A HUMAN RIGHTS APPROACH TO CYBER CONFLICT*

Abstract
In recent years, it has become apparent that conflict in cyberspace, attacks on cyber users has remained unabated. Conflicts in cyberspace refer to actions taken by parties to a conflict to gain advantage over their adversaries in cyberspace by using various technological tools and people-based techniques. Thus, conflict in cyberspace is different from conflict in physical space in many dimensions, and however, attributing hostile cyber operations to a responsible party can be difficult. This paper focuses on the importance of a human right approach to addressing these challenges, relying on the highest attainable standard of cyber operation as well as to civil and political rights. This paper also observed that the problems of defending against and deterring hostile cyber operations have remained intellectually unresolved. This paper in particular examines the United Nation Charter and the Geneva Convention that are relevant to cyber operations as a normative framework. Thus, it is noted that the relevance of the above conventions is today unclear since cyberspace is a new phenomenon compared to these conventions.

Keywords: *Human Rights, Cyber, Conflict, Approach, Cyber space*

1. Introduction

In this twenty-first century, it has become apparent that a new range of sophisticated methods is being developed. Deploying cyber techniques to attack vulnerabilities in communications and navigation system has become alarming. Thus, this paper shall examine the nature of conflict in cyberspace, the tools and techniques of such conflict, the offensive operations in cyberspace, the actors that might use these tools and techniques, and the reason why they might do so. However, since cyber-related technology is relatively new and is often multi-purpose and dual-use in nature, legislation lags behind. In addition, the limited states department of defence defines cyberspace as 'a domain characterized by the use of electronics and electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructure'.[1] This paper rightly observed that cyberspace and cyber security points to the increasingly blurred line between 'offensive' and 'defensive' activities in cyber and space, given that technologically, offence is easier and cost-effective than defence.[2] Also, the paper noted that more advanced countries are increasingly vulnerable to attack from less developed states, and from terrorist groups and other actors such as organized criminals. This paper however, warns that the conjunction of cyber and space remains vulnerable to exploitation in the context of complex and internationalized supply chains and space-related infrastructure.

In the light of the above, the most important point of this paper is that it seeks to identify human rights approach and important questions associated with conflict in cyberspace, especially with respect to the International legal regime that governs such conflict. Indeed, this paper submits that the need to develop new knowledge and insight into the technical and legal instruments to support informed policy making in his area will provide analysts. This systematic challenge at the intersection of cyber and space security therefore requires a radical, innovative approach to build and maintain confidence in the use of the space domain. Human rights law applies all of these contexts. Its applicability to interference with cyberspace or other situations of cyber operations, however, has not been sufficiently explored. For instance, what is the extent of protection afforded to cyber operators, facilities in situation cyber-attacks? Thus, in cyber-attacks, do states have responsibilities to ensure adequate protection of facilities and cyber operators beyond those required by human rights law? This paper examines how human rights law can address these questions. Notably, human rights instruments are formulated in more general terms. Civil and political rights are the foundation of protection against attack, violence, discrimination and denial of rights.[3]

2. Understanding Conflicts in Cyberspace

Conflict in cyberspace implies when parties to a conflict seek to gain advantage over their adversaries, by using various tools and techniques for exploiting certain aspects of cyberspace.[4] More so, the tools and techniques of conflict in cyberspace can be separated into tools based on technology and techniques that focus on the human being. On the other hand, this paper noted that an offensive activity in cyberspace is seen as cyber-attack which

***Jorge C. NKWOH, PhD,** Senior Lecturer, Faculty of Law, Imo State University; and
***Augustus Uche NNAWULEZI, PhD**, Lecturer, Criminology and Security Studies, Alex Ekwueme Federal University Ndufu Alike, Ikwo.

[1] See the United States Department of Defense National Military Strategy for Cyberspace Operations, 2006
[2] See Baylon, *Challenges at the Intersection of Cybersecurity and Space Security*, 2014.
[3] See the Universal Declaration of Human Rights
[4] This definition implies that armed conflict' or 'military conflict' are subsets and only subsets of the broader term 'conflict', which may entail a conflict over economic, cultural, diplomatic, and other interests as well as conflict involving military matters or the use of arms.

refers to the use of deliberate activities to alter, disrupt, deceive, degrade or destroy computer systems or networks used by an adversary or the information and/or programs resident in or transiting through these systems or networks. In cyber conflict, the offence is inherently superior to the defence, in part because the offence needs to be successful only once, whereas the defense needs to succeed every time and in part because there is no way to guarantee that harmful, incorrect or flawed information inputs will not be entered in to an information technology based system. It is important to note that this paper is not intended comprehensively or conclusively cover all issues surrounding human rights in cyberspace but contribute to the ongoing debate on human rights approach to cyber conflicts. Various human rights instrument and/or commissions have relentlessly continued to work on a range of human rights issues connected with the internet. Indeed, understanding the issue of human rights and cyberspace three issues are raised in this paper for consideration such as Rights to access the internet, Freedom of expression and internet censorship and Effective responses to sexual harassment and homophobia on the internet.

3. The Philosophy of Human Rights to Cyber Conflict

The philosophy of human rights attempts to examine the underlying basis of the concept of human rights and critically looks at its content and justification. In light of the above explanation, this paper will therefore consider the definition of the term 'cyber conflict' as 'any use of information and communication technologies that may have disruptive or destructive consequences'. Furthermore, cyber conflicts are the umbrella phenomena encompassing several instances ranging from cyber warfare and hacktivism to cybercrime and cyber terrorism. Now to the nature of human rights law, the first thing that is noticed when examining human rights treaties is that they are arranged in a series of assertions, each assertions setting forth a right that all individuals have by virtue of the fact that they are human. Thus, the law concentrates on the value of the persons themselves, who have the right to expect the benefit of certain freedoms and forms of protection. Also, it has been observed that there are a number of theories that have been used as a basis for human rights law, including those stemming from religion, the law of nature which is permanent and which should be respected, positivist utilitarianism and socialist movement.[5] Also under human rights law, the other important factor to be taken into account in the development of human rights is the existence of various cultural traditions and advocates for social development. This paper noted that as the development of human rights progressed from theories of social organization to law, lawyers began to analyze the nature of those rights from the legal theory point of view. These however, gave rise to several arguments on whether human rights are really legal rights if the beneficiary cannot insist on their implementation in court.[6] Thus, the basis for this argument is centered on the nature of economic and social rights which many legal theorists argue cannot therefore be described as legal rights.

With regard to the first major international instrument defining human rights that is the 1948 Universal Declaration on Human Rights, this paper noted that it contains not only civil and political, but also economic and social rights. In addition, a further development of importance in the philosophy underlying human rights law is the appearance of what is commonly referred to as 'third generation rights'.[7] There is strong contention on whether human rights law can be applied at all times, thus, in cyber conflict as well, given that the philosophical basis of human rights is that by virtue of the fact that people are human, they always possess them. They submit that they are applicable. Also in the same vein, the difficulty as regards human rights treaties is that most of them allow parties to derogate from most provisions in times of conflict, with the exception of what are commonly termed 'hard-core' rights, i.e. those which all such treaties list as being non-derogable such as the right to life, the prohibition of torture and other human treatment and the prohibition of retroactive criminal legislation or punishment. However, the other rights do not thereby cease to be applicable, but must be respected in so far as this is possible in the circumstances. In highlighting the links between human rights norms and cyber conflict situations, the focus of this paper will be on the obligations of states. However, the increasing recognition of cyber criminals as violations of human rights represent an important shift in discourse, and expands the scope of human rights protection to include cyber conflicts, especially when considering other features of a rights-based approach such as monitoring and accountability. It should be noted that accountability and enforcement mechanisms are more advanced under human rights law in terms of formal compliance reviews, rights to individual remedy, reparation and the obligation to investigate.[8]

[5] B. Shestack, 'The Jurisprudence of Human Rights' in T. Meron, ed; *Human Rights in International Law*, Oxford University Press, London 1984, volume 1, p. 69.
[6] M. Cranston, *What are Human Rights?* 1973
[7] K. Drzewicki 'The Rights of Solidarity – the Third Revolution of Human Rights', 53 *Nordisk* 1984, p. 26
[8] C. Droege, 'The Interplay between international human rights law and international humanitarian law in situations of armed conflict' in *Israel Law Review*, vol. 40, NO. 2 2007 p-340

4. Cyber Warfare and the Law of Armed Conflict: A Conceptual Clarification

It is worth stating that the legal tools applicable to the changing environ have often been created before modern advancements in the methods and means of warfare. Public international law as a whole is struggling to come to grips with cyber-attacks as this phenomenon presents complex questions.[9] Again, cyber-attacks or computer network attacks are according to the United States define as 'actions taken through the use of through the use of computer networks to disrupt, deny, degrade of destroy information resident in computers and computer networks, or the computers and the networks themselves'.[10] From the above definition, it follows that cyber-attacks have turned the attention of the law of armed conflicts to a set of pressing questions which are fundamental to the law. Thus, these questions are as follows: Are there concrete and precise restrictions regarding the employment of cyber-attacks? Can law of armed conflicts be a body of law mostly regulating international conflicts and conventional weapons provide workable solutions? Can cyber-attacks be regarded as a means of warfare? Are cyber-attacks in compliance with requirements of neutrality? This paper however, will try to examine the above questions and provide answers to the questions posed above and argue that the current body of law of armed conflicts applies to cyber-attacks by way of fundamental principles or norms and that the law is capable of providing guidance to operators and practitioners in the conduct of military operations. It is pertinent to note that the law of neutrality under law of armed conflict should be the main obstacle impeding the conduct of either offensive or defensive cyber-attacks. However, the obvious fact remains that some of the body of law regulating the law of neutrality is contained in the 1907 Hague convention V, which predates the existence of internet and cyber weaponry by more than half a century. Regrettably, the architecture of internet does not facilitate neutrality. In juxtaposing cyber-attacks with the concept of law of armed conflicts, this paper noted that law of armed conflicts prescribes an obligation to evaluate the new weapons to determine whether the employment of new weapons would under some or all conditions, be prohibited or restricted under the standards of humanitarian or some category of international law.[11]

5. Human Rights Implications and Potential Exploits

The role of Human rights from a command, control and communications perspective is to restrain governmental action with respect to individuals under the government jurisdiction. Cyber operators or users are protected from violence by Article 6 of the International Covenant on Civil and Political Rights (ICCR), under which states have a non-derogable obligation not to subject any individuals under their jurisdiction or control to arbitrary deprivation. Furthermore, the paper noted that such rights may as well emanate from the country of the individual such as the rights granted to citizens of America under their constitution or that seen in international treaties, or in customary international law. This paper however, does not claim that emerging technologies are the primary risk to consider in cyber warfare, or that risks of cyber-attack are new, rather, the paper argues that while key risks areas have existed for a long time, new technology in cyber warfare has exacerbated these risks. Thus, with the potential for such catastrophic consequences from cyber-attack, it is crucial to have the most robust human rights policies in place. Also, given that a number of human rights instruments have addressed the protection of cyber operators from cyber-attacks, two of the rights enumerated in the International covenant on Civil and Political Rights ratified by the United States ratified by the United States in September 1992 may be relevant. The cyber domain of note herein is that the issue of protecting privacy and reputation might be relevant to cyber operations intended to harm the reputation of an individual[12] or protecting rights to seek information which may be relevant to cyber-attacks intended to prevent individuals from obtaining service from the internet or other media.[13]In addition, a number of other rights, such as the rights to life, to health, and to food, may be relevant as well depending on the nature and targets of the cyber-attack. Thus, the respect for the aforesaid rights may suggest that cyber-attack intended to enforce economic sanctions. Interestingly, it might seem that no country would be willing to face the consequences of starting a cyber-offensive campaign in the cyber warfare; however, what is paramount to human rights in this regard is the extent of its applicability during acknowledged armed conflicts r hostilities. Thus, human rights law should not place additional constraints on the actions of its armed forces to avoid this outcome, a number of international bodies such as the international court of justice[14] and the Human Rights Committee,[15] have submitted that human rights law can and should be applicable as well as law of Armed Conflict during hostilities. It is generally assumed that achieving respect, protection and fulfillment of the right to cyber operation in armed conflict and other situations of violence may amount to a colossal challenge, but as the international Court of

[9] E. Kodar, 'Computer network Attacks in the Grey Areas of Jus ad Bellum and Jus in Bello', *Baltic Yearbook of International Law*, vol. 9, 2009.
[10] See Department of Defence Dictionary of Military and Associated Terms Joint Publication 1-02, 2001
[11] See Article 36 Additional Protocol 1
[12] See Article 17 of the International covenant on Civil and Political Rights 1992.
[13] Article 19 of the International Covenant
[14] See International court of Justice, on legality of the threat or use of Nuclear Weapons, Advisory Opinion, 8 July, 1996
[15] See United Nations Human Rights Committee, General Comment No. 31 2004 para 11

justice has expressly affirmed, economic, social and cultural rights obligations remain in force in armed conflict. In this case, states are under an obligation to provide a powerful framework for assessing to what extent human rights are reflected in state's norms, institutions, legal frameworks and political and policy environments.

6. Protection and Termination of Conflicts in Cyberspace

The paper noted that in order to reduce the vulnerability in the supply chain the emerging conflicts in cyber operations, a holistic approach is needed, which will takes into account the possible risks system architecture. Thus, this paper however suggests that by identifying the party that should be held responsible for the offensive cyber operation, it will help to protect the rights of the cyber operator. Also it has been observed that conflict does occur in cyberspace and its termination has remained a great challenge. But however, the fact remains that the question of how to respond to hostile actions in cyberspace that has not risen to these thresholds is the most pressing concern of policy makers today as almost all hostile cyber operations conducted to date have not risen to these thresholds.[16] As noted above, conflict termination in cyberspace in really a big task faced by decision-makers on when to cease hostilities. Under the duty to protect, the international court of Justice has set a high threshold for attribution of conduct to a state in the context of the right to self-defence. Thus, the court held that 'the burden of proof rests on the state invoking the right of self-defence'.[17] In this case, a state is responsible for the conduct of a person or group of person in fact acting on the instructions of, or under the direction or control of that state in carrying out the conduct.[18] In the same vein, the commentary on the Articles on state responsibility requires that the state direct or control the specific operation and that the conduct must be an integral parts of that operation.[19] Clearly, numerous issues need to be addressed as the international criminal tribunal for former Yugoslavia (ICTY) has argued that where a group such as an armed opposition group is organized, it is enough that the state authoritative exercise overall control over such an organized and structured group without a need for specific control or direction over individual conduct.[20]

7. Nature of Cyber Threats and Risks

The concept of cyber conflict relating to the nature of the cyber threats and risks has been the subject of several philosophical thoughts and beliefs, both locally and internationally. Cyber security threats and risks has been viewed as a systematic challenge to modern society. Communications as well as the transfer and storage of data are key targets for cyber-attacks. Notwithstanding this statement, this paper rightly observed that there are several areas within nuclear weapons systems[21] that could be potentially vulnerable to cyber-attacks,[22] such as Robotic autonomous systems within the strategic infrastructure, communications between command and control centers, cyber technologies in transport and several other areas. But it is worthy of note that these areas are subject to exploitation by groups or individuals with malicious intent. This paper however submits that a system-level response is therefore the only viable approach, enabling the full set of agencies and organizations to work together in a synergistic and complementary manner. In the same vein, it should be pointed out that in risk analysis, as the attack surface, the number of vulnerabilities in a system or network increases while cyber-security measures lapses, then malicious cyber-attacks are likely to become non-frequent. The paper however suggest that what is required in the circumstance is a mutually agreed framework within which strategic and operational approaches can be networked so as to cross-fertilize information and foster an innovative, self-governing and accountable culture.

It is worth reiterating that in the cyber realm, it is possible for instance, that states might treat computer networking attacks on their military infrastructure differently from those affecting civilian systems. From the foregoing analysis, it is apparent that although this might not be entirely technically logical because use of force is use of force, whether directed at the civilian or a military object. But the threshold of harm that states are willing to tolerate might be lower when it comes to operations that are targeted at and degrade their military capability. Although states currently possess the necessary capabilities and know-how to conduct attacks on advanced strategic assets and industrial control systems, the higher degree of cooperation between hackers and organized crime groups has been identified as a growing concern.[23] The foregoing, however suggests that as technology changes rapidly,

[16] H.Lin, 'Responding to sub-threshold cyber intrusion: a fertile topic for research and discussion in Georgetown Journal of International Affairs, Special Issue, International Engagement on Cyber: Establishing International Norms and Improved cyber security, 2011, pp. 127-135.
[17] See ICJ, Oil platforms case *Islamic Republic of Iran v. United States of America*, Judgment of 6 November 2003 para 57.
[18] Article 8 of the State Responsibility
[19] See United Nations Document A/56/10. Commentary on Article 8 of the Draft Articles on State Responsibility, Para 3.
[20] See ICTY, Prosecutor Y. usko Tadic, IT-94-1, Appeals Chamber Judgment 1999, Para 120
[21] See Unaland Lewis, *Cyber Threats and Nuclear Weapons Systems*, 2017
[22] Ibid
[23] M. Glenny, 'Organized Crime finally embraces cyber theft', *Financial Times*, 7 March, 2017. http://www.crime.research.org/library/cybercrime.htm accessed 8 February, 2019

jamming, spoofing and cyber-attacks are almost impossible to prevent or defend against completely, although there is a growing recognition of the problem, hence, many national space security policies.[24] Even those in countries where cyber security is more advanced have been slow to identify the significant risk to space-based assets. Moreover, very little is as yet being done to address cyber security at a system-of-systems level.[25] One point appears outstanding from the foregoing analysis, namely, that lack of consistency in the internationalized domain addressing threat-response vulnerabilities has resulted in a failure to examine the range of risks. But the evidence suggests that imagining the risk to be small could be fatal blunder.[26] Despite this constant threat, it now seems that, details of the attacks, whether successful or not are scarce in the public domain in line with a wider culture of secrecy pervading the private sector in cyber security. The paper noted among other things that the reason why this attitude is prevalent is the pace at which technology evolves which makes it hard or even impossible to device a timely response to such cyber threats as rightly pointed out in this paper.

8. Challenges of Combating Cyber Threat

The Cyber industry in Nigeria and even the whole world particularly developing or third world countries has been at the receiving end of cyber-attacks. Also, as technology continues to evolve so also do the opportunities and challenges expand. Although there are laws enacted for the purpose of tackling these challenges, its enforcement is still faced with challenges. Thus, some of the notable challenges of tackling the problem of cyber-threat include: the problem of jurisdiction, anonymity, the nature of the evidence, the issue of locating and securing relevant material in the investigation and prosecuting of cyber offences. Having seen above some of the notable challenges, would it be correct to say that the problem with invoking the ordinary meaning of jurisdiction for purposes of prosecuting cyber offences is tricky mainly because determining where a cyber-offence was committed is difficult since the offender and the victim may be in different nations? If this is a possibility, it therefore becomes logical to call for improvements in the traditional court litigation system. More so, the issue of anonymity is a visible challenge in detecting and prosecuting cyber offenders as law enforcement operatives have been faced with the challenges of profiling and locating criminals as noted by the United Nations.[27] Also on the question of the nature of evidence, it is submitted here that the nature of evidence that will be material to the offence of cybercrime is fundamental, thus, digital evidence.[28] This proposition notwithstanding in some jurisdictions, has been adopted as creating enforceable cyber security right. It must be stated that in Saudi Arabian Courts, digital evidence is now accepted as a trusted source of evidence. The supreme court of Saudi, for instance held that Digital Forensic Evidence is enough to prosecute as major evidence.

9. Conclusions and Recommendations

Human Rights Law has remained a critically important set of rules through which to address obligations with respect to cyber offences either in armed conflict or internal violence. Conflict can and does occur in cyberspace. Although cyber security is a technical issue, technology alone cannot provide the basis for driving policy. There is also the need to foster bilateral and multilateral cooperation to facilitate exchange of ideas and the transfer of environmentally sound cybercrime laws that will be complementary with the existing human rights law adaptable to local needs. Also one of the greatest contributions of human rights is its role in ensuring that the interests and needs of the cyber operators and vulnerable are addressed. Thus, the essential elements of a human rights approach to cyber conflict include principles of non-discrimination and equality, coupled with entitlements to adequate security and protection. Indeed, this is a strong framework through which various cyber offences can be addressed. To develop the required and sound human rights framework capable of addressing cyber conflicts, this paper has developed full set of requirements as follows: There is need to raise awareness of the existing laws. In this case, awareness of the existing laws will help to reduce the rate of cybercrime. Publication of reports and cases on cyber offences is necessary. Through the publication of reports and cases on cybercrime, the public will be aware of the nature of attack. Updating of the existing laws to reflect new cybercrimes with their related specific details and different scenarios will be commendable. There is equally need for establishment of forensic laboratories and compliance with cyber security best practices. There should be developed and maintained a risk matrix by matching vulnerabilities to threats that will not be commercially compelling to resolve, and ensure that regulators are aware. Experts should be trained on how to notice unusual activity and how to verify suspicious and then alert the community. Finally, mechanisms for analysis and sharing of sensitive information should be instituted.

---

[24] See United Kingdom Space Agency on National Space Policy 2015, p.11

[25] C, Clark, 'Cyber Attack on Satellite could be Act of War: HPSCI Ranking', *Breaking Defence*, 10 June 2016, http://breaking defence.com/2016/06/Cyber-attack-on-satellite-could-be-act-of-war-hpsci-ranking accessed 8 February, 2019.

[26] C, Baylon, R. Brunt and D. Livingstone , *Cyber security at Civil Nuclear Facilities: Understanding the Risks,* Chatham House Report, London: Royal Institute of International Affairs, 2015.

[27] See R. Bryant, *Policing Digital Crime*, Routledge, New York United States of America, 2016, pp.111-123

[28] See the *Black's Law Dictionary* 9th Edition, p.635