PalArch's Journal of Archaeology of Egypt / Egyptology

RESPONSIBILITY OF STATE TOWARDS THE ISSUES OF CYBER WARFARE UNDER INTERNATIONAL LAW: WITH SPECIAL REFERENCE TO THE CASE OF PROJECT LAKHTA

YORDAN GUNAWAN[1], NAUFAL BAGUS PRATAMA[2]
[1, 2] Universitas Muhammadiyah Yogyakarta, Indonesia
Tamantirto, Kasihan, Bantul, Yogyakarta, Indonesia
[1]Yordangunawan@umy.ac.id, [2]Naufalpratama@umy.ac.id

Yordan Gunawan, Naufal Bagus Pratama. Responsibility of State towards the Issues of Cyber Warfare under International Law: With Special Reference to the Case of Project Lakhta. – Palarch's Journal of Archaeology of Egypt/Egyptology 17(6) (2020). ISSN 1567-214X.

Keywords: Cyber Warfare, International Law, Project Lakhta, State Responsibility

ABSTRACT
Within a very first decades of the 21st century, the world has witnessed some severe cyber-attacks. In 2018, the Department of Justice of United States of America announced a criminal complaint in Alexandria, Virginia, against a Russian national for her alleged role in interfering with U.S Presidential Election 2016, including the 2018 midterm election under the operation called Project Lakhta. This will give a raise to a question on how the prevailing law could cover this new type of conduct such as the cyber-attack. Even though it is clearly stated under the ILC Draft on Internationally Wrongful Act, it is still poses challenges for cyber-attack to meet these conditions to give a rise to a state responsibility. Therefore, by using normative legal research to answer the problem statement, this research will show how the state responsibility towards the issue of cyberwarfare is under international law with the special reference to the case of Project Lakhta. The result shows that it is hard and challenging to determine whether a state responsibility could be given a rise for the cyber-attacks done by a state to another sovereign under the prevailing law, therefore there is a need for the world community to reach upon a consensus on determining the criteria and establishing International legal instrument concerning cyberwarfare in order to give security and certainty.

Introduction

Since the beginning of the 21st century, the world has witnessed such spectacular and severe cyber-attacks. These attacks include the attack on Estonia in 2007 as well as in Georgia in 2008. On 27 April of 2007, for weeks Estonia was hit by big cyber-attacks that taken down several online services with an internet traffic which disabled Estonian government bodies, banks, and media (Damian Mcgunniess, 2017). Furthermore, the attacks against Georgia took place in August 2008 and affected Georgian governmental web resources, mass media, forums and a lot of Georgian domains. It led to significant

communication delays, as well as financial losses. The Russian Government denied the allegations that it was behind the attacks, saying that individuals in Russia were unfeasible that individuals in Russia or anywhere would be able to start the attacks (John Markoff, 2008).

In 2018, the U.S. Justice Department reported a criminal complaint in Alexandria, Virginia, accusing a Russian national of her supposed role in a Russian plot to interfere with the U.S. political system, including the 2018 mid-term elections. Elena Alekseevna Khusyaynova has been accused of being an alleged core member of the "Project Lakhta," a scheme aimed at interfering with the 2016 US presidential election. The project operated to create chaos and aggravate the political situation during the election by creating thousands fake social media account which were also posted so many messages before the election took place (US Department of Juctice, 2018).

The notion on cyber warfare cannot be separated with the discussion about the development of technology and the internet itself. Project Lakhta is in fact a result of the invention of the internet where in the late 1960s, the first workable Internet prototype came with the development of ARPANET, or the Advanced Research Projects Agency Network (Evan Andrews, 2019). In 1969, the first demonstration was done through the ARPANET project which at that time Demonstrated University of California, Los Angeles (UCLA) communication with Stanford Research Institute through an integrated network now known as the Internet (Gregory Gromov, 2012). Actually, in a very early years of the emergence of the internet, it was invented for the military purposes, yet, with the rapid growth of the internet and the advent of the World Wide Web (WWW), the internet has grown quickly and exponentially across the world.

All countries over the globe have becoming so dependent with computer and internet. Computerization happened everywhere and becoming a must in a modern life nowadays. It is widespread and used in every dimensions of life, such as politic, economic, social, culture, law, defense, and security. The internet's emergence and global expansion has proven to be the most successful and the fastest technological revolution in human history. Within a period of only 18 years the number of active Internet users has increased from an estimated 1.9 billion in 2010 to over 3.9 billion in 2018 (Statista, 2018). Nowadays, we witness that states, businesses, academia, and individuals all are interconnected to a point never before imagined.

War and technological growth have coexisted for centuries. Military operations rely heavily on computer systems and networks, opening up a "fifth" war-fighting environment in addition to generally recognized areas of land, sea, air and outer space (US Department of Defense, 2006). For a very long time, states within their military operations has been seeking to develop weapons systems that will work more effectively and could minimize the risk for soldiers in order to decrease the casualties in battle (Vincent Bernard, 2015). Weapons systems are becoming more and more advanced, creating a way for humans to move further away even are no longer needed to be directly and physically in the battlefield. As artificial intelligence advances in weapons systems, direct human involvement has become minimal (Geneva Academy of International Humanitarian Law and Human Right, 2014).

Information Technology and the internet have become a main units of a national power because on how they have grown and developed to such extent, cyber war has echoed as nation-states are preparing themselves for cyber battle space. Many states are already preparing themselves to engage in a cyber war with frightening frequency as they are not only conducting cyber espionage and reconnaissance, yet also developing national strategies and creating an offensive capabilities in cyberwar. Many Cyber-attacks and network

infiltrations are widely documented, where this actions can be related to states and political goals. What possible is that more economic and human resources are expended on how to execute cyber warfare than on efforts to prevent it. Indeed, there is an amazing lack of international dialog and activity regarding cyberwar containment. This is such an unfortunate, because the cyber environment is a field where technological innovation and organizational art have far outstripped policy and strategy, and because cyberwarfare is, in theory, a phenomenon that must inevitably be controlled politically (Fred Schreier, 2015).

The case of Project Lakhta turns out to be one of the prime example on how these technological advancement could poses a serious threat. Where the Russian Nationals, Elena Alekseevna Khusyaynova is alleged to be the core member of the operation which intervened with United States Political System. Project Lakhta was designed to create and disseminate campaigns of misinformation on various issues, including misinformation on political candidates (Criminal Complaint, 2018). While it is clearly constitutes a breach of International Law and International customary law when it interferes with the domestic affairs of the United States, yet it raises questions whether these conduct could be connected with the Russian government because the perpetrator was a Russian and was committed on Russian soil. When it does, could the Russian government be held liable and the state responsibility could be given a rise. When a cyber-attack such Project Lakhta occurred, the issues on how to determine whether the attack has any connection to a particular state will face a difficulty. Since the attribution of cyber-attack is very difficult to do and pose some challenges because it brings new means of method and need a new way of approach.

Cyberwar is in turn part of the evolution of traditional warfare, which is also linked to broader social and political changes. It is now difficult to foresee any confrontation in a conflict where the elements of cyber-activity such as surveillance or sabotage are not involved. Whether the cyber war is real is not as relevant as how we can focus on preserving and mitigating the threats posed by this computer technology. After all, a cyber-attack does not need to kill someone or even inflict significant material harm to be deemed dangerous (Jarno Limnell and Thomas Rid, 2014).

This trend raises the question of how far the prevailing international law can be used into the cyber domain. There is no doubt that the prevailing international law governs state activities wherever they might occur, with no exception as in cyberspace. Nonetheless, in a point of view from some specific characteristics of the technology in question, trying to apply some of these prevailing laws, principles and terminology to a brand new technology that brings somethings new could pose some difficulties (Rain Liivoja, 2015). One of the very challenging obstacle is pertaining on how is the state should be responsible when this cyber war ever occurred. According to International Law Commission Articles on Internationally Wrongful Acts, every internationally wrongful act of a State entails the international responsibility of that State. Looking at the Project Lakhta case, then how the Russian government is could bear liable and should be responsible for the cyber-attack in this case. Therefore this thesis will find out on how a state responsible for a cyber-attack under international law with special reference to the case of project Lakhta.

Research Method

The researcher uses normative legal research to answer the problem statement, which means that the research will show how the law regulates such condition

and how the application of law itself. Normative legal research is used to find the truth of coherence, namely discovering whether the existing law is in conformity with the rule of law, whether the norms in the form of a command or prohibition is in line with the principles of law and whether one's actions are in accordance with the norms of law or legal principles (McConville, Mike and Hong Chui, 2012). The research used secondary data in that the research materials are taken from literatures. Moreover, it consists of primary, secondary and tertiary legal while the method of data collection in this investigation will be through library analysis and will attempt to draw conclusions from relevant records, such as conferences, books, scientific journals and others related to the key problem as the topic of this research. The data will be systematically analyzed by legal qualitative means. Systematically ensures that analysis is conducted according to international law. Judicial qualitative implies that this will be linked to the theory of law, convention and other relevant regulations. This study will use qualitative analysis. Qualitative analysis emphasizes the analysis of the process of inference from descriptive data in the form of words compiled based on data that has been obtained by researchers from literature studies (Hancock Beverly, 2002).

Discussion

History and Development of Warfare

The notion about war will take us to a very beginning and basic cause of it all, human being itself. As a creature that is dependent to other, human is communal creature that has to live together to ensure their live, no human can live in solitude. Aristotle mentioned that human is a Zoon Politico on or political animal or how as Adam Smith stated that human is Homo Hominy Socinus or a creature of social. Aside of that, a very famous scholars, an English philosopher with his very famous quote saying that Homo Hominy Lupus, which means that human is a wolf to other human. Realizing that human is a creature of interest, they always try to maximize their own benefits. Since the beginning of time conflict was already occurred whereas there are more than one individuals within the area (Herbert Gintis and Carel Van Schaik, 2013).

From a very small scale of conflict which is the individual feud, human history has shown us on how wars were waged across the world and time. The earliest evidence for prehistoric warfare belongs to Site 117 of the Mesolithic Cemetery, which was estimated to be about 14,000 years old. Around 45 percent of the skeletons showed signs of violent death there (Lawrence H. Keeley, 1996).

The discovery and spread of agriculture preceded in fifth millennium B.C by the domestication of animals. Are seen as the developments that set the stage for the development of the first large, complex urban societies. Such societies which emerged probably simultaneously around 4000 B.C. Stone tools were used in both Egypt and Mesopotamia, but stone tools and weapons gave way to bronze within 500 years. Within the founding of bronze mining and production, a revolution in warfare occurred. In this period the development of many new equipment such as housing or daily life tools including the weaponry. Weapons such penetrating axe, composite bow and body armour, helmet, until the utilization of the wheel to make a chariot gave birth to a range of tactical innovations-phalanx lines, enhanced mobility, pursuit, rank structures and also the emergence of the whole range of social, political, economic, psychological, and military technologies that made the conduct of war a relatively normal part of social existence (Robert Drews, 1993).

What made war possible was the advent of societies with clearly developed

social structures that supported the new social roles and behaviors with cohesion and legitimacy. These early civilizations provided the first examples of institutions ruled by the state, initially as centralized chiefdoms and later as monarchies. It is paramount to be noted that the period of 4000 to 2000 B.C is an early period where the war was developed and also its instrumentalities. When this era started, cities or any other social structure had not developed by the people of that time. In which such things were so important in order to sustain a large scale of communal life. Agriculture, which in ancient times became the foundation of the nation-state, was not yet and not well developed to provide enough food supplies for so many people within a large or even moderate populations of the people. As psychologically, people have not yet learned to assign importance to any wider social group as the immediate family, clan or tribe. Warfare itself had not have any important meaning and people had no sense about on the need of going to war. Military technology and organization were primitive, and army and war professionalization had not yet begun. The two thousand years following the dawn of the fourth millennium changed all this. As a mechanism for cultural progress, the conduct of war became a legitimate social activity assisted by an extensive institutional framework, and it became an integral feature of the social order if citizens were to survive the aggressive actions of others (Richard A. Gabriel and Karen S. Metz, 1992).

The most significant invention in weaponry of the period of the Hundred Years War was the introduction of gunpowder which, when coupled with the introduction of new techniques for casting metal, produced the primitive cannon. By the 15th and 16th centuries gunpowder changed the field of war. The emergence of the musketeer, the predecessor of the modern rifleman, and his firelock musket allowed tightly packed infantry formations to engage in cavalry without having to engage in close combat directly. However, the slow rate of fire of these early short-range weapons required the musketeers to be protected from the hostile advance, an issue which led to the mixing of musketeer formations with pike man. While the mixture of pike to musket has changed considerably over the next 300 years, for the next three centuries the mixed type of infantry remained the basic structure of infantry (Spencer C. Tucker, 2015).

The American Revolutionary war gave a way the US to achieved its freedom and brought us to what so called as the modern warfare nowadays. The Revolutionary War bridged the gap between medieval-era hand-to-hand fighting and the precursors of modern warfare. Mostly, the battle that took place during this war waged on the battlefield rather than on the sea, while mainly the American fleet limited to privateering. The battles were fought with soldiers lining up in fields facing each other, where they shot at each other, usually around 100 yards apart. Commanders would often have their troops fire a volley before ordering a bayonet charge, which would manage the largest number of casualties (Robert W. Coakley and Stetson Conn, 2010).

The whole world waged war for the first time in history – a war that devoured men, resources and energy; that divided loyalties, reignited old fervours, and created new horrors (Annette Becker, 2015). World War I (WWI) brought immense technological improvements to the way wars were fought. The advances in gas, tanks, aircraft and other equipment resulting in some of the most violent warfare and destruction ever seen. The fighting style focused primarily on trench warfare, with the days of standing in lines across fields facing the enemy lines. The Western Front, a region of Belgium and northern France, witnessed the most trench warfare, where fighting between Germans and Allied forces was largely taking place. The trenches were a direct product

of the latest technology, because the trenches were built to protect the soldiers from guns, aircraft and chemical weapons (Stephen Bull, 2002).

The WWI illustrated just how much more devastating new technology could bring war. Some of the major innovations of the World War I are the machine Guns, flame throwers, aircrafts, and tanks. Although many modern weapons emerged in the First World War, the Second World War brought about major changes in the way war was waged. Instead of battling in trenches, troops started to cover shell craters and foxholes, instead of hunkering down in fixed lines. There were even more options for troops to get to the front, with motor vehicles, railways and aircraft adding extra speed and combat techniques developing. To understand how warfare changed since WWI, consider the evolution of war weaponry and the top military developments showcased in WWII By the time WWII started, airplanes had advanced significantly. Since bombers were able to destroy cities, strike strategic locations and cause destruction, air supremacy was a crucial factor in both sides' war plans (Thomas New Dick, 2015). Nuclear technology is possibly the most well-known military technology first used during the war. If you wonder how technology has changed war, you can look at the nuclear bomb to account for much of it. The ability to lay waste a city with a single bomb or missile provides a considerable power to any nation with nuclear weapons in preventing or winning a military conflict (Joseph Siracusa, 2008). The United States famously created the first atomic bomb, dropping it into the city of Hiroshima, killing 80,000 people and causing considerable damage to the city. When the Japanese did not surrender, the American forces dropped another much stronger atomic bomb on Nagasaki and immediately killed 70,000 civilians. The detonation of this second bomb has brought the war to an end.

In the later part of the 1990s, concerns regarding the use of cyber operations and their legal consequences started to arise (Paul Bracken, 2017). In 1999 The Naval War College of the United States held a legal conference where legal experts delivered papers on different aspects of cyber operations (BT. O Donnell and JC Kraska, 2003). The conference proceedings were later collected in an edited volume, which has since become a significant resource in cyber operations research (MN. Schmitt and BT O Donnel, 2002). However, in the years since the 1999 US Naval War College meeting, cyber warfare and, in particular, its international legal implications have received little attention. This mind-set would subsequently shift in the aftermath of several cyber events, which made it clear that the once theoretical and hypothetical scope of major cyber operations causing harm, death or destruction, directly or indirectly, was becoming increasingly possible (Michael Ignatief, 2000).

Cyber operations returned to the forefront of international concern in 2007 following the unprecedented assault on Estonia's computer network and, in particular, the interruption and disabling of government information systems and commercial Internet infrastructure (Michael Schmitt, 2011). Another notable example of the cyber operation is the mounted cyber operation in its armed conflict with the Russian Federation in 2008, against Georgia. The cumulative effect of these cyber incidents has brought to light the reality that cyber operations pose a critical threat to States ' national security and the well-being of human life and commercial interests (Peter Berkowitz, 2011).

Cyber Warfare as the Use of Force

Under international law, the notion of "use of force" has always been concerned with the intrastate relations, and not merely domestic use of force by government officials against their citizens. For centuries the decision to wage war was not subject to any legal restrictions. States have had the freedom

to decide whether or not to wage war on each other. No strict legislation on the use of force existed, the only form of control for States was a moral question as to whether the war was just or not. No objective method existed for deciding what was just or unjust. In addition, war was seen as a legitimate means of action, its main aim being to alter territorial boundaries. The earliest form of control of the use of force can be found in classical Greek and Roman philosopher Cicero's bellum justum or 'just war' doctrines, which were subsequently based on and developed by some Christian theologians in the Middle Ages, such as Saint Augustine and Saint Thomas Aquinas (Robert A. Markus, 1983). While the existing legislation on the use of force is relatively modern, dating from the adoption of the UN Charter in 1945, control of the resort to force in some form can be traced back to ancient times (Stephen C. Neff, 2005).

The Peace of Westphalia 1648 marks the historic milestone of the birth of the modern sovereign state, which has become the pre-eminent founder and subject of international law. In the ensuing centuries, the prevailing theory seems to be that 'the jus ad bellum has withered to the mere knowledge that the sovereign state has the right to use force or war to enforce its claims or to preserve its protection and interests. Indeed, international law regarded the use of force by states as being indifferent, so that the decision to go to war was not a matter of law, but an expediency. War has basically become an important instrument of state craftsmanship, or another form of conducting policy (Agatha Verdebout, 2014).

By the end of the First World War in 1918, the international community started to look for ways of regulating the States' use of force. Thus the League of Nations was founded in 1919. The Constitution creating the League of Nations was the League of Nations Covenant. The Covenant did not prohibit the use of force but instead advised states not to attack another sovereign state. The end of Second World War brought nations to gather at the San Francisco Conference to adopt the UN Charter on 26 June 1945 (Stephen C. Schlesinger, 2003). This establishes the UN, an organization whose primary goal is to preserve international peace and security that led to the world in which the current era of the legal regulation of the use of force was (UN Charter, Article 1). The prohibition of threat or the use of force is expressly stipulated in Article 2 Paragraph 4 of the 1945 Charter of the United Nations. This also followed with the obligation on members to resolve their conflicts through peaceful means and the development of a collective security system.

Article 2 paragraph 4 of the United Nation Charter does not specify what kind of force States are prohibited from using, whether force is merely constitutes a military or economic, or even combination of both. The general understanding between writers and states is that Article 2(4) prohibits only military force. Those in favor of this position offer two key reasons. First, they claim that since the UN itself was created in reaction to the disaster of the Second World War, the force referred to in the clause represents the kind of force employed in that war, which is primarily military force. Second, this view is supported by the history of UN negotiations. When the establishment of the UN was discussed in the United States, several states suggested banning economic aggression. However, the majority of other participants rejected the proposal. The latter argued that because states were usually free to choose whether to trade with each other or not, one state's refusal to trade with another should not be deemed a breach of international law. While military force is still considered an object of prohibition pursuant to Article 2(4), the United Nations has made it clear that economic aggression is unacceptable when used to coerce States (Ademola Abass, 2011) .

The vast majority of commentators today consider the word 'force' to be basically synonymous with 'armed' or 'military' force in Article 2(4) of the UN Charter since the ordinary definition of 'force' is clearly broad enough to encompass both armed and unarmed types of coercion (Yoram Dinstein, 2005). This does not necessarily mean the prohibition of inter-state action is limited to the use of kinetic, chemical, biological or nuclear weapons. According the International Court of Justice, the prohibition applies "to any use of force, regardless of the weapons employed" (International Court of Juctice, 1996). Indeed, it is generally uncontroversial that cyber operations fall under the prohibition laid down in Article 2(4) of the UN Charter until their effects are comparable with those of kinetic, chemical, biological or nuclear weapons (Michael Schmitt, 1999). It will definitely include the use of cyber operations as an offensive or defensive weapon intended to cause death or injury to persons or the destruction of object and infrastructure, irrespective of whether such destruction entails physical damage, functional harm or a combination of both. Cyber operations manipulating target computer systems to cause a meltdown in a nuclear power plant, or opening the floodgates of a dam above a densely populated area, or disabling air traffic control at a busy airport under bad weather conditions, each possibly horrendous consequences in terms of death, injury and destruction, would therefore be conspicuous examples of the use of 'force' within the meaning of Article 2(4) of the UN Charter. While Project Lakhta case did not deliver such devastation resulting in death or physical destruction, it is still necessary to address another view to the case in determination of its unlawfulness. Articles 2(4) and 51 of the UN Charter prohibit the use of force irrespective of the weapons used as explained in the ICJ Advisory Opinion in Legality of Threat or Use of Nuclear Weapons (1996). Nevertheless, it has been argued that there is still no global consensus on the precise threshold at which a cyber-attack can be regarded as a use of force within the meaning of Article 2(4) of the UN Charter (Susan W. Brenner, 2014).

According to Rule 11 of the Tallinn Manual, "cyber activity constitutes a use of force when its scale and consequences are comparable with non-cyber operations rising to the level of use of force". Acts whose scale and consequences classify as use of force include actions that harm or kill people, or damage or loss of objects. They do not need to include the use of military or other armed forces, nor do they require immediate physical consequences if they meet eight key non-exclusive requirements to be measured on a case-by - case holistic review of each incident in the light of the circumstances surrounding them. These non-exhaustive factors include: "severity in damage, destruction, injury or death; immediacy (the speed with which consequences manifest); directness (the causal relation between a cyber operation and its consequences); invasiveness (the degree to which a cyber operation intrudes into targeted systems); measurability of the effects; military character of the cyber operation; extent of State involvement; and presumptive legality" (i.e., the acts not expressly prohibited by international law are less likely to be considered by States as uses of force) (Michael N. Schm.

Rule 12 of the Tallinn Manual states that: "A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force." Rule 12 of the Tallinn Manual represents the widely agreed view that a threatened cyber operation will be lawful if, in the event that it is carried out, the threatened activity would itself be compliant with the UN charter. More specifically, a threatened cyber operation would be legal if the threatened action were to constitute a legitimate exercise of the right of self-defence or an action

pursuant to Chapter VII of the UN Charter implementing a UN Security Council resolution.

However, overall there is still no consensus on the precise threshold at which cyber operations should amount to an internationally unjustified threat or use of force. Indeed, there is not even a controversy identifiable with clear positions and conflicting criteria. The truth is that cyber operations, which almost always fall within the grey zone between traditional military force and other forms of coercion, were simply not anticipated by the drafters of the UN Charter and, to date, neither state practice nor international jurisprudence provide clear criteria as to the threshold at which cyber operations which do not cause death, injury or destruction should be looked at. It should also be remembered that a cyber operation does not need to be "forced" to be internationally wrongful within the context of Article 2(4) of the UN Charter, nor will all cyber operations amounting to "force" inherently be unlawful. Firstly, the illegal nature of a cyber operation could result from a breach of any international law obligations. For example, interstate computer network manipulation for intelligence gathering, electronic transmission of hostile propaganda, or denial of service attacks will each infringe the sovereignty sphere of the affected state and, thus, the customary principle of non-intervention, even if they do not qualify as use of force within the context of Article 2(4) of the UN Charter. Similarly, non-destructive cyber operations intruding into computer-based files, records and correspondence of a foreign diplomatic mission, or interfering with the free contact of the mission, will infringe the receiving State's international obligations under the diplomatic relations law. Potentially important legal problems may also arise under international trade law or human rights law, for example where denial of service attacks conflict with the freedom of speech of individuals within the operating State's jurisdiction (Universal Declaration on Human Right, Article 19). As it is happened in Project Lakhta where at the very least the operation certainly breach the Non-intervention principle. However, the focus of the analysis is on the constraints placed on cyberwarfare by current international law and not on the international permissibility (or not) of cyber operations more generally.

State Responsibility on Cyber Warfare

An act may be considered internationally wrongful if, under international law, the harmful action or omission is attributable to the State and, at the same time, conduct constitutes infringement of an international obligation. Guidance on the attribution of responsibility for international law is to be followed from the Draft Articles on the Responsibility of States for International Wrongful Acts (2001) of the International Law Commission, which the International Court of Justice has extensively relied on to understand international law in this matter. The Tallinn Manual also follows the ILC's Draft Articles very closely when it posits: "Under international law, States may be responsible for cyber operations that their organs conduct or that are otherwise attributable to them by virtue of the law of State responsibility. The actions of non-State actors may also sometimes be attributable to States" (ICJ Report, 1949).

In addition to responsibility for cyber activities attributed to a State, general international law imposes on every State the due diligence duty "not to allow knowingly its territory to be used for acts contrary to the rights of other States". The ICJ stipulated this provision in the case of Corfu Channel. The territorial State shall exercise its duty of due diligence, as can reasonably be expected. Thus, a transit State through which the Internet is routed through its territory or a developing State from which cyber-attack is initiated can only be expected to take whatever action it wants if it becomes aware of the crime and only in

compliance with its technical capability (Michael N. Schmitt, 2015). While the International Group of Experts who wrote the Tallinn Manual could not agree on whether constructive knowledge was adequate to entail due diligence, the present author believes that a State must take steps to avoid or stop its territory, either in accordance with its real or constructive knowledge and in the light of its technical potential (Karine Bannelier Christakis, 2014). However, it will take time for State practice to settle on what such reasonable measures actually are.

Identifying an international norm that cyber-attacks constitute the breach of is rather simple. As stated previously, Article 2(4) of the Charter of the United Nations forbids the use of force in international affairs and is considered a peremptory rule. On the basis of the already cited UN documents (i.e. the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations and the Charter of Economic Rights and Duties of States) Attacks on key state infrastructure carried out by electronic means can be defined as 'any other type of measures to coerce another State,' thus constituting an infringement of international law. What is more difficult, however, is the attribution of a cyber-attack to a particular state, one that initiated it or allowed it. A State may be held accountable for its own acts (acts of its organs) and the actions of private individuals acting on its behalf or order (ILC Draft, Article 5, 7, 8).

At the present state of technical development, it is not extremely difficult to determine the physical location of a computer from which cyber-attacks were carried out. However, the very fact that a computer used for a cyber-attack physical location does not (and should not) allow that cyber-attack to be attributed to a particular state. Such an assumption would be highly unjustified as a state is not responsible for the actions of its residents operating hardware in its territory. In the traditional concept of state responsibility, a State will be solely responsible for those of its residents, it has explicitly authorized it to act on its behalf. Proving a formal link between a State resident and a State authority in the case of cyber-attacks could be excessively difficult and any remedial proceedings could be deemed unsuccessful.

However, a state could also be held responsible for a breach of an international obligation not only because of its actions but also because of its omission, or in other words because it does not prevent that attack from taking place. Both doctrine and the judiciary make it clear that a State may be held liable not only for its actions but also for its omissions, in particular for failing to exercise due diligence (Ian Brownlie, 1983). Such an interpretation is supported by the formulation of Article 14(3) of the ILC draft, which specifies that a State may be held responsible for the actions of an insurrectionary movement's organs where such attribution is valid under international law. As explained by Crawford in his commentary to the ILC Draft Articles (J. Crawford, 2002), this article regards a situation in which a state is in “breach of obligation to prevent a given event”. Such an obligation is generally defined as an obligation to make best efforts, calling on a state to take all "reasonable" and "necessary" steps to avoid a particular event, but without a guarantee that such an event will not take place. The doctrine recognizes State responsibility for quasi-legal person's acts as an example of this situation. This can also be applied directly to the action of the "Naszi" organization in the case of the attacks in Estonia where the State did not prevent the attacks and did not take any measures to prevent them.

In the case of Project Lakhta, where a state does not provide adequate international protection from cyber-attacks by its citizens from its territory, a

jus cogent norm obliging governments to protect the sovereignty and integrity of other states results not only from the article 2(4) UNC, but also from a peremptory customary principle of the same substance. Such an obligation may be comprehended as both: an intolerability of any active intrusion into internal affairs of a state, as well as a due diligence requirement to prevent such an intrusion of foreign sovereignty from one's own territory. As Vark rightly pointed out, arising from the nature of such a responsibility, it is the duty of every State from whose territory an internationally unlawful act is carried out to comply with the victim state in such a way as to eradicate such a harmful act or, if it cannot be avoided, its consequences (R. Vark, 2006). Therefore, if a State is unable to protect the interests of another sovereign, it cannot allow private individuals acting within its territory to inflict harm or create a danger to that sovereign while being shielded by his immunity.

In cyber warfare, attribution is extremely difficult due to the nature of the weapons and techniques employed. As mentioned above, states or non-state parties may use many zombie computers around the world to commit a particular attack, leaving little opportunity for the victim nation to discover who operated behind the mask of zombie computers around the globe (Giles Trendle, 2002). For example, the China-based "Ghostnet" hacker organization infiltrated thousands of computers worldwide, from India to New York to London (Oona A. Hathaway, et al, 2012). While the authorities in these respective countries knew that the hackers were based in China, they were unable to decide if these Chinese computers were merely zombie computers used to discard the scent of the real perpetrators' location or the actual perpetrators' computers themselves. But if a state ever believes and can confirm the attribution of a cyber-attack, the question remains whether the host state is kept responsible if the perpetrators are non-state actors.

Attribution can be considered as a normative procedure used to create a connection between an act, its physical author and a state by applying rules that specify if there is a sufficiently close relation between a certain conduct and a state to attribute that conduct to the state (Crawford J, et al, 2010). Importantly, the very essence of attribution is to "make a state answer for, or face the consequences of, deeds of persons or entities that belong to its organization or function under its control" (Niels Blokker, Nico Schrijver, 2005). In a sense, states could be considered as abstract entities which operate through physical individuals. Any State may be responsible for the conduct of its institutions and for the acts of private individuals, acting on their behalf or order. Therefore, it is important to show that the offenders acted under the direction or control of a state for the purpose of attributing a certain conduct to a State. Until now, two potential measures have been used in international law to evaluate a degree of state control over perpetrators of such crimes, namely the "effective control" and the "overall control" measures (James A. Green, 2015). Moreover, the third approach of "virtual control" test has recently been suggested.

Firstly, to address the effective control test, according to the ICJ ruling in the case of Nicaragua, in order to assign responsibility to a state, it must be shown that it possessed effective control of military or paramilitary operations that resulted in such violations (ICJ Report, 1986). The effective control test which was subsequently applied by the ICJ in the case of the Bosnian Genocide requires the State to have clear, specific control over the actor involved until it can be attributed to the actions of that actor. Providing proof of control over a group's particular activities involves proving the orders, commands or particular instances of State control over the acts concerned. Meanwhile for the overall control test, it was in 1999, when the ICTY applied this test in the

Tadić Case. However, the overall control test is regarded to be wider than the effective control test. Nonetheless, in its judgment in the case of the Bosnian Genocide, the ICJ argued that this measure is unpersuasive, because the overall control measure expands excessively the domain of state responsibility and the effective control test applied (ICJ Report, 1996). Overall control requires a general degree of control that goes beyond mere assistance or funding provision. According to the ICTY, a state has the overall control if it has a role in the organization, management and support of a group (Tadic Judgement, 1999).

Given the above-mentioned tests, it is legitimate to claim that they are of little use in the context of cyber-attacks. As an illustration, the mere fact that the malware used in the cyber-attack was traced to certain network infrastructures in the territory of a given state does not constitute a compelling argument for holding it responsible for the attack. First, experts emphasize that networks are complex, data paths can go through many systems in many countries, or can be managed by many different administrative areas. In addition, the computer network environments are not configured to support attacker attribution (David A. Wheeler, Gregrory N. Larsen, 2003). In addition, such an infrastructure may have been operated by non-State actors who use the infrastructure to conduct cyber operations. It should be emphasized that the attribution is a sufficient criterion to find a State responsible for a certain conduct. Apparently, international law does not comply with the rapidly evolving IT and the usefulness of the existing acquis of international lawmakers, jurisprudence and scholars is highly doubtful.

There is abundant proof that Russia has waged a sophisticated campaign to manipulate the US political system in the run-up to the 2016 presidential election and, more generally, to weaken the American democratic process (Christina Lam, 2018). Russian participation in the social media campaign was first reported in the January 2017 Study of the Director of National Intelligence, Evaluating Russian Activities and Intentions in the Recent US Elections. In its March 2018 Report on Russia's Active Measures, The House Permanent Select Committee on Intelligence agreed with the intelligence community's earlier findings and considered them "to be based on compelling facts and well-reasoned analysis." These findings were expressed in the Senate Select Intelligence Committee's July 2018 report, which also endorsed the assessment of the intelligence community and the findings on Russian involvement. The Internet Research Agency's federal indictment of February 2018 offers more information on the Russian Government's position. It explained how companies with direct ties to the Russian Government provided Internet Research Agency funding. It also explained how those organizations tried to conceal their ties to Russian government. In addition, several people with close connections with Vladimir Putin have also been prosecuted for their role in the social media campaign (Neil MacFarquhar, 2018). Elena Khusyaynova's federal indictment in October 2018 gave even more information about the Russian link to Project Lakhta and the internet research agency's work (Criminal Complaint, 2018).

Under international law, the Project Lakhta actions are attributable to Russia. President Putin and the Russian government were specifically approving the operations (National Intelligence Report, 2017) . Thus, they can be attributed to Russia because the Project Lakhta was acting under Russia's direction and control. As the International Law Commission stated, "The attribution to the State of conduct in fact authorized by it is widely accepted in international jurisprudence". This concept is echoed in the Tallinn Manual, which states that cyber operations carried out by a non-state actor are attributed to a state

when such operations have been carried out "pursuant to its instructions or under its direction or control" as well as if the state "acknowledges and adopts the operations as its own." Russia can also be held liable for failure to uphold the principle of due diligence and the prevention of transboundary harm (Rebecca Crootof, 2018). Although the Russian government has denied any ties to the Project Lakhta. Elena Khusyaynova did not answer the criminal charges brought against her, although this is not shocking as she is in Russia and is unlikely to be extradited to the United States (Quinta Jurecic, 2018).
Therefore under the perspective of international law, state responsibility could be given a rise by applying the pre-existing international legal instrument and principles on the issues of cyber-attacks such in the case of Project Lakhta. Even though in applying these pre-existing law and principles to a considerably new type of conduct in such a new domain, cyberspace, encounters some certain and particular difficulties and gives some important questions to arise. Some of these questions can be resolved through classic treaty interpretation in conjunction with a good measure of common sense, whereas others require a unanimous policy decision by the international legislator, the international community of state.

Conclusions

The use of cyber threats and attacks in a cyber warfare are becoming more common, sophisticated and damaging. Without a doubt, there is an urgent need to find the solution of this stalemate situation. Under International Law Commission Draft on Internationally Wrongful Acts, in order for a state responsibility to arise, 2 criteria must be met. Firstly, there must be an illegal act which constitutes a breach of international law or international customary law. Secondly, it must be attributable to a state. In case where cyber-attacks is concern, the determination of the unlawfulness of the conduct is rather simple. Meanwhile the attributability is exceptionally difficult to do. As it has been shown in this research, as far as international law is concerned, the phenomenon of cyberwarfare including the issue of responsibility of state does not exist in a legal vacuum, yet is a subject to a well and pre-established regulations and principles. However applying these prevailing law and principles to this kind of new type of conduct and environment will certainly face some particular difficulties and gives some important questions to arise. While concerning the responsibility of Russian Government towards the case of Project Lakhta, It is attributable to the Russian, since President Putin and the Russian Government specifically approved this activity. Russia may also be held liable for failure to comply with the principle of due diligence and the prevention of transboundary harm. Therefore the state responsibility could be given a rise under the International Law. Even though the Russian government has denied any connections to Project Lakhta.

References

Ademola Abass. (2011). Complete International Law. New York: Oxford University Press.

Agatha Verdebout. (2014). The Contemporary Discourse on The Use of Force in The Nineteenth Century: A Diachronic and Critical Analysis. Journal on the Use of Force and International Law. 1(2).

Annette Becker. (2015). The Great War: World War, Total War. International Review of the Red Cross. 97(900).

Crawford J, Pellet A, and Olleson S. (2010). The Law of International Responsibility, Oxford/New York: Oxford University Press.

Bradley Raboin. (2011). Corresponding Evolution: International Law and the

Emergence of Cyber Warfare. Journal of the National Association of Administrative Law Judiciary. 31(2).

BT O'Donnell & JC Kraska. (2003). Humanitarian Law: Developing International Rules for the Digital Battlefield. Journal of Conflict and Security Law. 8(1).

Christina Lam. (2018). A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election. Boston College Law Review. 59(6).

Criminal Complaint. (2018). United States v. Khusyaynova.

Damien McGunniess, "How a Cyber-attack Transformed Estonia", https://www.bbc.com/news/39655415, accessed on 3 March 2020 at 1:15 p.m.

David A. Wheeler, Gregory N. Larsen. (2003). Techniques for Cyber Attack Attribution, Alexandria: Institute for Defense Analyses.

Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States.

Evan Andrews, "Who Invented the Internet?", https://www.history.com/news/who-invented-the-internet, accessed on 20 February 2020 at 7:17 p.m.

Fred Schreier. (2015). On Cyberwarfare, DCAF Horizon 2015 Working Paper No. 7, Geneva, Geneva Centre for Democratic Control of Armed Force.

Geneva Academy of International Humanitarian Law and Human Rights. (2014). Academy Briefing No. 8: Autonomous Weapons Systems under International Law, Geneva, Geneva Academy.

Giles Trendle. (2002). Cyberwar. The World Today. 58(4).

Gregory Gromov, 2012, "History of Internet and World Wide Web - Roads and Crossroads of the Internet History", http://www.netvalley.com/, accessed on 20 February 2020 at 8:12 p.m.

Hancock, Beverly. (2002). An Introduction to Qualitative Research, Leicester: Trent Focus Group.

Herbert Gintis and Carel van Schaik. (2013). "Zoon Politicon: The Evolutionary Roots of Human Sociopolitical Systems", Santa Fe Institute and Central European University.

Ian Brownlie. (1983). System of the Law of Nations: State Responsibility. Oxford: Oxford University Press.

ICJ Report. (1980). Case Concerning United States Diplomat and Consular Staff in Tehran.

ICJ Report. (1986). Case Concerning Military and Paramilitary Activities in and Against Nicaragua.

International Court of Justice Report. (2005). Case Concerning Armed Activities on the Territory of the Congo (DR Congo v. Uganda).

International Court of Justice. (1996). Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion.

International Court of Justice Report. (1949). The Corfu Channel Case.

International Court of Justice Reports. (1996). Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide.

Indictment at 2-4. (2018). United States v. Internet Research Agency L.L.C.

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries 47 (2008).

International Law Commissions Draft on Responsibility of States for Internationally Wrongful Act.

James A. Green. (2015). Cyber Warfare: A Multidisciplinary Analysis. New York: Routledge.

Jarno Limnéll, Thomas Rid. (2014). Is Cyberwar Real? Gauging the Threats. Foreign Affairs. 93(2).

Jean S. Pictet. (1952). Commentary of the First Geneva Convention for the

Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, International Committee of the Red Cross, Geneva, International Committee of the Red Cross.

John Markoff, "Before the Gunfire, Cyberattacks", https://www.nytimes.com/2008/08/13/technology/13cyber.html, accessed on 3 March 2020 at 2:47 p.m.

Joseph Siracusa. (2008). Nuclear Weapons: A Very Short Introduction, New York: Oxford University Press.

Lawrence H. Keeley. (1996). War Before Civilization: The Myth of the Peaceful Savage: Oxford University Press.

McConville, Mike and Wing Hong Chui. (2012). Research Methods for Law, Edinburgh: Edinburgh University Press.

Michael N. Schmitt. (2011). Cyber Operations and the Jus Ad Bellum Revisited. Villanova Law Review. 56(3).

Michael N. Schmitt. (2015). In Defense of Due Diligence in Cyberspace. Yale Law Journal. 125 (168).

Michael Schmitt. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law. 37(681).

Michael Ignatief. (2000). Virtual War: Kosovo and Beyond, United Kingdom: Picador.

MN Schmitt & BT O'Donnell. (2002). Computer Network Attack and International Law. US: Naval War College.

National Intelligence Report. (2017). Assessing Russian Activities and Intentions in Recent US Elections.

Neil MacFarquhar, "Oligarch Tied to Troll Factory Earned Nickname "Putin's Cook,", https://www.wral.com/meet-yevgeny-prigozhin-the-russianoligarch-indicted-for-interfering-in-the-u-s-elections/17347516, accessed on 31 August 2020 at 14 p.m.

Niels Blokker, Nico Schrijver. (2005). The Security Council and The Use of Force. Brill Academic Publishers.

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel. (2012). The Law of Cyber Attack. California Law Review. 100(4).

Paul Bracken. (2017). Cyberwar and Its Strategic Context. Georgetown Journal of International Affairs. 1(3).

Peter Berkowitz. (2011). Future Challenges in National Security and Law. California: Hoover Institution

Quinta Jurecic, 2018, "Where in the World is Elena Khusyaynova?", https://www.lawfareblog.com/where-world-elena-khusyaynova accessed on 31 August 2020 at 14:30 p.m. Damien McGunniess, "How a Cyber-attack Transformed Estonia", https://www.bbc.com/news/39655415, accessed on 3 March 2020 at 1:15 p.m.

R. Vark. (2006). State Responsibility for Private Armed Groups in the Context of Terrorism. Juridica International. 11(1).

Rain Liivoja. (2015). Technological Change and the Evolution of the Law of War. International Review of the Red Cross. 97(900).

Rebecca Crootof. (2018). International Cybertorts: Expanding State Accountability in Cyberspace. Cornell Law Review. 103(3).

Richard A. Gabriel and Karen S, Metz. (1992). A Short History of War: The Evolution of Warfare and Weapons. Pennsylvania: Strategic Studies Institute U.S Army War College Carlisle Barracks.

Robert A. Markus. (1983). Saint Augustine's Views on the Just War. Studies in Church

History. 20 (104).
Robert Drews. (1993). The End of the Bronze Age: Changes in Warfare and the Catastrophe Ca. 1200 B.C. New Jersey: Princeton University Press.
Robert W. Coakley and Stetson Conn. (2010). The War of American Revolution. Washington D.C: Center of Military History United States Army.
Spencer C. Tucker. (2015). Instrument of War: Weapons and Technologies that Have Changed History. Santa Barbara: ABC-CLIO.
Stephen Bull. (2002). World War I Trench Warfare. Oxford: Osprey Publishing.
Stephen C. Neff. (2005). War and the Law of Nations: General History. Cambridge: Cambridge University Press.
Susan W. Brenner. (2014). Cyber Threats and the Decline of the Nation-State. New York: Routledge
Statista, "Numbers of Internet Users Worldwide", https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ accessed on 20 February 2020 at 8:45 p.m.
Thomas Newdick. (2015). The World's Greatest Military Aircraft: An Illustrated History. United Kingdom: Amber Books Ltd.
United Nations Charter
Universal Declaration of Human Rights
U.S Department of Justice, "Russian National Charged with Interfering in U.S. Political System", https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system, accessed on 3 March 2020 at 5:15 p.m.
US Department of Defense. (2006). The National Military Strategy for Cyberspace Operations.
Yoram Dinstein. (2005). War, Aggression and Self-Defence. Cambridge: Cambridge University Press 4th Edition.
Vienna Convention on Diplomatic Relations.
Vincent Bernard. (2015). Tactics, Techniques, Tragedies: A Humanitarian Perspective on the Changing Face of War. International Review of the Red Cross. 97(900).

Submitted:
Published: