastructure is owned or operated by technology companies. Cooperation between different entities (governments, technology companies, internet service providers, cloud computing providers, academic institutions and civil society organizations) should, therefore, be institutionalized in future cyber governance. The areas of public-private cooperation include public-private information sharing on threats, joint incident response, vulnerability disclosure programs and building of cybersecurity capability and protection of critical infrastructure. The protection of essential civilian infrastructure should be a priority for future legal reforms. Protected sectors shall consist of hospitals, water systems, electricity grids, nuclear facilities, financial systems, telecommunications, Transportation networks and emergency response services. International law must take account of fact that cyberattacks on critical civilian infrastructure in times of peace and armed conflict can have humanitarian consequences similar to conventional military attacks. The strengthening of civilian resilience, coupled with an increased level of protection, would help reinforce IHL.

In context of fast-moving militarization of AI, meaningful human control, Algorithmic transparency (where possible), Verification procedures, Accountability standards, Ethical review mechanisms and International technical cooperation should all be elements of future international regulation. While the Recommendation on the Ethics of Artificial Intelligence (2021) from UNESCO is an important normative document, there will be a need for further legally binding documents at some point in future. Worldwide cybersecurity is extremely polarized. Technical expertise, Cybersecurity institutions, Digital forensic capabilities, Legal frameworks and Incident response capacity are not available in many developing countries. The International organizations should step up to provide more assistance via technical training, legal advices, transfer of technologies, cyber Security centres, Academic cooperation and Judicial capacity building. Since cyber space is inherently interconnected, strengthening of cyber security will be beneficial for international community. The ultimate aim is not just improved cybersecurity, but building a stable, predictable and rules-based digital international order. A set of such fundamental principles must underpin such an order including respect for sovereignty, peaceful settlement of disputes, Protection of human rights, Accountability for internationally wrongful cyber conduct, responsible state behavior, multilateral cooperation, transparency, civilian protection and Technological innovation consistent with international law. This task will need continued diplomatic activity between key powers driving cyber space, developing nations, international institutions, technology firms and civil society.

7. Conclusion:

The worldwide phenomenon of a digital transformation has turned cyberspace into a strategic domain that is alongside land, sea, air and outer space, profoundly redefining the nature of conflict, diplomacy and statecraft. Unlike conventional warfare, cyber warfare is a borderless activity, acts at high speed and can cause serious damage without the involvement of armed forces and without the attackers' identity being disclosed. These features violate traditional norms of sovereignty, attribution, use of force and state responsibility. While there is no comprehensive treaty that governs cyber warfare, this study shows that UN Charter, customary international law, International Humanitarian Law, International Human Rights Law and Articles on State Responsibility (ARSIWA) together constitute legal framework for regulation of state behaviour in cyberspace. The applicability of existing international law is confirmed by reports by UN Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG), although there is a dispute over its interpretation. The biggest obstacle to accountability is problem of attribution, a principal finding. In the cases of cyber operations, legal responsibility under international law is hard to establish because they often use proxy servers, botnets, encryption, false-flag and transnational infrastructures. The increasing occurrence of the involvement of proxy actors, private cybersecurity companies, patriotic hackers, and cybercriminal groups further muddles the accountability issue of states, and there is a need to further define notions like effective control, due diligence or indirect responsibility. The major cyber incidents outlined such as those in Estonia in 2007, Georgia in 2008, Stuxnet in 2010, SolarWinds in 2020 and Colonial Pipeline in 2021 demonstrate that cyber operations are now an important part of contemporary security, alongside military and intelligence measures and economic strategies, and have brought critical civilian infrastructure to new and significant threats. The study poses a call to action for enhanced cooperation and collaboration, institutionalization, information exchange, and strengthening cyber capabilities at international level. A more pragmatic way forward will be to adapt the current global legal framework progressively over time. There is a need for more clarity and direction on issues of attribution, cyber uses of force, sovereignty, critical infrastructure protection and AI-powered cyber operations to ensure accountability, safeguard human rights and uphold a rules-based international order in an increasingly complex digital world.

2.Botanical background and chemical constituents

Cymbopogon citratus belongs to the grass family Poaceae. It forms dense clumps of long, aromatic leaves and is harvested mainly for steam-distilled essential oil or for direct use of the dried foliage. Citral (the mixture of neral and geranial) normally accounts for the largest fraction of the oil, frequently 40–70 %, accompanied by geraniol, nerol,

limonene and smaller amounts of other monoterpenes. Leaf powders and aqueous extracts contain residual volatiles together with flavonoids and other polar constituents.Citral disrupts bacterial membranes and interferes with energy metabolism, explaining much of the observed antimicrobial activity against aquaculture pathogens such as Aeromonas hydrophila. Antioxidant effects arise both from direct radical scavenging and from stimulation of endogenous enzyme systems. These properties provide a rational basis for exploring lemongrass as a functional feed ingredient.

3.Influence on growth performance and feed utilisation

Most trials conducted before 2023 reported positive growth responses when lemongrass was included at moderate levels. In Nile tilapia, dietary essential oil at 200 or 400 mg kg^{-1} for twelve weeks improved final weight, specific growth rate and feed utilisation relative to an unsupplemented control (Al-Sagheer et al., 2018). Similar trends appeared with higher oil inclusions in other tilapia studies (Brum et al., 2017; Saccol et al., 2018).African catfish (Clarias gariepinus) responded well to leaf meal or powder. Inclusion rates between 5 and 10 g kg^{-1} commonly increased weight gain and specific growth rate while lowering or maintaining feed conversion ratio (Dada, 2015; Adeniyi et al., 2017; Adebayo et al., 2018). One economic assessment indicated a more favourable benefit–cost ratio at the higher end of the effective range.In tambaqui (Colossoma macropomum), essential oil at 0.25 or 0.50 ml kg^{-1} produced measurable gains in weight over a 60-day period, accompanied by elevated intestinal protease activity (Copatti et al., 2022).

Improvements in feed efficiency have been linked to greater digestive-enzyme activity, modest changes in gut morphology and, in some cases, reduced metabolic stress. Dose–response curves frequently show an optimum beyond which further increases yield little additional benefit or even slight declines, underscoring the need for careful calibration.

4.Haematological, immune and antioxidant responses

Haematological values in lemongrass-fed fish have generally remained within normal ranges or shown modest positive shifts. Red-cell counts, haemoglobin and haematocrit tended to be stable or slightly elevated, indicating absence of toxicity and possible support of oxygen transport. White-cell responses varied; some trials recorded higher counts consistent with immune activation, while others observed lower values that authors interpreted as reduced infectious or stress burden.Innate immune markers frequently improved. Lysozyme activity and total immunoglobulin levels rose in tilapia receiving essential oil (Al-Sagheer et al., 2018). Antioxidant enzymes such as superoxide dismutase and catalase increased, while lipid-peroxidation markers declined in several studies (Brum et al., 2018; Saccol et al., 2018). These changes suggest that lemongrass can help maintain redox balance under the oxidative load typical of intensive culture.Collectively the pre-2023 data portray lemongrass as a mild immunomodulator and antioxidant rather than a potent pharmacological agent, a profile compatible with continuous dietary use.

5.Resistance to experimental infection

Challenge trials provide the most direct evidence of health benefit. Nile tilapia fed lemongrass essential oil or combinations containing the oil showed higher survival and fewer tissue lesions after Aeromonas hydrophila infection (Brum et al., 2017; Al-Sagheer et al., 2018). African catfish receiving leaf powder exhibited improved survival when subsequently challenged with Aeromonas salmonicida (Adebayo et al., 2018).In tambaqui the essential-oil treatments improved pre-challenge health indicators, although post-challenge survival differences were not always statistically significant (Copatti et al., 2022).

In-vitro assays have confirmed inhibitory activity of lemongrass oil and extracts against several fish-pathogenic bacteria, reinforcing the biological plausibility of the in-vivo results. Protection appears more consistent when the additive is supplied prophylactically at growth-promoting doses than when it is used as a sole therapeutic measure during acute outbreaks.

6.Practical dosage ranges and formulation notes

Synthesis of the available trials suggests the following approximate working ranges (subject to product composition and species):

- **Essential oil:** 0.25–0.50 ml kg^{-1} diet for tambaqui; 200–400 mg kg^{-1} for tilapia.
- **Leaf powder or meal**: 5–10 g kg^{-1} for African catfish, with some benefit recorded at lower levels.

Essential-oil components are volatile; losses during pelleting can be reduced by encapsulation or late-stage addition. Leaf powders are simpler to prepare in regions where the plant grows abundantly and may therefore suit small- and medium-scale producers. Palatability remains acceptable at the effective doses reported.

7.Safety considerations

Within the inclusion levels tested up to 2022, survival, organ indices and routine haematology showed no consistent adverse trends. Occasional improvements in these parameters further support safety. Residue data specific to fish were still limited by the end of 2022, yet the rapid metabolism of monoterpenes in vertebrates suggests low risk of accumulation in edible tissues under normal feeding periods.

8.Limitations and research needs

Most studies available by 2022 were short-term (4–12 weeks) and performed under controlled laboratory or semi-intensive conditions. Commercial-scale, long-duration trials remained scarce. Species diversity was narrow, with heavy emphasis on tilapia and African catfish. Standardisation of citral content and extraction methods was incomplete, complicating dose translation between laboratories. Mechanistic work on gut microbiota, precise molecular pathways and interactions with other feed components was only beginning.Future investigations should therefore prioritise multi-site field trials, broader species coverage, product standardisation, economic analyses and combined use with probiotics or other phytogenics.

9.Conclusions

Experimental evidence published up to 2022 indicates that dietary lemongrass (Cymbopogon citratus), whether supplied as leaf powder, aqueous extract or essential oil, can improve growth performance and feed efficiency, support haematological and innate-immune parameters, enhance antioxidant status and contribute to greater resistance against bacterial challenge in several important aquaculture species. Effective doses are moderate and the safety margin appears adequate. Because the plant is inexpensive and widely available, it constitutes a realistic option for reducing dependence on antibiotics and synthetic growth promoters. Continued work to refine dosages, confirm long-term commercial performance and clarify mechanisms will strengthen the basis for routine use.

References

1. Commission, I. L. (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries. United Nations.
2. Commission, I. L. (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries . United Nations.
3. Cross, I. C. (2021). International humanitarian law and cyber operations during armed conflicts. Geneva: Geneva: ICRC.
4. Delerue, (. (October 2019). Reinterpretation or Contestation of International Law in Cyberspace? : 21 October 2019). Israel Law Review, Published online by Cambridge University Press.
5. Douwe Korff. (January 2019). First do no harm: the potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions in Research Handbook on Human Rights and Digital Technology). Douwe Korff, First do no harm: the potential of harm being causPublis.
6. Finnemore, M. &. (1998). International norm dynamics and political change. International Organization, 52(4), 88-917.
7. Healey, J. (. (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association.
8. Kavanagh, (. D. (2019). Cybersecurity and human rights. Handbook on Human Rights and Digital Technology, 73–97 Publisher: Edward Elgar Publishing).
9. Keohane, R. O. (2012). Power and Interdependence (4th ed.). Pearson. Pearson.
10. Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.
11. Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365-404.
12. Madeline Carr. (2017). (Madeline Carr, Cyberspace and International Order. The Anarchical Society at 40: Contemporary Challenges and Prospects (pp. 1-25). Oxford.
13. Morgenthau, H. J. (1948). Politics Among Nations. Alfred A. Knopf. Alfred A. Knopf.
14. Nye, J. S. (2011). The Future of Power. . PublicAffairs.
15. Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. Ottis, R. (2008). Analysis of the 2007 cyber attackProceedings of the 7th European Conference on Information Warfare and Security, 163–168.
16. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. . Australian Journal of Defence and Strategic Studies, Volume 2, Number 2 (2020), 269-274.
17. Sander, (. (May 2019). The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations. 11th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia).
18. Schelling, T. C. (1966). Arms and influence. Yale University Press.
19. Schmitt, (. S. (n.d.). An international attribution mechanism for hostile cyber operations. International Law Studies, Volume 96 2020, Stockton Center for International Law, P.215.
20. Schmitt, M. N. (2017). Tallinn Manual 2.0 on International Law Applicable to Cyber Operations. Cambridge University Press.
21. Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
22. Segal, A. (2016). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs.
23. Valeriano, B. &. (2015). Cyber War versus Cyber Realities. Oxford University Press. Oxford University Press.
24. Walker, (. A. (2015). Law of horse to law of the submarine: The future of State behavior in cyberspace,. 7th International Conference on Cyber Conflict: Architectures in Cyberspace. Tallinn, Estonia).
25. Wendt, A. (1999). Social Theory of International Politics. Cambridge University Press.