PalArch's Journal of Archaeology of Egypt / Egyptology

THE STATE RESPONSIBILITY FOR THE ACTIONS OF NON STATE ACTORS IN CYBER SPACE BASED OPERATIONS

Mian Muhammad Sheraz

Mian M Sheraz is a Ph.D Law candidate in Department of law, International Islamic University, Islamabad, Pakistan and currently working as a Vice principal Mardan Law College, affiliated University of Peshawar.

Mian Muhammad Sheraz , The State Responsibility For The Actions Of Non State Actors In Cyber Space Based Operations , Palarch's Journal Of Archaeology Of Egypt/Egyptology 18(10), 1229-1238. ISSN 1567-214x.

KEY WORDS: State responsibility, cyberspace, cyber attacks, cyber operations.

ABSTRACT

At a time during which the unbridled sovereign authority of states is being challenged across several domains, state responsibility continues to be a cardinal rampart of international security. But creating a workable regime to outline state responsibility in international law has proved to be equivocal. The cases of state sponsored terrorist acts have exaggerated since the end of the cold war, however, proving State responsibility for such acts continues to be extremely tough.

This drawback is increased in cyberspace by the speed and obscurity of cyber attacks, making in line with the White House "distinguishing among the actions of terrorists, criminals, and nation states is troublesome". As the world had seen in the 2007 cyber attack on Baltic State, a possible sponsoring state might not collaborate in the probe, apprehension, and surrender of those who committed criminal or terrorist acts on its behalf. Given the covert nature of cyberspace, states could, therefore, motivate civilian groups within their territorial borders to perpetrate cyber attacks then hide behind a veil of arguable deniability and therefore escape obligation. This paper analyses the concept of state responsibility along with the effective and over all control standards in cyber operations.

INTRODUCTION

With the significant number and sophistication of the cyber attacks against the States show a subsequent increment in the recent times for discussing about the international law problems, associated to the state responsibilities in cyber operations.[1] As per the International law (IL), a state incurs the major responsibility when an omission or act is being attributed to the State for constituting a major breach in the obligations of IL.

The major attribution is regarding the assignment of an act to the state and it establishes a relation within the respective state and the act. Three significant and noteworthy characteristics of the domain are responsible for making this attribution quite difficult and there could be major chance of attribution becoming difficult. The first and the foremost characteristic of this domain is anonymity, where the respective authors of the cyber operations could easily hide their identities.[2] The second important and significant characteristic of this domain is the subsequent possibility of the multi stage activities, in which the computer systems are being operated by separate persons and are also placed in various jurisdictions for further utilization. The final significant and noteworthy characteristic of this domain is the speed, by which the operations could occur.

For the technical aspect of attribution, different jurisdictions concern the forensic recognition of the source of the cyber activity. In spite of the fact that technical attribution could easily yield good results after tracing back the computer systems, it could never be exact and could not recognize the individual, which had operated the respective computer system and affiliation.[3]

For understanding the respective legal aspects of attribution, the law of state responsibility is being presented for assessing the relevance whenever applied to the cyber domain. A model of responsibility on the basis of the obligation is required to be considered for causation and due diligence.As per the international law criteria about attribution, there exist three major tests on attribution within the law of state responsibility, which includes an institutional test, a control based test and finally a functional test.[4] The institutional test declares that the acts of different state organs are being attributed to the Referent state. However, it is not always clear that what degree of control is required with the state for mentioning the effective and general control as well as it becomes easier to equate the entities and persons with different state organs, when they do not comprise of the status under internal laws.

The second test is for the functional test, which is an act that is being attributed to a state for exercising the governmental authorities or when it is being committed by the organ of any other state that is being placed at the removal of the first state.[5] The final test is the control test, which is an activity that is attributed to the state when it is being committed by a specific group or individual, directed under the control of a state. Different standards of instructions would eventually attribute to a state for understanding a cyber activity that is being committed by the persons, prompted by any particular state organ.

The respective instructions eventually establish a proper relationship within the state and the author of the act and these instructions are proven in relation to any specified activity. As the law of state responsibility concerns about states, different standards of attribution could easily determine the variety of public and state acts to be held responsible.[6]

Hence, the acts of the private actor are being attributed to a state, when the actions get subordinated by the state. One of the vital issues that is required to be taken into consideration for this state of responsibility is for the cyber context. The subsequent application of the state of responsibility to the cyber operations could eventually leads to the reversal of burden and attack in the state. As a result, it can be stated that the state of responsibility is extremely important and significant for the cyber operations.

The Fundamental Issue of Attribution and the Case for the Overall Control Standard

The epochal issue of attribution within cyber operations is extremely significant to be eradicated on time for ensuring error free operations and warfare. This cyber attribution is the procedure to track, recognize as well as lay blame on the perpetrator of any cyber attack or any other hacking exploit.[7]hese cyber attacks could have major consequences for the entire country, regarding the public relations, finances, reputation and compliance. The respective country could easily conduct subsequent investigations for attributing the cyber attack incident towards certain threat actors for obtaining the entire access to the attack and also helping to ensure that the attackers are brought into justice. The respective efforts of cyber attribution are being conducted in the conjunction with official investigation conducted by the law enforcement agencies.[8]

The entire aspect of attribution of cyber operations could be quite difficult, as the underlying architecture of the internet subsequently offers several methods for the attackers in hiding their tracks. One of the major challenges for cyber attribution is that the attackers do not carry out the attacks from their own places of warfare, however launch cyber attacks with the help of devices or computer systems that are owned by any other victim, which is being previously compromised by the attacker. Proper identification of an attacker is made more difficult since the attackers could easily spoof their own IP addresses as well as utilize the other techniques like proxy servers for the purpose of bouncing the distinct IP addresses for confusing different attempts of cyber operation.[9]

The jurisdictional restrictions could eventually hinder such attribution in the cross border cyber activities or cyber crime investigation, since a law enforcement agency has to undertake an investigation, which could cross the border for requesting help.

The inherent nature of the cyber space has eventually created a major opportunities for distinct adversaries, for involving exploitation of vulnerabilities of the cyber infrastructures of the victim state anonymously for a series of reasons. The state and non state actors could easily utilize multiple avenues as well as techniques for routing malware with better safety and ease.

These states could even use the non state actors in the efforts for achieving political objectives with the core capability of denying involvement within the act. The main reason for such denying of involvement is due to the deficiencies within the International law as well as issue of attribution.[10] A multi dimensional approach is required to be followed for attribution to ensure that the responsibilities for malicious cyber acts and providing the victim States the confidence to respond properly.

Due to the cyber space nature, the attribution is referred to as the action of about any issue that is being caused by a thing or person. The Geneva and Hague Conventions comprise of four treaties as well as three additional protocols, which eventually create the different standards of IL within war.

This particular convention helps in defining the basic rights of wartime prisoners like military and civilian personnel, after understanding the most significant rights and protections that are being afforded to the non combatants for not addressing the warfare or utilization of weapons in the war. One of the most significant assumptions related to the attribution of cyber operations is required for modifying the negativity of the capability of the actors for acting anonymously.[11]

The science of tracing cyber attacks is primitive at the best, refined attacks with the aid of by knowledgeable hackers, whether or not private or State sponsored, nearly not possible to trace to their origin using contemporary practices.[12] Can the cyber infrastructure be modernised to reinforce security and stop cyber attacks once and for all? The short answer is in affirmative, however not simply. Certain ways and strategies pioneered by the U.S. Cyber Emergency Response Team (CERT) are promising, like the employment of probabilistic trace back techniques to audit a little percentage of packets therefore on realize the supply of major distributed denial-of-service (DDoS) attacks of the sort that Baltic State (Estonia) suffered in 2007.[13] here is additionally the likelihood of tracing back single IP packets, although this is often way more troublesome.[14] The cyber warfare as a weaponry race that can't be won by defense alone. In the end, these attacks can seemingly still proliferate each in numbers and severity; the question then is how best they must be proscribed in law and relations.

Attribution of a cyber attack to a state could be a key part in building a functioning legal regime to mitigate these attacks. The laws of war demands one state to determine and identify itself once it is offensive against another state, although this convention is honoured more in the breach than in compliance.[15] When there's an issue concerning State support of aggression, two competitive standards for state responsibility currently exist in international law under Article VIII of the International Law Commission's (ILC) Draft Articles on the Responsibility of States for International Wrongful Acts. Article VIII entails state control when state actors or governmental organs are acting under the direction of the state.[16]

An verbatim definition of “control” Nevertheless, has been left up to the courts to explicate. The initial standard that the courts have declared is the ICJ Nicaragua“effectiveoperationalcontrol” standard,[17]Nicaragua requires that a country's control over paramilitaries or other non-state actors can only be set up if the actors in questions act in “complete dependence” on the State. The second standard is the ICTY Tadic “overall control” standard. The ICTY held that “where a state has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient overall control, and the group's acts are attributable to the state”.[18] In this finding, the bulk understood the decision of the ICJ in Nicaragua as necessitate the State to exercise “effective” control over the operations of a military force in order for the acts of that force to be attributed to the state.[19]

The Effective Control Standard

Because of the divergence of opinion on the issue of state responsibility, in international law, there are two competitory standards emerging for cyber attacks, the “effective control standard” relevant to non-state actors, and both the “effective” and “overall control standards” pertinent to state sponsors of cyber attacks. For non-state actors, the ICJ adjudged in Nicaragua case that “effective control” was the suitable standard to employ at least in the paramilitary circumstance of that case.[20] If this judgement were to be protracted and extended to the cyber militia, it might mean that the sole instance during which State sponsors of cyber attacks would be held responsible for their engagement would be if their effective control may be proven or evidenced indisputably. Given what has been validated about the intense technical difficulties of proving the identity of cyber attacks due to the nature of the Web's edifice, such control would, fundamentally, give a free license to State sponsors of cyber attacks. In a sophisticated international cyber attack, missing or corrupted data commands could also be adequate to negate State control and defeat responsibility.

Without either new techniques like the probabilistic tracing project or very unsophisticated hackers, effective control would create state responsibility for cyber attacks just about a failure or non starter.

There are other vital disadvantage in espousing the ICJ's Nicaragua conceptualization with regards to evidencing state responsibility for cyber attacks, among them being the reality that the court divided the use of force into "most grave" and "less grave" categories,[21] and this has left the commentators divergent on the issue. Some commentators understand this view as a 'formalistic' and 'restrictive'. Christine Gray, stated it "will encourage aggression of a low key kind".[22] Others comprehend a low threshold of armed attack mixed with collective self-defense as a formula for the internationalization of civil conflicts.[23]As applied to cyber attacks, this philosophy might arguably provide low-level cyber attacks, possibly up to and together with the cyber attacks on Estonia, a pass at least as applied to international humanitarian law. This could encourage criminals and like minded people, if all they need to concern regarding law enforcement, and not the military. Rather, and whereas the law of cyber warfare remains ductile, the overall control standard ought to be adopted.

The Overall Control Standard

The ICJ has systematically utilised the more restrictive effective control standard in its legal philosophy, in Bosnian Genocide case,[24] however alternative tribunals, like the ICTY, haven't. The first President of The Hague Tribunal attacked the Bosnian Genocide judgement as strict an "unrealistically high standard of proof".[25] This burden of proof is almost not possible to satisfy in the context of cyberspace while no significant improvements in the tracing of cyber attacks.

Consequently, if international law is to have sufficient pertinence to cyber warfare, it is necessary that the overall control standard be assumed as a part of a forthcoming international regime for cyberspace. Lacking a pact or treaty on cyberspace, and or else to espousing the ICTY overall control standard, there is in addition precedent within the ICJ context itself to support a third more versatile standard of state responsibility.

Categorically, the ICJ admitted in the Iran hostage case that the actions of a state's citizens could be ascribed to the government if the citizens "acted on behalf of the State, having been charged by some competent organ of the Iranian state to carry out a specific operation".[26] Whereas, the court failed to notice enough proof to attribute the actions of the people to the government., the court did notice that the Iranian government was, all the same, accountable as a result of it aware of its obligations "under the 1961 Vienna Convention on Diplomatic Relations and the1963 Convention on Consular Relations to protect the U.S. embassy and its staff, and failed to comply with its obligations".[27]

This reasoning may be extended to cyber attacks in two ways in which. First, the quality may be adopted that, if the citizens of a state acted on behalf of a competent government organ, then the government may be vicariously responsible for the ensuing harm from such cyber attacks.

Second, if there's inadequate proof to search out attribution outright, as there was in Iran hostage, then the standard might become one amongst governmental awareness, i.e. if the government was attentive and vigilant to its obligations under international law to prevent its people and information infrastructure from launching cyber attacks and didn't befit these responsibilities and that state might then be held in breach of international law.

Either the Tadic or Iran hostage standards has the benefit of moving beyond the strict effective control framework, and holding State sponsors of cyber attacks responsible once fundamental proof exists of their engagement and involvement.

Hitherto, there are difficulties posed by espoused a typical of state responsibility with a lower burden of proof than effective management that ought to be addressed. Principal among these is that the danger of prosecuting suspect state sponsors of attacks that are indeed innocent. Politically, this concern might cause some states to push for the higher burden of proof enshrined within the effective control standard in order not to wrongly incriminate of sponsorship.

Such reviews and critiques may also in part be addressed though by way of a clarification that a requirement of “beyond a reasonable doubt” under the overall control standard is all the same a very excessive burden of proof that the prosecuting body have to meet, making frivolous or unwarranted cases unlikely.[28]

In short, it's so much too straightforward for governments to cover their cyber war operations under effective control standard. It ought to, therefore, be sufficient as a matter of international law to prove overall control by a government in a cyber attack, rather than complete control. For instance, if the overall control standard were utilized alternatively of effective control, it might be realizable that Russian incitement behind the cyber attacks on Estonia and Georgia, if established, would be adequate to satisfy state attribution. A complete and extensive future legal regime may want to grant Estonia or Georgia, and different sufferer nations, enough reparations for such cyber attacks.

Who are the Non State Actors in CyberSpace activities?

The growing importance of the cyber space is considered as a national security concern for the armed forces and governments globally. The most significant features of thiscyber space include asymmetric nature, lacking attribution, low costs of entries are referred to as the efficient medium for different protests, espionage, crime as well as military aggression.[29] All of these together make an attractive domain for the non actors within cyber space operations. Cyber dependency has become one of the major aspects in the entire society with complicated inter connections within several sectors has incremented the vulnerabilities towards attacks against the military and civilian infrastructures. The increased focus on this cyber defence in the armed forces is being observed in different parts of the world. For the military, cyber space has been identified as one of the five arenas, apart from land, air, space and air, where military operations can take place.[30] These distinct operations are referred to as cyber space operations, after consideration of both defensive and offensive measures and might be performed independently as the complement to the conventional warfare.

The concept of cyber warfare is eventually becoming much more relevant for all types of nation states and the requirement of quicker achievement of the capability of a military cyber space operation being the top priority for various armed forces as well as intelligence agencies in the entire world. The similar trends of cyber mobilization could be observed in various countries and the developed countries primarily check the requirement of a defensive capability for protection of the most vulnerable digitalized resources like control systems and commands.[31]

The following may act as a non-state actors in the the cyber warfare context;

Ordinary Citizens and Script Kiddies

The ordinary citizens can be defined as the inhabitants of any specific city or town, who are not involved in any type of controversial issues. Citizen is the respective status of any person recognized under the law or customer as being a legalized member of the sovereign state or even belonging to a nation.[32]

The entire idea of citizenship is being defined as the major capacity of different individuals defending their own rights for the governmental authorities. Any particular individual might comprise of several citizenships and an individual, who does not comprise of the citizenship of any state in the world, is referred to as stateless. A script kiddie or a skiddie can be defined as an unskilled individual, who eventually utilizes programs and scripts that are being developed by others for attacking the computerized system and network as well as deface web site like the web shell.[33] Most of the script kiddies are few juveniles, who lack the core capability of writing sophisticated exploits and programs on their own and the main objective is to gain credit within computer enthusiast communities.

Hacktivists and Hackers

A hacktivist is a person, who utilizes hacking to bring out social and political changes. The major motive of hacktivism is related to free speech, human rights as well as freedom of information movement.[34] The individuals, who perform hacktivism, are termed as hacktivists. They call the public's attention towards anything that is believed to be a vital issue like human rights and freedom of information. The hacktivists display personal messages over the website of any company.A computer hacker is a skilled computer expert, who utilizes their core technical knowledge for overcoming any type of problem. The hacker utilizes exploits and bugs for breaking into the computer systems and is advert to the computer security.[35] The hacker has an adherent of the technology as well as programming sub culture and can easily subvert computerized security. They often do not have major knowledge about hacking techniques and can create issues by manipulating data permanently.

Patriot Hackers and Cyber Insiders

Patriot hacking is the computerized hacking, where the supporters and citizens of a country for perpetrating attacks by the perceived enemies of the state.[36] According to the recent media, there had been major attention to the efforts, associated to the terrorists andtheir own attempts in conducting the electronic cyber terrorism. This type of hacking is illegal in different countries like the United States.[37]

One of the most popular and significant examples of patriot hacking was in the summer Olympics in the year of 2008. During the torch relay in this summer Olympics that was marred by the unrest within Tibet; few hackers from China have claimed to have hacked the web sites of CNN, Carrefour and the forums and web site provided tutorials for the process of launching DDoS attacks on the web site.

The cyber insiders are those hackers, who violate cyber security rules in military interest network, which is consistent with the activities of cyber espionage. The mode of threat caused by them is termed as cyber insider threat and is mainly related to unauthorized data access.[38] These attackers could be identified by consideration of different methodologies for detecting the activities, as soon as an exposure is being realized for better analysis of the result. A reconciliation of every data from the object actions is possible and these hackers could be stopped by CINDER security solution.

Cyber Terrorists and Malware Authors

The cyber terrorists are those individuals, who create cyber terrorism in the organization.[39] It is the utilization of the Internet for conducting violent activities, which result in the loss of lives for the core purpose of achieving ideological and political gains through intimidation and threats.

Malware author is a special type of attacker, who write original item of malware and comprises of certain amount of skill at programming or operating systems. They are talented developers of malware, who utilize botnets and complex tools like rootkits.[40] Malware authors utilize software packages after choosing from a set of options to enable the users in varying delivery methodologies, payloads, propagation means and any other similar factor. They are often considered in the type of script kiddies, since both of them do not require specific skill of programming.

Cyber Militias

The cyber militias are those individuals, who comprise of different risks from the lack of control on membership. Several opportunities for the cyber militia member exhibit subsequent behavior of the United States for establishing the threats internationally.[41] The countries like Iran, Russia, China and the United States are making heavy investments in their cyberwar capabilities and are even accumulating cyber weapons for using in the wartime. As a result, cyber space offers major opportunities to different countries for eliminating the chance of superiority in terms of military aspects.

Conclusion

The domestic and international implications of human society's increasing and crucial dependence on the internet makes essential the ability to deter, detect, and decrease the outcomes of cyber assaults. Today, NATO and also the US alike are at the point of determinant how the governance of cyberspace ought to develop, together with influencing the vector of the jus ad bellum from the beginning of the legal framework for cyber warfare. The strategies and practices that are assumed within the short-run therefore can greatly impact how this rapidly evolving body of law is moulded. The case has been made during the chapter that there are presently two competing regimes for state responsibility under international law, the effective and overall and overall standards. Owing to the technical difficulties with proving attribution for cyber attacks, at the side of the unconscionably high standards of evidence necessary by the effective control standard.

In my humble opinion, the adoption of the overall control standard has the advantage of holding state sponsors of cyber attacks responsible wherever there exists ample proof beyond a reasonable and an affordable doubt as critical to beyond any doubt. This standard could only be the one aspect to determine the state responsibility in cyber security, there are other issues that needs further research, and attention by policy makers and scholars likewise to prosecute the responsible state of cyber attacks, in an appropriate forum.

Notes:

[1] Oltramari, Alessandro, Lorrie Faith Cranor, Robert J. Walls, and Patrick D. McDaniel. "Building an Ontology of Cyber Security", In STIDS,(2014), Pp. 54-61

[2] Schmitt, Michael N. "The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision", Israel Law Review 48, no. 1 (2015), Pp. 81-109

[3] Pipyros, Kosmas, Lilian Mitrou, Dimitris Gritzalis, and Theodoros Apostolopoulos. “Cyberoperations and International Humanitarian Law: A review of obstacles in applying International Law rules in Cyber Warfare”, Information & Computer Security 24, no. 1 (2016), Pp. 38-52

[4] Gutzwiller, Robert S., Sunny Fugate, Benjamin D. Sawyer, and P. A. Hancock. “The human factors of cyber network defense”, In Proceedings of the Human Factors and Ergonomics Society Annual Meeting,Sage CA: Los Angeles, CA: SAGE publications, vol. 59, no. 1,(2015)Pp. 322-326

[5] Roscini, Marco. “Cyber operations as a use of force”, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ,(2015), Pp. 233-254

[6] Ducheine, Paul, and Jelle Van Haaster. “Fighting power, targeting and cyber operations”, In 2014 6th International Conference On Cyber Conflict (CyCon 2014),IEEE, (2014)Pp. 303-327

[7] Gompert, David C., and Martin Libicki. “Waging cyber war the american way”, Survival 57, no. 4 (2015), Pp. 7-28

[8] Rid, Thomas, and Ben Buchanan. “Attributing cyber attacks”, Journal of Strategic Studies 38, no. 1-2 (2015), Pp. 4-37

[9] Brown, Gary D., and Andrew O. Metcalf. “Easier said than done: legal reviews of cyber weapons”, J. Nat'l Sec. L. & Pol'y 7, (2014), p. 115

[10] Bannelier-Christakis, Karine. “Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?”, Baltic Yearbook of International Law Online 14, no. 1 (2015), Pp.23-39

[11] Jajodia, Sushil, V. S. Subrahmanian, Vipin Swarup, and Cliff Wang, “Cyber deception” Springer, (2016)

[12]Lipson, H. F, “Tracking and Tracing CyberAttacks: Technical Challenges and Global Policy Issues”,CERT Coordination Centre, (2002) page ix

[13] R. B. Hughes, “NATO and Cyber Defence: Mission Accomplished?”, NATO-OTAN, (2009),available athttps://www.atlcom.nl/ap_archive/pdf/AP%202009%20nr.%201/Hughes.pdf

[14]Lipson, H. F, “Tracking and Tracing CyberAttacks: Technical Challenges and Global Policy Issues”,CERT Coordination Centre, (2002), p.27

[15]Brenner, “The Hague Convention Relative to the Opening of Hostilities”,1910art. I(2006), p. 398

[16] “Responsibility of States for Internationally Wrongful Acts”,(2001)

[17]Nicaragua v. United States, 1986, p. 392

[18]Prosecutor v. Tadic, 1995, para. 70

[19]Pronk, R. J.P. 1997, “ICTY Issues Final Judgement Against Tadic in First International War Crimes Tribunal Since World War II”, Human Rights Brief, Centre for Human Rights and Humanitarian Law

[20]Capaldo, “Providing a Right of Self-Defense Against Large Scale Attacks by Irregular Forces: The Israeli-Hezbollah Conflict”,Harvard International Law Journal Online, 48, (2007) p.104

[21]Nicaragua v. United States, 1986, p. 101

[22] Christine, Gray, “International Law and the Use of Force”,Oxford University Press, (2000), p.141

[23]Watkin, K., “Controlling the Use of Force: A Role for Human Rights Norms in ContemporaryArmed Conflict”, American Journal of International Law98, (2004) , p.5

[24]Bosnia and Herzegovina v. Serbia and Montenegro, "the ICJ adopted the effective control rather than the overall control standard in deciding that Bosnia lacked the specific intent to commit genocide"

[25] Tosh, C. , "Genocide Acquittal Provokes Legal Debate", Institute for War and Peace Reporting,(2007)

[26]United States v. Iran, 1980, p. 29

[27] Barkham, J, "Information Warfare and International Law on the Use of Force". New York University Journal of International Law and Policy, 34, (2001.) Pp.57-114

[28] Erikkson, S. "Humiliating and Degrading Treatment under International Humanitarian Law:Criminal Accountability, State Responsibility, and Cultural Considerations", Air Force Law Review, 55, (2004), p.285

[29] Connell, Michael, and Sarah Vogler, "Russia's Approach to Cyber Warfare", (1Rev). No. DOP-2016-U-014231-1Rev. Center for Naval Analyses Arlington United States, (2017)

[30] Mancuso, Vincent F., James C. Christensen, Jennifer Cowley, Victor Finomore, Cleotide Gonzalez, and Benjamin Knott. "Human factors in cyber warfare II: Emerging perspectives", In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 58, no. 1, Sage CA: Los Angeles, CA: SAGE Publications, (2014), Pp. 415-418

[31] Roscini, Marco. "Evidentiary issues in international disputes related to state responsibility for cyber operations", Tex. Int'l LJ 50 (2015), p.233

[32] Inch, Andy. "Ordinary citizens and the political cultures of planning: In search of the subject of a new democratic ethos", Planning Theory 14, no. 4, (2015), Pp.404-424

[33] Roscini, Marco. "Cyber operations as a use of force", Research Handbook on International Law and Cyberspace", Edward Elgar Publishing (2015) Pp.233-254

[34] Tanczer, Leonie. "The Terrorist–Hacker/Hacktivist Distinction: An Investigation of Self-Identified Hackers and Hacktivists, Terrorists' Use of the Internet" , (2017), Pp.77-92

[35] Murphy, Brian C, "The risky shift toward online activism: do hacktivists pose an increased threat to the homeland?" Naval Postgraduate Scholl Montery,(2014), Pp. 1-157

[36] Gompert, David C., and Martin Libicki. "Waging cyber war the american way", Survival 57, no. 4 (2015),Pp. 7-28

[37] Wood, Steven. "Patriotic hackers", PhD diss., Manchester Metropolitan University, (2017), Pp. 1-24

[38] Ho, Shuyuan Mary, and Jonathan M. Hollister. "Cyber insider threat in virtual organizations",In Encyclopedia of Information Science and Technology, Third Edition, IGI Global, (2015.), pp. 1517-1525.

[39] Brown, Gary D., and Andrew O. Metcalf. "Easier said than done: legal reviews of cyber weapons", J. Nat'l Sec. L. & Pol'y 7 (2014),p.115

[40] Williams, Henry C., Joi N. Carter, Willie L. Campbell, Kaushik Roy, and Gerry V. Dozier. "Genetic & evolutionary feature selection for author identification of html associated withmalware", International Journal of Machine Learning and Computing 4, no. 3, pp. 1-3, (2014): 250

[41] Tinker, Paul W, "For the Common Defense of Cyberspace: Implications of a US Cyber Militia on Department of Defense Cyber Operations",Army Command and General Staff College for Leavenworth KS, Pp. 1-113, 2015