APPLICABILITY OF INTERNATIONAL LAW IN CYBERSPACE[i]

Written by ***Zakayo Lukumay***

Senior Lecturer, The Law School of Tanzania, Dar es Salaam, Tanzania

ABSTRACT

This Article aims at examining the applicability of International Law principles on cyberspace as response to the increasing cyber-attacks. It should be borne in mind that global challenges facing the modern international community cannot be adequately addressed by any single international actor, irrespective of how powerful that actor may be.

It was observed in this Article that the law of war is comprised of well-known and widely accepted principles. Applying these principles to cyber-attacks poses challenges. The reason is that the principles were developed in response to conventional wars between states. Unfortunately, when a cyber-attack is launched, it becomes difficult for states to figure out who is responsible for it. For this reason, states have been reluctant to respond to cyber-attacks in self-defense for fear of violating the law of war.

It is recommended that, first, an international binding instrument under the auspices of the United Nations should be put in place. In view of the fact that cybercrime conventions/instruments can be overtaken by technological advances, there is need for technological neutral legal instruments.

Second, international cooperation is critical in curbing cybercrimes. However, such cooperation can only be achieved when an agreement has been reached on what activities should be outlawed. Harmonization of the fragmented laws is a first step towards international cooperation.

Third, technological wise, state governments should impose censorship to block internet contents that tend to threaten the security of the country as well as protecting citizens, particularly the vulnerable ones like children.

Keywords: International Law, Cyberspace, Applicability

INTRODUCTION

Afroditi[ii] once wrote that:

> *in the not-so-distant future, a concerted 'Cyber Attack', effectuated via the Internet, could cause massive destruction to any society dependent on computer networks, especially in key target fields of transport, energy supply and communication infrastructures, leading to human casualties and serious destruction of property – reproducing the same, if not more, damage that would be caused by conventional armed attacks.*

The above statement is a warning that cyberattacks could reach critical infrastructure or even cause harm to people now that so many devices are connected to the internet if no action is taken in the near future. The world is likely to witness disruptions of major operations that depend on computer networks particularly at this time of Covid-19 pandemic which has forced many companies and governments to rely heavily on ICT in all transactions. Security of things like communication, militaries are now beginning to consider cyber as a military domain, with the potential to exploit networked assets and use internet-based attacks in addition to or instead of their use of conventional weapons. Such disruptions may cause physical damages leading to deaths of innocent citizens. A "distributed denial of service" attack can take the entire population in a country offline. There is danger that a terrorist may use the internet to mount an attack.

The purpose of this discourse is to examine the applicability of international law principles to cyberspace in order to respond to the threat of cyber-crime. The reason for this is that the global

challenges facing the modern international community cannot be adequately addressed by any single international actor, irrespective of how powerful that actor may be.

THE NATURE OF CYBERSPACE

Information Technology (IT) or Information and Communications Technology (ICT)[iii] continue to have an ever-growing impact upon society and the way that society conducts its affairs.[iv] ICT usage has permeated almost every professional, commercial and industrial activity and many organizations would find it difficult, if not impossible, to function without relying heavily on computers.[v] As a result, ICT has, in the recent years, gained a very important place in both the national and international economies in the world,[vi] drastically transforming the way business is conducted, services are rendered, products are sold and communications are handled.[vii]

Indeed, the technology revolution has had a profound and irreversible impact on the way the world is moving and interacting whereby the new technologies provide for cheaper, easier and faster solutions to the traditional way of living since the mid-90s.[viii] As a result, ICT has been used as a tool, changer, catalyst, sharpener and solution to some of the most annoying problems.[ix] For example, the convergence of technologies in telecommunications, broadcasting and computers create a new market place with a two-way flow of information involving the processing and transmission of data, including text, sound and video in diverse activities.[x] These activities include electronic trading of goods and services, online delivery of digital content, electronic funds transfer, electronic share trading and many others.[xi] It is these activities that have given birth to e-terminologies like e-finance, e-money, e-banking, e-learning, e-brokering, e-insurance, e-ticketing, e-exchanges, e-commerce, e-government, and the list goes on as the technology rapidly advances[xii] creating what is now referred to as cyberspace.

The United States Department of Defense (DoD) defines cyber as:

> *a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet,*

> *telecommunications network, computer systems, and embedded processors and controllers.*[xiii]

It is also defined as a domain characterized by the use of electronics and the electromagnetic spectrum to store, modifies, and exchange data via networked systems and associated physical infrastructures.[xiv] The Armed Forces of the United States defines cyber-space as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[xv]

The global cyber system is expanding at an exponential pace, with ever greater dependence of, *inter alia*, the energy, transportation, economic, financial and military critical infrastructures on networking.[xvi]

This dependence on technology on all facets of human life has provided opportunities for criminals to exploit security vulnerabilities in the on-line environment. The cross-national nature of most computer related crimes has rendered many time-honoured methods of policing both domestically and in cross-border situations ineffective even in advanced nations, while the 'digital divide' provides 'safe havens' for cyber-criminals.

The United States possesses the most powerful and technologically advanced military forces in the world and has successfully deterred most conventional attacks against its homeland.[xvii] Recently, the Federal agencies have warned that the US healthcare system is facing an "increased and imminent" threat of cyber crime, and that cyber criminals are unleashing a wave of extortion attempts designed to lock up hospital information systems, which could hurt patient care just as nationwide cases of Covid-19 are spiking.[xviii]The alert said malicious groups are targeting the sector with attacks that produce "data theft and disruption of healthcare services."[xix] Charles Carmakal, chief technical officer of the cyber security firm Mandiant, is reported to have said that: "We are experiencing the most significant cyber security threat we've ever seen in the United States,"[xx]

It is reported that in September, a ransomware attack hobbled all 250 US facilities of the hospital chain Universal Health Services, forcing doctors and nurses to rely on paper and pencil

for record-keeping and slowing lab work. Employees described chaotic conditions impeding patient care, including mounting emergency room waits and the failure of wireless vital-signs monitoring equipment.[xxi]

The UK's National Cyber Security Centre found evidence that Russian military intelligence hackers had been planning a disruptive cyber-attack on the later-postponed 2020 Tokyo Olympics.[xxii] Again, in October, 2020, the U.S. indicted six Russian GRU[xxiii] officers for their involvement in hacking incidents including the 2015 and 2016 attacks on Ukrainian critical infrastructure, the 2017 NotPetya ransomware outbreak, election interference in the 2017 French elections, and others. In another incident, a Chinese group targeted diplomatic entities and NGOs in Africa, Asia, and Europe using advanced malware adapted from code leaked by the Italian hacking tool vendor HackingTeam.[xxiv]

Unfortunately, these attacks have proven that no single country is immune despite its superiority in all aspects.

THE NATURE OF CYBER CRIME

There is no commonly agreed single definition of cybercrime. Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission. Cybercrime encompasses any criminal act dealing with computers and networks. Cybercrime is "international" or "transnational" – there are 'no cyber-borders between countries'. Cybercrime includes unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and response is typically the jurisdiction of law enforcement agencies. It becomes a cyber-attack when a national security is threatened.

Cyberattack" is a relatively recent term that can refer to a range of activities conducted through the use of information and communications technology (ICT). The use of Distributed Denial of Service (DDoS) attacks has become a widespread method of achieving political ends through the disruption of online services. In these types of attacks, a server is overwhelmed with Internet traffic so access to a particular website is degraded or denied. The advent of the Stuxnet worm, which some consider the first cyber weapon, showed that cyber attacks may have a more

destructive and lasting effect. An example of a cyber attack is distributed denial of service attack, planting inaccurate information, infiltrating a secure computer network.

The challenging characteristics of cybercrime is the fact that it is borderless and cross territorial in nature, and its impacts are much wider than those of traditional crimes. This means that while the legal and institutional frameworks are grounded on real geographical locations, cybercrimes are not affected by physical boundaries as such. For that matter, cybercrime poses threats not only to the confidentiality, integrity or availability of computer systems, but also to the security of critical infrastructure.[xxv]

It is for this reason that a call for the fight against this contemporary form of criminality inevitably necessitates employing individual and the collective initiatives and efforts among States at regional and inter-regional levels to combat the same. For this reason, different countries including Tanzania are adopting their own strategies to face the challenges posed by cyber criminals. Some of such strategies include having a piece of legislation to curb the vices caused by ICT.

There is no consensus on which acts should be outlawed and this makes international cooperation more difficult. Cooperation among and between governments in pursuing cyber criminals is possible when we can speak the same language as far as cybercrimes is concerned. We can achieve this end by harmonising our cybercrimes laws and enhance cooperation in enforcement.

However, many countries' cybercrime legislation also categorizes publishing or transmission of illegal content in a particular country via computer networks or the internet as "cybercrime". The Cybercrime Act of 2015 of Tanzania, for example, criminalises activities like: illegal access, illegal remaining, illegal interception, illegal data interference, data espionage, illegal system interference, illegal devices, computer related forgery, child pornography, pornography, identity related crimes, publication of false information, racist and xenophobic material, racist and xenophobic motivated insult, genocide and crimes against humanity, unsolicited massages, disclosure of details of an investigation, obstruction of investigation, cyber bulling, violation of intellectual property rights. Other offences are aiding and abetting,

attempt to commit an offence, conspiracy to commit offence and offences relating to critical infrastructure.

Upon conviction the offender maybe condemned to a jail term or a fine or compensation or all the above depending on the offence. The heaviest sentence under the Act is imprisonment for not less than seven years and a fine of not less than one hundred million Tanzanian Shilling.

The problem with country specific legislation is that there is no agreement on what constitutes crime. When state's laws criminalise content that other countries do not recognise as criminal, and then devote cybercrime enforcement resources to chasing this kind of "crime" rather than what people generally think of as cybercrime, it complicates or prevents international cooperation, discredits cybercrime legislation and enforcement efforts, and diverts resources from solving the serious problem of cybercrime.

As pointed out elsewhere in this Article, the potential serious consequence of a cyber-attack could include catastrophic consequences as meltdown of the economy, total disruption of the transportation system and widespread property destruction and death.[xxvi]

APPLICATION OF INTERNATIONAL LAW

The global reach of the Internet has made it possible for computer related crimes to come from outside the borders of one state. For this reason, cybercrime is an international crime. An international crime is an act which the international community recognises as not only a violation of ordinary State criminal law but one which is so serious that it must be regarded as a matter for international concern.[xxvii]

Solutions to the problems posed by cybercrime can be addressed by international law through the adoption of binding international legal instruments - Treaties and conventions, customary international law, general principles and scholarly works.

Application of international law on cyberspace poses a number of issues like global governance of cyberspace, sovereignty of states on cyber infrastructures, online data, cyber activities and

governance of internet within its own jurisdiction, online freedom, application of the law of armed conflict to cyberspace and international cooperation in combatting criminal activities in cyberspace.

NATIONAL LEGAL FRAMEWORK ON CYBERCRIME IN TANZANIA

Tanzania was late to receive cyber technology as in 1990s is when it received this technology since then there being serious problems caused by this technology. Tanzania has recorded significant development of ICT applications at a very fast rate thus boosting the economy.[xxviii] The increasing capacity of ICT has further been empowered by the growth of a global network of computer known as internet, which open up new ways of committing crimes through the internet as most of the people in Tanzania use the internet especially the companies which make the extensive use of the networked computers. For example, the banking sector makes heavy use of ICT to provide improve customer service which some banks using Very Small Aperture Terminal (VSATs) or public leased lines to interconnect their branches and cash dispensing Automatic Teller Machines (ATMs).[xxix]

In 2015, Tanzania enacted two pieces of legislation in response to challenges associated with the advancement of ICT. These are the Cybercrimes Act of 2015 and the Electronic Transactions Act of 2015. Apparently, while ETA borrowed heavily from UNCITRAL Model Law on Electronic Commerce, Cybercrime Act does the same from the African Union Convention on Cyber Security and Personal Data of June 2014. Under Article 25,[xxx] the Convention requires member states to adopt legislation to combat cybercrime.

The Cybercrime Act aims at making provisions for criminalizing offences related to computer systems and Information Communication Technologies and to provide for investigation, collection, and use of electronic evidence[xxxi] and for matters related therewith. The crimes include illegal Access, illegal interception, illegal data interference, data espionage, illegal system interference, illegal device, computer-related forgery, computer-related fraud, child abuse and identity related crimes, among others.[xxxii]Apparently, the enactment of the Cybercrime Act is a response to the difficulties faced in prosecution of crimes committed

through the use of computers and computer networks. The Act was not meant to prevent the exchange and drafting of information but to protect people from abuse, such as online fraud.

The provision that can be applied is section 16 the Cyber Crime Act.[xxxiii] It provides that:

> *Any person who publishes information or data presented in a picture, text, symbol or anyother form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with internet to defame, threaten, abuse, insult or otherwise deceive or misleading public or concealing commission of an offence, commits an offence, and shall on conviction be liable to a fine of not less than five million shillings.*

Upon conviction, the offender may be condemned to a jail term or a fine or compensation or all the above depending on the offence. The heaviest sentence under the Act is imprisonment for not less than seven years and a fine of not less than one hundred million.

In a similar vein, section 103 of the Postal and Electronic Communication Act, CAP 306 allows the Minister to make regulations in respect to content- related matters. Based on this, in 2018, the Minister published regulations entitled the Electronic and Postal Communications (Online Content) Regulations, 2020. Under Regulation 4, a person is required to obtain a license to provide online content.[xxxiv] Sub-rule 2 imposes a fine of Tanzania Shilling Five Millions (Tshs. 5,000,000/=) in contravention of sub-regulation 1.[xxxv]

The regulations[xxxvi] prohibit some content from being published online.[xxxvii] These content in relation to sexuality and decency; personal privacy and respect to human dignity, public security, violence and national safety, criminal activities and illegal trade activities, healthy and public safety, protection of intellectual property rights; respect to religion and personal beliefs; public information that may cause public havoc and disorder; use of bad languages and disparaging words and false, untrue, misleading content.[xxxviii] Sub-regulation 21 imposes a fine of Tanzania Shilling Five Millions (Tshs. 5,000,000/=) in contravention of the provisions of the regulations.

There is, however, no consensus on which acts should be outlawed and this makes international cooperation more difficult.[xxxix] Many countries' cybercrime legislation categorizes publishing or transmission of illegal content in a particular country via computer networks or the internet as cybercrime.[xl] The closest provision is section 66A[xli] of the Information Technology Act of India which reads:

> *Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.*

In and Indian case of *Shreya Singhal v. Union of India* the Supreme Court determined the main issue whether Section 66A of ITA violated the right to freedom of expression guaranteed under Article 19(1)(a) of the Constitution of India. As an exception to the right, Article 19(2) permits the government to impose "reasonable restrictions . . . in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offense."

Invalidating Section 66A of the Information Technology Act of 2000 in its entirety, the Court held that the prohibition against the dissemination of information by means of a computer resource or a communication device intended to cause annoyance, inconvenience or insult did not fall within any reasonable exceptions to the exercise of the right to freedom of expression.

In this case, Police arrested two women for posting allegedly offensive and objectionable comments on Facebook about the propriety of shutting down the city of Mumbai after the death of a political leader. The police made the arrests under Section 66A of the Information Technology Act of 2000 (ITA), which punishes any person who sends through a computer resource or communication device any information that is grossly offensive, or with the knowledge of its falsity, the information is transmitted for the purpose of causing annoyance, inconvenience, danger, insult, injury, hatred, or ill will.

Commenting on the usefulness of the repealed provision, Halder[xlii] noted that a brief over view of the judgement may show that there are several issues which the Court did not address or left unattended while judging the necessity of the existence of Section 66A. One such issue is the decision or the lack of on the type of "information" that may not be considered as open to be viewed by cyber bystanders. In the cyber space communication, certain information may essentially involve questions of privacy. Chilling of speech becomes essential when such privacy is infringed. Internet speech can become viral in nature if the harasser wishes to gather more viewers to witness humiliation of the victim. If such information consists of speech which may turn its character from a 'free speech' to a dangerous information due to the viral nature of the internet, the person who makes such speech must be made liable for punishment, depending upon his prior knowledge about the consequence of such use of internet.

The above case and the comment show that countries are not in wide agreement as far as online content regulation is concerned. [xliii] When state's laws criminalize content that other countries do not recognize as criminal, and then devote cybercrime enforcement resources to chasing this kind of crime rather than what people generally think of as cybercrime, it complicates or prevents international cooperation, discredits cybercrime legislation and enforcement efforts, and diverts resources from solving the serious problem of cybercrime. Cooperation among and between governments in pursuing cybercriminals is possible when we can speak the same language as far as cybercrimes is concerned. This end can be achieved by harmonizing our cybercrimes laws and enhance cooperation in enforcement.

The next section presents a discussion on how international instruments be applied to cyberattacks**.** The instruments and theories that will be examined are the International Covenant on Civil and Political Rights (ICCPR), universal principal theory, the Rome Convention to Cyber terrorism, the Budapest Convention, the Law of Armed Conflict to Cyber Warfare and the Tallinn Manual.

APPLICATION OF ARTICLE 19 OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (ICCPR) TO REGULATE ONLINE CONTENT

For some states, free speech is an exceptionally important principle. For others, the control of offensive or dangerous content is essential. Achieving agreement on how to approach these differences is, frankly, going to be a challenge.

Article 19(3) of the ICCPR imposes restrictions in respect of the rights of reputations of others and for protection of national security, or public order, or public health or morals. Again, apart from its beneficial role, the Internet is open to misuse, giving the State a justification to regulate online content in the interests of the public at large. We have all witnessed several cyber-crimes, defamation, invasion of privacy, incitement of offences, racist remarks, stalking, abuse, hacking, harassment being committed through social media and once such objectionable content is uploaded, it becomes viral and consequently, very difficult to contain. Hence, the importance of the State regulating social media cannot be denied.

Tanzania, for example, should be able to exercise extra- territorial jurisdiction over people who violate the above provision under Article 19 of the ICCPR using section 16 of the Cybercrime Act of 2015 and the Electronic and Postal Communications (Online Content) Regulations, 2020. By its nature, the internet allows every person to be an instantaneous broadcaster and an author. It allows a person to communicate anything to the entire world on instantaneous basis.[xliv] It is for this reason that Tanzania has decided to enact the law to regulate the use of the internet

Critics have, however, argued that the above provision infringe the right of expression guaranteed by the Constitution of the United Republic of Tanzania as well as international instruments.

It is the strong view of the author of this article that one should enjoy his freedom of expression in a manner that it does not affect human rights of others. As Duggal[xlv] noted, people should not have a feeling that their right to freedom of speech and expression is an absolute right when

it comes to the internet. For this reason, restrictions to the freedom of speech in the cyber world are needed to give protections to the human rights. These restrictions are very important as the misuse of the internet may threaten national security, public order or the lawful rights and freedom of others, including the rights of privacy and intellectual properties Restrictions are also made to meet the demand of fairness in accordance with morality consideration and religion values.

UNIVERSAL JURISDICTION THEORY

The theory of universal jurisdiction allows a state to claim criminal jurisdiction over an accused person regardless of where the alleged crime was committed and regardless of the accused's nationality, country of residence, or any other relation with the prosecuting entity.

A country can invoke universal jurisdiction when the offence has the international character like piracy, genocide, crimes against humanity, extrajudicial executions, war crimes, torture and forced disappearances.[xlvi]It is argued that cybercrime has international character; hence universal jurisdiction theory can apply as it has the potential of causing a serious threat to the international community as a whole that states have a logical and moral duty to prosecute an individual responsible. However, the scope and application of universal jurisdiction must be clearly defined to avoid abuse of the principle, which could endanger international law, order and security.[xlvii]

According to Amnesty International, a proponent of universal jurisdiction, certain crimes pose so serious a threat to the international community as a whole that states have a logical and moral duty to prosecute an individual responsible; therefore, no place should be a safe haven for those who have committed genocide, crimes, extrajudicial executions, war crimes, torture and forced disappearances.

APPLICATION OF THE ROME CONVENTION TO CYBER TERRORISM

The increase of international cyber terrorism in recent years has resulted in computer-based criminal activities that generate worldwide fear, destruction and disruption. Cyberterrorism can be considered "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."[xlviii]

National laws and policies that address cyber terrorism are mainly limited to developed nations and are not cohesive in managing 21st century cyber terrorism. Given the absence of an international legal framework to address cyber crimes, authorities and governments around the world face extreme challenges in finding and prosecuting those responsible for cyber terrorism.[xlix]

In March 1988 a conference in Rome adopted the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation. The main purpose of the Convention is to ensure that appropriate action is taken against persons committing unlawful acts against ship.[l]It is argued that this Convention can as be used to curb cyber terrorism.

THE USE THE BUDAPEST CONVENTION

Legal challenge on cybercrimes is that, electronic evidence can be very difficult to obtain when it is scattered across a system located in different countries whereby success will in most cases depend on the international cooperation between the countries.[li]

Article 23 of the Budapest Convention states enjoins parties to co-operate with each other, in accordance with the provisions of the Convention, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related

to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

The problem is that this convention does not resolve issues of international jurisdictions. It leaves cooperation on the good will of a third country. The convention is also short on giving states the necessary weapons to fight this type of crime.

APPLICATION OF THE LAW OF ARMED CONFLICT (LOAC) TO CYBER WARFARE

The Law of Armed Conflict (LOAC) is comprised of a specific set of principles that apply in a distinct situation that involves violence, destruction, injury, and death. It applies only when States or armed groups have broken the peace. At least one (and often more) of the parties involved in the armed conflict have already shown disdain for legal constraints on behavior by their resort to violence in the first place. Still, the body of law applies to all parties involved in an armed conflict, regardless of whether the conflict is just or unjust, and no matter who started it.

LOAC is critically important for regulating conduct in warfare. It limits the use of inhumane weapons, prohibits the targeting of civilians and civilian property, and guards the wounded and captured, among other things. The question that should task our mind is: Does LOAC apply to cyber warfare?

The United Kingdom has identified cyberspace as a likely medium of conflict, one standing on equal footing with such traditional media as land, sea and airspace. It went further to characterize a cyber-attack including by either States, and by organized crime and terrorists' as one of four 'Tier One' threats to British national security, the others being international terrorism, international military crisis between states and a major accident or natural hazard.[lii]Despite these developments, cyber armed conflict has introduced a host of unique issues to the bodies of international law governing warfare.[liii] Time and geography offer few limits to cyber operations, which can happen in less than the blink of an eye anywhere on the

globe. Further, most of the modern LOAC developed when States had a monopoly on the means of warfare but, unlike tanks, ships, and bombers, cyber techniques are widely available to the public. Also, there are real questions about which cyberspace activities would violate "cyber sovereignty." For example, do electronic penetrations of computer systems violate territorial sovereignty as military invasions do?

Cyberwar is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force. In the current absence of specific jus ad bellum rules,[liv]we are left with the provisions contained in the UN Charter.

How can the principle of *jus ad bellum* be applied in Cyber Attacks? To answer this question, we must begin by reference to Article 2(4) of the UN Charter as the general rule. The answer would be affirmative only if one should conclude that a cyber-attack triggers the right to self-defense under Article 51 of the UN Charter or under customary international law. However, Article 2(4) generally prohibits the use of force except in the case of self-defense as set out in Article 51 or with Security Council authorization. The issue is whether Article 51 of the UN Charter can be interpreted as allowing a reaction in self-defense against a cyber attack

Article 51 of the UN Charter provides that,

> *Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.*

Thus, the state victim of a use of cyber force will thus be entitled to react in self-defense only to the extent that such use of cyber force can be qualified as an "armed attack". In the Nicaragua case, the ICJ acknowledged that a definition of "armed at-tack" does not exist in the Charter and is not part of treaty law. The ICJ, however, made clear that Article 51 does not refer to specific weapons and that it applies to "any use of force, regardless of the weapons employed." According to Article 2, the fact that cyber attacks do not employ traditional kinetic weapons does not necessarily mean they cannot be "armed"[lv].

When attributed to a state, a cyber attack is a violation of the customary principle of non-intervention "on matters in which each State is permitted, by the principle of State sovereignty, to decide freely", such as "the choice of a political, economic, social and cultural system, and the formulation of foreign policy. For this reason, several of the situations described in the 1981 UN General Assembly Declaration on Non-intervention would perfectly cover cyber attacks. The Declaration reiterates:

> *the right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations, based, inter alia, on the relevant articles of the Universal Declaration of Human Rights and the principles of the new international information order.*

The question is, are all uses of cyber force "armed attacks"? It is well-known that the ICJ identified "the gravest forms of the use of force", i.e. armed attacks, and less grave forms and adopted the "scale and effects" criterion in order to distinguish them.

According to the ICJ, an armed attack must be carried out "with the specific intention of harming. Nonetheless, the problem is whether a cyber attack on the computer network of any civilian infrastructure could potentially amount to an armed attack (providing it satisfies the scale and effects criterion). It has been claimed, for instance, that, as Google is the most powerful presence on the Internet, an attack on it would be an attack on the United States critical infrastructure. There is no agreement, though, on what "critical infrastructures" are. The UN General Assembly recognized that "each country will determine its own critical information infra-structures."[lvi]

The problem of the identification of national critical infrastructures is further complicated by the fact that, in most countries, the majority of such infrastructures are owned by the private sector. At the end of the day, the notion of "critical infrastructure" is linked to that of "national security", which is equally difficult to define, both in domestic and international law.

The reaction in self-defense against cyber attacks amounting to armed attacks must meet the requirements of necessity, proportionality and immediacy. Necessity means that the use of force is a means of last resort and that all other available means have failed or is likely to fail. As a minimum, it implies an obligation to identify the author, verify that the cyber attack is not an accident and that the matter cannot be settled by less intrusive means (for instance, by preventing the hackers from accessing the networks and websites under attack through the use of cyber defenses). The major problem with using self-defense to react against a cyber attack is the identification of the aggressor.

Aware of this difficulty, certain commentators have suggested that responses in self-defense to a cyber attack against national critical infrastructures should be allowed even without first attributing and characterizing the attack. According to this view, "the law should permit an active response based on the target of the attack, regardless of the attacker's identity." This position, however, cannot be accepted.[lvii]

Apart from being at odds with the law of state responsibility, it is inherently illogical. If it has not yet been established where the attack comes from and to whom it is attributable, against whom and where will the reaction be directed?

The challenge is also for the victim state to be able to identify the origin of the cyber attack and attribute the conduct to a state. Another problem lies in the fact that, in case of a DDoS attack carried out by millions of hijacked computers, the risk of a counter cyber attack for the actual attacker would be negligible, because the counter attack will be directed towards the hijacked computers (which could be located even in the victim State. Here State then better s should be capital letter).

According to Roscini,[lviii] the United States has repeatedly taken a stance in favor of the right to self-defense against cyber attacks. The 1999 DoD's Assessment of International Legal Issues in Information Operations puts it that "[s]tate-sponsored [cyber] attacks may well generate the right of self-defence."[lix] The document goes on to say, that "if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no

one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed at-tack."[lx]

The 2003 United States National Strategy to Secure Cyber-space[lxi] states that an investigation, arrest, and prosecution of the perpetrators, or a diplomatic or military response in the case of a state sponsored action will follow large cyber incidents. More ambiguously, the 2006 National Security Strategy affirms that the United States is "pursuing a future force that will provide tailored deterrence of both state and non-state threats (including WMD [Weapons of Mass Destruction] employment, terrorist attacks in the physical and information domains, and opportunistic aggression) while assuring allies and dissuading potential competitors.[lxii]

TALLINN MANUAL

Tallinn Manuals were written by groups of international legal experts (the Experts) gathered by the CCD COE and Michael N. Schmitt, a prominent global cyber expert. The first group included law of armed conflict (LOAC).[lxiii] The first group included law of armed conflict (LOAC) experts primarily from the Western Hemisphere. In response to criticism, the international group of experts for Tallinn 2.0 was broader both in origin (including members from Thailand, Japan, China, and Belarus) and substantive expertise (including experts in human rights, space law, and international telecommunications law). The International Committee of the Red Cross (ICRC) was invited to send observers to both groups as were other states and organizations.[lxiv]

The intent of the project was never to make law or to produce a manual that would have the force of law. As the introduction makes clear:

> *Ultimately, Tallinn Manual 2.0 must be understood only as an expression of the opinions of the two International Groups of Experts as to the state of the law .... This Manual is meant to be a reflection of the law as it existed at the point of the Manual's adoption by the two International Groups of Experts in June 2016. In is not a 'best practices' guide, does not represent 'progressive development of the law', and is policy*

> *and politics-neutral. In other words, Tallinn Manual 2.0 is intended as an objective restatement of the lex lata.*

The Tallinn Manual breaks the functionality issue into the following three basic scenarios: A cyber operation can physically damage a component of a computer system, can cause it to cease functioning until the operating system is reinstalled, or can cause it to cease functioning by deleting or interfering with data on the system (e.g., the targeted computer still functions as a computer, but isn't functional as a communications node because the communications program has been deleted).[lxv]

The above observations raise a number of questions:

i) Is cyberspace a battle space between nations?

ii) Can the international law principles on warfare be invoked in the cyber-attacks? and

iii) Can it be established that an attack has been sanctioned by a State?

Due to the anonymous nature of the internet, it has been possible for criminals to engage into a variety of criminal activities in cyberspace. Cybercrimes are considered an anonymous medium where someone's is unknown and cyber criminals can completely hide their real identities. Criminals need not be present at the same location as the target. As the location of the criminal can be completely different from the crime site, many cyber offences are transnational. International cybercrimes offences take considerable effort and time.[lxvi] In most cases, identity of perpetrators is disguised because criminals can attack from a remote site almost from anywhere around the world.[lxvii]

For this reason, it is critical that an international consensus on the role of international law as far as cyberspace is concerned is built. States should engage in negotiations under a mandate from the UN to have a convention on cyberspace.

Such efforts are ongoing. In 2013, for example, the UN Group of Governmental Experts on the use of cyber technologies, affirmed the application of existing international law to states' cyber

activities. On 26 June 2015, the UN Expert Group recognised that the UN Charter applies in its entirety to cyberspace. The Group affirmed the relevance of a state's inherent right to act in self-defence in response to a cyber operation meeting the threshold of an armed attack. In addition, the 2015 Report confirmed that the fundamental protections of international humanitarian law: necessity, proportionality, humanity and distinction, apply in cyberspace.[lxviii]

Despite these developments, more dialogues should be continued particularly on the extent of application of international law on activities in the cyberspace. As pointed out in this paper, it is still not clear as to how the principles of international law can be applied to reduce cyber threats around the globe.

CONCLUSION

We have seen in this Article that the law of war is comprised of well-known and widely accepted principles. Applying these principles to cyber-attacks is a difficult task. The principles were developed in response to conventional wars between states. Unfortunately, when a cyber-attack is launched, it becomes difficult for states to figure out who is responsible for it. For this reason, states have been reluctant to respond to cyber-attacks in self-defense for fear of violating the law of war, and they have turned cyber warfare into one of the hottest topics in international law.

RECOMMENDATIONS

It is recommended that first, an international binding instrument under the auspices of the United Nations should be put in place. In view of the fact that cybercrime conventions/instruments can be overtaken by technological advances, there is need for technological neutral legal instruments.

Second, international cooperation is critical in curbing cybercrimes. However, such cooperation can only be achieved when an agreement has been reached on what activities should be outlawed. Harmonization of the fragmented laws is a first step towards international cooperation.

Third, technological wise, the governments should impose censorship to block internet contents that tend to threaten the security of the country as well as protecting citizens, particularly the vulnerable ones like children.

ENDNOTES

[i]The article was initially presented as a Paper at the 58th Annual Conference of Asian-African Legal Consultative Organization (AALCO) held in Dar es Salaam held on 21-25th October 2019. (See Conference Report at http://www.aalco.int/SR-19%20Nov%202019-final.pdf p. 13).
[ii]Papanastasiou, Afroditi, Application of International Law in Cyber Warfare Operations (September 8, 2010). (See https://ssrn.com/abstract=1673785 or http://dx.doi.org/10.2139/ssrn.1673785 (accessed on October 15, 2020).

[iii] ICT consists of all technical means used to handle information and aid communication, including computer and network hardware as well as necessary software. It is often used as a synonym for Information Technology (IT) but is usually a more general term that stresses the role of communications (telephone lines and wireless signals) in modern information technology. Sometimes ICT is used with technologies in the plural. (See https://www.igi-global.com/dictionary/hoping-best-qualitative-study-information/13620 (accessed on October 15, 2020).

[iv] See D. Bainbridge, *Introduction to Computer Law*, (Harlow, United Kingdom: Pearson, 2004), at 1.
[v]*Ibid*, at 22.
[vi] See A. Mollel and Lukumay Z., *Electronic Transactions and the Law of Evidence in Tanzania*, (Songea: Peramiho Printing Press, 2008) at 1.

[vii] See Debjani, Nag & K.K Bajaj, *E-Commerce: The Cutting Edge of Business*, 2nd Ed, (New Delhi: MK Graw Hill, 2004), at 14

[viii] Majid Yar, *Cybercrime and Society*, 2nd Ed., (New Delhi: Sage, 2013), at 3.
[ix] See Ubena, J., "ICT as a Solution to Delay of Cases in the Administration of Justice in Tanzania", *The Tanzania Lawyer*, Vol. 2, No. 2, 2008, pp. 116-130.

[x] See "A Study Report on Electronic Transactions Law, Uganda Law Reform Commission (2004), p. 10.
[xi]*Ibid*.
[xii] Ringo, C. Z., "Debit Cards and Customer Satisfaction: the Case of CRDB Bank Ltd," MBA Dissertation, the University of Dar es Salaam, 2007, p. 1.
[xiii] Tromp, Joshua, "Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-attacks" (See https://smallwarsjournal.com/jrnl/art/law-of-armed-conflict-attribution-and-the-challenges-of-deterring-cyber-attacks accessed on 16th October, 2019).
[xiv] See the United States Department of Defense (DoD), The National Military Strategy for Cyberspace Operations, December 2006, 3 (accessed at www.dod.gov/pubs/foi/ojcs/ 07-F-2105doc1.pdf on 16 October, 2019).

[xv] Armed Forces of the United States, Doctrine for the Armed Forces of the United States, Joint Publication Roscini, World Wide Warfare −Jus ad bellum and the Use of Cyber Force.
[xvi] E, Wilmshurst (Ed.), *International Law and the Classification of Conflicts*, (Oxford: Oxford University Press, 2012), at. 458.
[xvii]Trompt, J., "Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-attacks." *Small War Journal*, https://smallwarsjournal.com/jrnl/art/law-of-armed-conflict-attribution-and-the-challenges-of-deterring-cyber-attacks (accessed on 15 October, 2019).
[xviii] See the Report on Guardian, https://www.theguardian.com/society/2020/oct/28/us-healthcare-system-cyber-attacks-fbi (accessed on 15 October, 2019).

[xix] *Ibid.*
[xx] *Ibid.*
[xxi]*Ibid.*
[xxii]The Centre for Strategic & International Studies "Significant Cyber Incidents," https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed on 13 October, 2019).
[xxiii] Russia's military intelligence service is commonly known by the Russian acronym GRU, which stands for the Main Intelligence Directorate. Its name was formally changed in 2010 to the Main Directorate (or just GU) of the general staff, but its old acronym - GRU - is still more widely used. (See https://www.reuters.com/article/us-britain-russia-gru-factbox-idUSKCN1MF1VK (accessed on September 11, 2020).

[xxiv]*Ibid.*
[xxv]A. Mwiburi, *Preventing and Combatting Cybercrime in East Africa*, (Berlin: Duncker &Hamblot, 2019), at. 15.
[xxvi] E. Wilmshurst, *op.cit.* at 458.
[xxvii] Claire de Than & Shorts, E. *International Criminal Law and Human Rights, (*Sweet &Maxwel: London, 2003), at13.
[xxviii] A. J. Bwana, "Electronic Banking and Law in Tanzania: Approaches to its Regulation", *Tanzania Lawyer*, 2003
[xxix] *Ibid.*
[xxx] Article 25 of the Convention provides that "each State Party to the convention shall adopt such legislative and/or measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity availability and survival of information and communication technology system, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders. State Parties shall take into consideration the choice of language that is used in international best practices.
[xxxi] Part IV of the Act contains provisions in relation to search and seizure. See ss 31-38.
[xxxii] Part II of the Act contains 25 provisions on various offences and penalties – ss 4-5 illegal access, remaining and interception; s 7 – illegal data interference; ss 8-12 data espionage, illegal system interference, illegal device, computer-related forgery and computer-related fraud; s. 13 – computer pornography; s. 14 – pornography; s. 15 – indentity crimes; s. 16 – publication of false information; ss 17 – 19 – racist and xenophobic material, racist and xenophobic motivated insult, and genocide and crimes against humanity; s. 20 – unsolicited messages; ss 20-21 – disclosure of details of investigation and obstruction of investigation; s. 23 – cyberbullying; s. 24 – violation of intellectual property rights.
[xxxiii] Cyber Crime Act No 14 of 2015.
[xxxiv] Reg. 4 (1) provides that "A person shall not provide online content services without obtaining a licence from the Authority."
[xxxv] Regulation 4 (2) provides that "A person who contravenes the provisions of sub-regulation (1) commits an offence and shall, upon conviction, be liable to a fine of not less than five million shillings or to imprisonment for a term of twelve months or to both."
[xxxvi] See the Third Schedule of the Regulations.
[xxxvii] Sub regulation 3 defines online as: "…a networked environment available via online whereby content is accessible to or by the public whether for a fee or otherwise and which is intended for consumption in or originated from Tanzania."

[xxxviii] In respect to false, untrue, misleading content, the regulation require a person to state that the content is a satire, parody or fiction; and where it should be preceded by a statement that the content is not factual.
[xxxix] See also Pavan Duggal, *op.cit.*, at 15.
[xl] This is the trend that Tanzania has decided to take. India also amended the India Information Technology Act to introduce section 66 A to make it illegal for anyone to transmit false information over the internet. However, the Supreme Court in *Shreya Singhal v. Union of India* (2013) 12 SCC 73 invalidated section 66A of ITA in its entirety as it violated the right to freedom of expression guaranteed under Article 19(1)(a) of the Constitution of India.
[xli] (2013) 12 SCC 73.
[xlii] D. Halder, "A Retrospective Analysis of Section 66 A: Could Section 66 a of the Information Technology Act Be Reconsidered for Regulating 'Bad Talk' in the Internet?" Source: https://www.semanticscholar.org/paper/A-Retrospective-Analysis-of-Section-66-A%3A-Could-66-Halder/52ffdabd6816444590f261ae1cea7a228028f6e7 (accessed on November 17, 2020).

[xliii] Cybercrimes of a number of countries examined vary on what content should be prohibited and what should be allowed. In America for example, the use of internet remains an open platform where anybody can just post anything. This is not the case in other countries like China as well as Arab and African countries.
[xliv] Duggal Pavan, *Textbook on Cyber Law*, 2Ed., (New Delhi: Universal Law Publishing, 2016), at 13.
[xlv] *Loc.cit.*
[xlvi] See Amnesty International, "Universal Jurisdiction: Strengthening this Essential Tool of International Justice" https://www.amnesty.org/download/Documents/24000/ior530202012en.pdf (accessed on 13 October, 2019).
[xlvii] See "General Assembly, Sixth Committee, Sixty-ninth session, 11th & 12th Meetings (AM & PM)" https://www.un.org/press/en/2014/gal3481.doc.htm (accessed on 10 October, 2019).
[xlviii] Congressional Research Service, "Cyberwarfare and Cyberterrorism: In Brief" https://fas.org/sgp/crs/natsec/R43955.pdf (accessed on 14 October, 2019).
[xlix] Prasad, K.," Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework" accessed at https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act (accessed on 20 October, 2019).
[l] See http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/SUA-Treaties.aspx (accessed on 20 October, 2019).
[li]Adam J, Mambi, ICT *Law Book: A Source Book for Information and Communication Technologies*, (Dar es Salaam: Mkuki and Nyota), p. 181.

[lii] E. Wilmshurst, *op.cit.*, p. 459.
[liii] *Ibid.*

[liv]Jus (or ius) ad bellum is the title given to the branch of law that defines the legitimate reasons a state may engage in war and focuses on certain criteria that render a war just.... Jus in bello, by contrast, is the set of laws that come into effect once a war has begun.

[lv] L. May, & Newoton, M., *Proportionality in International Law*, London: Oxford University Press, 2014), p. 261.
[lvi]*Loc.cit.*
[lvii]Jay P. Kesan* and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace" *Harvard Journal of Law & Technology*, Volume 25, Number 2 Spring 2012, http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech429.pdf (accessed on 21 October, 2019).

[lviii] Roscini, M., "World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force,*" Max Planck Yearbook of United Nation's Law,* Volume 14, 2015, p. 85-130, at p. 125
[lix] *Ibid.*
[lx] *Ibid.*
[lxi] See United States National Strategy to Secure Cyber-space document of February, 2003. See www.hsdl.org (accessed on 9th November, 2020).

[lxii] *Ibid.*

[lxiii] Jensen, T. E., "The Tallinn Manual 2.0: Highlights and Insights" https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf (accessed on 9th November, 2020).

[lxiv] *Ibid.*

[lxv] Karma Nabulsi, "Jus ad Bellum / Jus in Bello, CRIMES OF WAR", http://www.crimesofwar.org/a-z-guide/jus-ad-bellum-jus-in-bello/ (accessed on October 11, 2019).
[lxvi] ITU, "UNDERSTANDING CYBERCRIME: P H E N O M E N A , C H A L L E N G E S AND LEGAL RESPONSE", http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (accessed on October 22, 2019).
[lxvii]Robert Manumba, "Brief Remarks by the Director of Criminal Investigation", The Occasion of the Launching of a Cyber crime Training Programme Sponsored by the Government of India on 13th July 2010 Kempiski Hotel Dar es Salaam
[lxviii] Anna-Maria Osula and Henry Rõigas (Eds.), "International Cyber Norms Legal, Policy & Industry Perspectives", https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf (accessed on October 22, 2019).