The Challenge of Cyber Attacks in the "Information Age" and *the Jus Ad Bellum*

Pshtiwan Mohammed Qader
Department of Law, College of Law, University of Sulaimani, Sulaimani, Kurdistan Region – F.R. Iraq

***Abstract*—The present paper examines the problem of cyber-attacks under existing international law. It takes the view that the (United Nations) UN Charter provisions on the use of force can be extended to cyber-attacks by means of interpretation although the relevant provisions do not explicitly address such issue. This Article argues that cyber-attacks resulting in material damage or destruction to property, death or injury to persons, or severe disruption of the functioning of critical infrastructures can be characterized as use of armed force and therefore violate the prohibition contained in article 2(4) of the Charter. However, cyber-attacks not resulting in the above consequences may be illegal intervention in the internal affairs of other states if such attacks are coercive in nature. In addition, the current study discusses that a cyber-attack which amounts to a use of armed force per se is not sufficient to give the victim state the right to self-defense, unless its scale and effects are equivalent to those of a conventional armed attack. Finally, the study concludes that an international cyber treaty is truly necessary to more effectively address cyber-attacks.**

***Index Terms*—International Law, Cyber Attack, Use of Force, Self-defense, Armed Attack.**

I. INTRODUCTION

Modern societies have become highly dependent on computers and internet connections to accomplish their tasks. Hostile actors, however, attempt to attack computer servers and the information that they hold. This kind of operation is known as cyber-attack.

Legal scholars can study the issue of cyber-attacks from the *jus ad bellum* perspective, that body of international law regulating the recourse to force by states. The present study discusses the use of the cyber-attacks by states against other states. It does not address cyber-attacks that occur below the level of use of force such as cyber terrorism, cybercrimes, or cyber-attacks committed by individuals or "hacktivist" groups.

Despite the fact that cyber-attacks have not so far played a major part in any larger conflict, many cyber-attacks have drawn state's attention to the subject lately, for example, cyber-attacks against Estonia in 2007 and Georgia during its war with the Russian Federation in 2008, as well as cyber incidents such as targeting the Iranian nuclear facilities with the Stuxnet worm in 2010 (Tallinn Manual on the International Law Applicable to Cyber Warfare, 2010, 2). The UK, for example, considered "hostile attacks upon UK cyber space by other states and large scale cybercrime" as one of four "Tier one" to British national security in its 2010 National Security Strategy (HM Government, 2010, Part III). The 2010 US National Security Strategy as well characterizes cyber security threats as one of the most national security, public, safety and economic challenges they face as a nation (White house, 2010, 27). Similarly, NATO acknowledges the new threat and commits itself in its new Strategic Concept to develop further their ability "to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities" (NATO, 2010, para 19).

This article, firstly, examines whether the existing law on the use of force that apply to traditional uses of force applies to cyber issues as well. Secondly, it argues whether cyber-attacks fall under the prohibition of the threat and the use of force contained in Article 2(4) of the UN Charter. Then, it examines whether such attacks amount to 'armed attack' in the sense of Article 51. Finally, the study discusses the available remedies against cyber-attacks short of armed attack.

Journal of University of Human Development
Volume 5 No. 2(2019); DOI: 10.21928/juhd.v5n2y2019.pp79-89
Regular research paper: Received 20 April 2019; Accepted 29 May 2019; Published 11 June 2019
Corresponding author's e-mail: pshtiwan.qader@univsul.edu.iq

II. THE CONCEPT OF CYBER ATTACKS

There is no universally accepted definition of cyber-attack. The term cyber-attack is often used interchangeably with the terms cyber operation and Computer Network Attack (CNA) in literature. Cyber-attack is defined by the US government as "a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions" (Joint Terminology for Cyberspace Operations, 2010, 5). According to the Tallinn Manual on the International Law Applicable to Cyber Warfare, it is "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Tallinn Manual, 2010, Rule 30). In addition, one of the most widely cited definitions comes from government security expert Richard A. Clarke, who defines cyber-attack as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." (Hathaway, Crootof, Levit, Nix, Nowlan, Perdue and Spiegel, 2012, 823). This definition is, however, narrow because it only covers cyber-attacks carried out by states, thereby excluding attacks initiated by non-state actors.

It should be noted that cyber-attack is distinct from computer network exploitation (CNE) in the US documents. The latter is defined as a set of "enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks" (National Military Strategy for Cyberspace Operations, 2006, GL–1). The Joint Terminology for Cyberspace Operations adds that CNE must occur "through the use of computer networks" (Joint Terminology for Cyberspace Operations, 2010, 4).

Even though they are often labeled in the media as cyber-attacks, "the primary technical difference between cyber-attack and cyber exploitation is in the nature of the payload to be executed. A cyber-attack payload is destructive on the other hands a cyber-exploitation payload acquires information non-destructively" (Lin, 2010, 64). For instance, CNE can be used for propaganda purposes or be aimed at stealing sensitive information from websites and computers without damaging the information that they hold (Eriksen, 2015, 3) whereas cyber-attacks can be directed against websites and computers to alter, delete or deny access to computer data.

III. APPLICABILITY OF THE EXISTING *JUS AD BELLUM* RULES

A. The applicability of existing treaties to cyber-attacks conducted by states

International conventions are one of the most important sources of international law. Although there is no international treaty that directly addresses cyber activities in the context of military operations, the lack of prohibitive rules in international law does not mean that states can initiate cyber-attacks against other states without restrictions. The view according to which the "absence of a legal prohibition . . . constitutes the presence of a legal permission" (Stone , 1959, 36) has come under criticism for reflecting an old, tired view of international law (Kosovo Advisory Opinion [2010] ICJ Rep. p 403, Declaration of Judge Simma, para 2).

In the absence of ad hoc provisions, the question is whether existing treaties, in particular, the UN Charter rules on the use of force which apply to traditional uses of force can be applied to cyber-attacks while the Charter rules do not refer to cyber issues. International lawyers are not united on this matter. For instance, Jeffrey Addicott disagrees over the whole idea of applicability of *jus ad bellum* to the cyber warfare. He points out that international laws related to the use of force are insufficient to address the threat of cyber warfare (2010, 550). However, it can be said the Charter's rule on the use of force can be extended to cyber-attacks launched by states against other states by means of interpretation. The ICJ in its Advisory Opinion on *the Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa)* states that "an international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation" (at para 53). The concept of dynamic, or evolving interpretation, which is implemented in Article 31 para 3 (b) of Vienna Convention on the Law of Treaties (VCLT), was used by the Court in a subsequent ruling, (Eriksen, 2015, 7) where it stated that "where parties have used generic terms in a treaty, the parties necessarily having been aware that the meaning of the terms was likely to evolve over time, and where the treaty has been entered for a very long period or is of continuing duration, the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning" *(Costa Rica v Nicaragua* [2009] ICJ Reports, para 66). Therefore, based on the Court's ruling, the UN Charter's terms "use of force" and "armed attack" must be interpreted in the light of present-day conditions as modern societies have become heavily dependent on technology.

An "interpretive reorientation" of existing *jus ad bellum* rules to accommodate cyber technology finds support in the fact that many states and organizations like Australia, China, Cuba, the European Union, Hungary, Iran, Italy, Mali, the Netherlands, Qatar, the Russian Federation, and the UK have emphasized the application of the *lex lata* (the law as it exists), including the UN Charter to cyber-attacks (Roscini, 2014, 21). In his speech at CYBERCOM, the State Department's Legal Advisor points out that established principles of international law do apply in cyberspace (Koh, 2012). Likewise, when submitting its views to the UN Secretary General on information security, the US provides that "despite the unique attributes of information and communications technologies, existing principles of international law serve as the appropriate framework within which to identify and analyze the rules and norms of behavior that should govern the use of cyberspace in connection with hostilities" (UNGA Doc. A/66/152, 2011, 18). Furthermore, in their report in 2013, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security concluded that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT (Information and Communications Technologies) environment" (UNGA Doc. A/68/98, 2013, 2). Although the creators of the Charter could not have foreseen the possibility of cyber-attacks and its rules are conceived around kinetic principles, this does not mean that this instrument is unfit to face the new threats as it has been demonstrated above.

B. The role of customary international law

Legal scholars have different opinions regarding the applicability of existing *jus ad bellum* customary rules to cyber-attacks. On the one hand, commentator like Moore (2013, 234) believes that there is a growing tendency among western legal scholars and nations that customary international law is applicable to cyber-attacks. Moreover, Roscini (2014, 25) argues that "existing *jus ad bellum* customary rules extend to cyber-attacks that constitutes to a use of force or acts of hostilities". He explains that state practice (*usus*) as an element of custom includes not only physical acts of states, but it also constitutes of verbal acts such as official statements made by states especially those in debates in the UN bodies and national legal advisers' opinions. He considered the US State Department Legal Advisor's (Harold Koh) speech at the US CYBERCOM on international law in cyberspace and the UN member states' speech on information security while submitting their views to the Secretary-General as valuable examples of verbal acts. (Ibid 28). He further explains that military manuals are also an important element of state practice and agrees with Garraway (2004, 431) that national manuals provide evidence of state practice and *opinio juris* regarding the states by which they are issued.

On the other hand, other groups of scholars have argued that no customary international law has yet developed because the phenomenon is still too recent and there is no state practice. Schmitt (1999, 921) concludes that "a customary norm may develop over time, but it does not exist at present. Neither practice, nor *opinio juris*, is in evidence". Similarly, the group of experts in the *Tallinn Manual* (2010, 19) point out that "because State cyber practice and publicly available expressions of *opinio juris* are sparse, it is sometimes difficult to definitively conclude that any cyber-specific customary international law norm exists". The author agrees with the latter group of scholars because states have not dealt with cyber issue long enough for state practice to be established and no cyber-attacks have clearly attributed to any states yet.

Indeed, state practice must be extensive and virtually uniform (*North Sea Continental Shelf*, [1969] ICJ Reports, para.74). Statements and documents on the legality of military cyber-attacks come from limited number of states. It is noteworthy that most military manuals issued before 2000 and for this reason they do not specifically refer to military cyber-attacks except the British Manual of the Law of Armed Conflict (UK Ministry of Defence, 2004, 188) and the US Commander's Handbook on the Law of Naval Operations (US Department of Navy , 2017, p.8-20). It seems that the current position demands fulfillment of state practice and *opinio juris*. Therefore, it is hard to say that customary international law specific to cyber-attacks has already generated based on a few unattributed cyber-attacks and a limited number of military manuals.

IV. EXAMPLES OF CYBER ATTACKS

A. Estonia (2007)

In April 2007, the Estonian government moved a statue of a Russian soldier (known as the Bronze Soldier) from Tallinn to its suburbs. As a result, hackers began attacking the websites of the government, Estonia's biggest bank and several newspapers in the country by using large botnets which is a collection of high jacked computers that can be used without

the knowledge of the owner. The attacks were called Distributed Denial of Service (DDoS) attacks. The attacks were mainly launched from 178 different countries. At first, the attacks were simple, ineptly coordinated and easily mitigated. However, the DDoS attacks quickly became far more organized and sophisticated (Buchan, 2012, 218). The hackers hijacked approximately 85000 computers from all around the world to carry out the attacks, but experts have established that the computers initiating the attacks had Russian IP addresses. Russia has denied any involvement and no definite attribution has ever been made, but Estonia maintained that Russia was responsible for the attacks (Holmberg, 2015, 6).

B. Stuxnet (2010)

In 2010, Iranian nuclear centrifuges were infected by a computer worm named Stuxnet, with the alleged ultimate purpose of sabotaging the gas centrifuges at the Natanz uranium enrichment facility. The virus caused the nuclear centrifuges to spin far more rapidly than they should and then to drastically decrease. Therefore, it harmed the centrifuges. The Iranian government has not revealed specific details concerning the impact of the Stuxnet virus, including physical damage, but several hundred centrifuges were shut down (Ibid). The Iranian President admitted at 2010 press conference that the attack caused problems for their centrifuges with the software which was installed in electronic parts (Mousavian, 2012, 25). Although the exact consequences of the incident are still the object of debate, the International Atomic Energy Agency reported that Iran stopped feeding uranium into thousands of centrifuges at Natanz. According to the reports this damage set back Iran's aspirations to enrich uranium by up to two years (Buchan, 2012, 220). It was alleged that the perpetrators are Israel and the US, but it has never confirmed.

V. Cyber-attacks and the Prohibition of the Threat and Use of Force in International Relations

According to Article 2(4) of the UN Charter "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations". Certain conditions must be fulfilled to invoke applying Article 2(4) and its customary counterpart to cyber-attacks. Firstly, the cyber-attack must reach to the level of a "threat" or a "use of force". Secondly, the attack needs to be attributed to a state, not private individuals or armed groups. Finally, the cyber-attack must be initiated by a state against another state.

A. Cyber-attacks as a "Use of Force"

Article 2(4) bans the threat and the use of force, but the exact definition of what constitutes the use of force is still unclear. A starting point to establish the meaning of "force" must be the VCLT which provides the rules of treaty interpretation. Although it has been adopted after the UN Charter, international law experts generally agree that the Convention's rules reflect customary international law (Gervais, 2012, 536). Article 31 (1) of the Convention states that "a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose" (UN Charter 1945, Article 31(1).

Indeed, *Black's Law Dictionary* defines "force" as "power, violence, or pressure directed against a person or thing" (*Black's Law Dictionary*, 2009, 717). Therefore, the ordinary meaning of "force" could be extended beyond armed force to include economic and political pressures.

A closer examination of the Charter and its *travaux préparatoires*, however, lead to the result that the expression "force", within Article 2(4) is limited to "armed" force only. In light of the "object and purpose" of the Charter, "force" should be read more narrowly. The primary purpose of the UN is to maintain international peace and security (UN Charter, Article 1 (1). This means that the notion of "force" is limited to traditional use of force. The drafting history of the Charter reinforces this conclusion. At the San Francisco Conference, a Brazilian amendment prohibiting "the threat or use of economic measures" was vetoed. Likewise, the expression "armed forces" is specifically used in some points of the Charter such as the Preamble, Articles 41 and 46. In light of these observations, it seems that force means military armed force, not other forms of coercion. The General Assembly resolution 2625 (XXV) of 24 October 1970, which is also known as Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations and Resolution 3314 (XXIX) of 14 December 1974, on the Definition of Aggression point to interpreting Article 2(4) as banning the use of "armed" force.

It is also important to inquire into the meaning of "armed" force so as to determine whether cyber-attacks can be regarded as a use of "armed" force. *Black's Law Dictionary* defines

"armed" as meaning "equipped with a weapon" or "involving the use of a weapon" (*Black's Law Dictionary,* 2009, 123). A weapon is "an instrument used or designed to be used to injure or kill someone" (Ibid 1730). Roscini (2010, 106) believes that almost every object can be used as a weapon, if the intention of the holder is hostile.

In light of the discussion above, it appears that a use of armed force under Article 2(4) requires weapons. Now, the question is can malware be classified as a weapon? The ICJ in its Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons* ruled that the UN Charter provisions on the use of force apply to any use of force regardless of the weapons employed (*Nuclear Weapons Advisory Opinion* [1996] para. 39). Zemanek (2012, 599) believes that 'it is neither the designation of a device, nor its normal use, which make it a weapon but the intent with which it is used and its effect. The use of any device or number of devices, which results in a considerable loss of life and or extensive destruction of property must therefore de deemed to fulfill the conditions of an armed attack". The Security Council Resolutions 1368 and 1373 reaffirmed this conclusion by authorizing the US to respond forcefully in self-defense to 9/11 attacks where the weapons used in the attack were hijacked airplanes (SC Res. 1368, 2001 and SC Res. 1373, 2001).

Roscini (2010, 106) argues that there is no reason why weapons should necessarily have explosive effects or be created for explosive purposes solely. The use of biological and chemical weapons (non-kinetic weapons) against a state would certainly be characterized as a use of force by the victim state in the sense of Article 2(4). In fact, in the judgment on the merits of the Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v US*) *(Nicaragua case)* the ICJ qualified the arming and training of armed groups by the US as a use of force against Nicaragua *(Nicaragua case* para.228). This means that the Court implicitly recognized that the use of non-kinetic force can lead to a violation of Article 2(4).

The 1969 VCLT supports an interpretation of Article 2(4) which covers cyber-attacks as explained above. Article 31 para 3(b) of VCLT provides that treaties shall be interpreted taking into account "any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation". Many states have stated that cyber-attack is a type of armed force, including the UK, the US, Kuba, Panama, Kazakhstan, Belarus and Russia. The UK under-secretary for security and counter-terrorism, for instance, declared that a cyber-attack that takes out a power station would be an act of war (The Guardian, 2010).

The notion of force is also covers indirect use of force which refers to situations where a state allows its territory to be used for violent attacks against a third state as well as a state's participation in the use of force by unofficial bands organized in a military manner (Klamberg, 2017, 197). However, according to the ICJ not every form of assistance is amount to the use of force. The Court in the *Nicaragua* case cited that the financing of guerrillas engaged in prohibited activity against another state was not a use of force (*Nicaragua case* para.228). The authors of the *Tallinn Manual* also believe that merely funding a hacktivist group carrying out cyber-attacks as part of an insurgency would not amount to the use of force (Tallinn Manual, Rule 11. para.3). By contrast, supplying malware to an organized group conducting cyber-attacks against another state and the training of such group would qualify as a use of force if the attacks conducted reaching to the level of a use of force (Ibid Rule 11. para.4).

B. Leading Approaches to Use of Force

Whether cyber-attacks fall within the scope of Article 2(4) depends on understanding the nature of a use of armed force. Three leading approaches have emerged in this regard.

According to the instrument-based approach, cyber-attack alone will almost never qualify as "armed" force because "it lacks the physical characteristics traditionally associated with military coercion" (Hollis, 2007, 1041). This view has been criticized because even when cyber-attacks result in physical damage, it cannot be qualified as a use of force under Article 2(4) (Waxman, 2013, 111).The advantage of this approach is, however, the simplicity of application, since uses of military weapons and force are relatively easy to identify.

The target-based approach holds that cyber-attack amounts to a use of armed force whenever it penetrates national critical infrastructure (NCI) system, even in the absent significant destruction or casualties (Klamberg, 2017, 196). The flaw in this approach is that it is too broad and cyber-attack will be qualified as use of armed force under this approach if it only causes inconvenience or merely aim to collect information (Eriksen, 2015, 22). In addition, this approach increases the likelihood that cyber-conflicts will escalate into more destructive conventional armed conflicts. A cyber-attack need only penetrate a critical system to justify a conventional military response that could start a physical, kinetic war. This approach could undermine the security of the international community by making war much more likely. Another

problem with this view is that there is still no official definition of NCIs which may lead to different practice by states.

Finally, the effects -based approach classifies a cyber-attack as an armed force whenever it intends to cause effects equivalent to those produced by kinetic weapon (death or destruction of property). Under this view, economic or social damage taking down the stock market or bringing transportation systems to a halt or covert actions such as influencing elections or planting information would likely not be as an action justifying a use of force in response (Hathaway et al, 2012, 847). By contrast, a cyber-attack that causes a meltdown in a nuclear power station, or one that disabled air traffic control resulting in airplane crashes, or opening the floodgates of a dam above a densely populated area could rise to the level of the use of armed force. The US Department of Defense has favored this approach by holding that the international communities will more likely focus on the results of a cyber-attack than on its mechanism (US Department of Defense, 1999, 18). In addition to this, the State Department's Legal Advisor, Harold Koh, argues that "if the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force" (Koh, 2012).

This view has also been criticized because "modern society`s heavy reliance on interconnected information systems means that the indirect and secondary effects of cyber-attacks may be much more consequential than the direct and immediate ones" (Waxman, 2011, 445). In addition, most cyber-attacks do not directly cause physical damage or death. A cyber-attack that temporarily shuts down the communication lines for emergency police and ambulance services, for instance, may not cause physical damage or deaths directly, but it could easily cause both indirectly. Drawing the line between direct and indirect consequences of a cyber-attack is extremely difficult (Gervais, 2012, 539).

Aware of this problem, Michael Schmitt, the proponent of the effects-based approach develops six criteria to distinguish cyber-attacks from other forms of coercion not amounting to the use of armed force which include: 1-severity: the degree of physical injury or property damage, 2-immediacy: how quickly the negative consequences manifest, 3-directness: the proximity of the act and its consequences, 4-invasiveness: the extent of territorial penetration, 5-measurability: to what extent the consequences can be quantified, and 6- presumptive legitimacy: whether the act is presumed valid (Schmitt, 1999, 914-15).

Schmitt's criteria, however, are not without problems. Directness, for example, is not necessarily an inherent characteristic of the use of armed force (Roscini, 2014, 48). The Definition of Aggression considers actions which do not necessarily entail direct destructive effects, including the violation of a stationing agreement, a naval blockade, and allowing the use of the territory by other states for the purpose of perpetrating aggression as an "act of aggression" (UNGA Res. 3314 (XXIX), Article 3 (c), (e) and (f). The ICJ in the *Nicaragua* case qualified the arming and training of armed groups (not directly destructive actions) as a use of force (*Nicaragua* case para.228). Similarly, these criteria are illuminating; they call for such a wide-ranging inquiry that they may not provide sufficient guidance to decision makers. As Silver (2002, 89), former General Counsel of the CIA, points out the wide ranging criteria allow for broad interpretation to whichever direction wanted.

As it has already been noted, the effects based approach is not without problems. Therefore, the author of this article agrees with the authors of the *Tallinn Manual* that focus on "scale and effects" as well to be an equally useful approach when distinguishing acts that qualify as uses of force from those that do not (Tallinn Manual, 47). Rule 11 of the Manual provides that a cyber-attacks amounts to a use of force when its scale and effects are comparable to non-cyber-attacks reaching to the level of a use of force (Ibid Rule 11).

The phrase "scale and effects" is derived from the *Nicaragua* Judgment, where the ICJ distinguished between an armed attack and a mere frontier incident (*Nicaragua* case para.195). In light of this, disruptive cyber-attacks that severely incapacitate the function of critical infrastructures fall under the scope of Article 2(4) if the incapacitation or disruption caused is significant enough to affect the welfare of the nation or national security, public safety and national economic security (Roscini, 2014, 55). If the targeted infrastructure is not critical, it is very unlikely that the consequent disruption will affect a state's essential functions or its internal public order.

There is, however, no agreement on the notion of "critical infrastructure". But it has been defined by the 2010 US *Joint Terminology for Cyberspace Operations* (2010, 5) as "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety,

environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction".

C. Cyber-attacks Below the Level of the Use of Force

Cyber-attacks conducted by states, but falling below the level of the use of force such as cyber-attacks seriously incapacitate of non-critical infrastructure or non-seriously disruptive cyber-attacks can be considered as unlawful on the base of violations of the customary principle of non-intervention in the internal affairs of other states if they are accompanied by an intention to coerce the target state in relation to a matter that it is freely entitled to determine. According to the International Group of Experts "non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy does not amount to the use of force (Tallinn Manual, Rule 11, para 3). The cyber-attack against Estonia in 2007 provides a good example in this regard. But cyber exploitation operations lacking a coercive element nevertheless do not *per se* violate the prohibition of the use of force or even the non-intervention principle. It may constitute a violation of the principle of territorial sovereignty when they target cyber infrastructures (governmental or private) of the targeted state (Heinegg, 2013, 129).

VI. CYBER-ATTACKS AND LAW OF SELF-DEFENSE

A. The Difference among "Force", "Aggression" and "Armed Attack"

Article 51 of the UN Charter provides that "nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations". This terminology suggests that there exists a gap between the notions "use of force" and the "armed attack". In fact, the scope of article 2(4) is wider than that of article 51 because it does not only prohibit armed force, but also unarmed, indirect use of force and the threat of force as well. This means that not every use of force contrary to article 2(4) will trigger the right of self-defense. The responding state must have suffered an "armed attack" (Melzer, 2011, 11). The gap has been confirmed by ICJ in the *Nicaragua* case when the Court distinguished "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms" (at para.191). This was also reaffirmed in the *Oil Platforms* case *(Iran v US)* (at para. 51).

The distinction between "use of force" and "armed attack" is made mainly due to the gravity of the act or of its effects. Brownlie (1963, 366) believes that a use of force must attain certain gravity in order to be defined as an armed attack. In addition, during the preparatory work aiming at defining aggression, numerous states stressed that only the most serious uses of force qualified as armed attack (Ruys, 2010, 150). Thus, an armed attack under Article 51 requires "a relatively large scale,...a sufficient gravity, and….a substantial effect" (Randelzhofer & Nolte, 2013, 1041).

Just as not all "uses of force" are "armed attacks", not all aggressions are armed attacks as well. Article 1 of the Definition of Aggression provides that "aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition" (UN Doc. A/RES/29/3314 (XXIX), Article 1). It is widely accepted that armed attack constitutes a part of aggression. Only most violent and gravest forms of aggression qualify as armed attack justifying the use of force in self-defense (Kittrich, 32, 2008). According to the Definition of Aggression Resolution, aggression includes not armed attack, but also other modes of the use of force such as ports or coasts blockaded and allowing one's territory to be used for perpetrating an act of aggression against a third state (Ibid Article 3 (c) & (f). If this is applied in the cyber context, it seems that that simply cuts off a country from the internet, without causing physical damage or severe incapacitation of essential services, would not reach to the level of an armed attack. Similarly, the action of a state in allowing another state to use its cyber infrastructure so as to initiate cyber-attacks amounting to an act of aggression against a third state would violate the prohibition of the use of force, but it does not constitute *per se* an armed attack (Ibid Article 3 (f).

B. Cyber-attacks as "Armed Attacks"

On the one hand, some scholars argue that any use of force by regular armed forces amount a *per se* to armed attack. According to this view, any offensive action by a military cyber unit is an armed attack because it emanates from the armed forces of a state. Thus, it triggers the right to exercise individual or collective self-defense. On the other hand, other scholars argue that the ICJ's "scale and effects" test is more appropriate to determine when Article 51 is triggered. (Gervais, 2012, 541).

Constantinou (2000, 63) has tried to specify this criterion by arguing that an armed attack is "an act or the beginning of a series of acts of armed force of considerable magnitude and intensity (i.e. scale) which have as their consequences (i.e. effects) the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental authority, i.e. its political independence, as well as damage to, or deprivation of its physical element namely, its territory" and the "use of force which is aimed at a State's main industrial and economic resources and which results in the substantial impairment of its economy". Therefore, the author of this article agrees with the latter group of scholars that it is both the "scale and the effects" of cyber-attacks which determine the occurrence of an armed attack. A large-scale cyber-attack, for example, that shuts down NCIs like the financial market for a prolonged time and cripples a state's economy or causes the collapse of the national currency would, if the effects are serious enough, potentially constitutes an armed attack for the purpose of self-defense (Roscini, 2014, 74). The US Department of Defense's *Assessment of International Legal Issues in Information Operations* points out that "if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities . . . it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack" (US Department of Defense, 1999, 18). Likewise, the 2011 AIV/CAVV Report on Cyber Warfare conclusions of which have been endorsed by the Dutch government provides that "a serious, organized cyber-attack on essential functions of the state could conceivably be qualified as an "armed attack" within the meaning of article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state" (AIV/CAVV No 77, AIV/No 22 CAVV, 2011, 21). According to the report a disruption of banking transactions or the hindrance of government activity would not qualify as an armed attack. By contrast, a cyber-attack that targets the entire financial system or an attack on the entire military communication and command network that prevents the government from carrying out essential tasks could well be equated with an armed attack (Ibid 21). In light of this, it seems a massive DDoS attack like the one occurred in Estonia that only disrupts NCIs for a limited amount of time is certainly significant with regard to its scale, but its effects are not. Furthermore, even though the exact impact of Stuxnet virus has never been concretely identified, it is likely that the attack against Iran was a use of force because the virus ended up causing material damage to centrifuges at Natanz. To conclude, not all cyber-attacks amounting to a use of force, not even those causing injury to persons or material damage to property, will automatically constitutes an armed attack. The destruction or disruption must be extensive enough to constitute a more serious use of force giving rise to the right of self-defense.

C. Necessity, proportionality, and immediacy of the Reaction in Self-defense

A victim state of a cyber-attack amounting to an armed attack may use armed force or cyber means in self-defense if (1) demonstrates that a cyber-attack occurred, (2) the attack meets the standards of armed attack and (3) it is attributed to another state or agents under that state's direct control (Janev and Aleksoski, 2013, 117). The use of force in self-defense is nevertheless not without restrictions; it must be "necessary" to repel the attack and "proportional" to the force used by the aggressor. The right to use of force in self-defense is further subject to a requirement of immediacy (Tallinn Manual, Rule 15). The ICJ has consistently confirmed the customary nature of the principles of necessity and proportionality (See *Nicaragua* case, para. 176 and *Oil Platforms case*, para. 76).

The principle of necessity requires that "force must be used only as a last resort, when peaceful means, such as a diplomatic settlement, cannot achieve the state's overall aim" while the principle of proportionality implicates that the means and extent of the self-defense needs to be proportionate in relation to the gravity of the armed attack (Hathaway et al, 2012, 849). Similarly, according to the immediacy requirement self-defense may not be undertaken to long after the armed attack but within some reasonable time after it occurred (Dinstein, 2005, 241).

However, applying the principles of necessity and proportionality to state responses to cyber-attacks is challenging. The cyber-attack has to be attributed to a state so as to evaluate the necessity of self-defense which is one of the greatest challenges when it comes to cyber-attacks. This is because of the difficulties of identifying the attacker and the modern technology makes it almost impossible to attribute a cyber-attack to a specific source to characterize the intent behind (Holmberg, 2015, 42). Likewise, assessing whether an invocation of self-defense complies with proportionality requirement is hard because the amount of damage especially indirect one caused by cyber-attacks is hard to estimate in

monetary categories (Hathaway et al, 2012, 849) because the private sector might be afraid to provide exact data on the damage suffered due to business confidentiality (Tikk, 2008, 17).

VII. Remedies against Cyber Attacks Short of Armed Attack

A. Resorts to the UN Security Council

The victim state of a cyber-attack may bring any situation to the attention of the Security Council under Article 35 (1) of the UN Charter and the Council might recommend the appropriate procedures or methods to solve the dispute (UN Charter, Articles 35 (1) & 36 (1). This would only be possible when the attack is attributed to a state. According to Article 39 of the Charter if the Council decides that the situation constitutes a threat to the peace, breach of the peace, or act of aggression, it could use its power under Chapter VII to maintain or restore international peace and security (Ibid Article 39).

B. Retortions and Countermeasures

The injured state of a cyber-attack under the threshold of armed attack may resort to retortion and non-forcible countermeasures against the responsible state. Retortion is "unfriendly" conduct which is not incompatible with any international obligation of the state engaging in it and can be adopted at any time such as withdrawal of voluntary aid programs whereas countermeasures counter measures are "measures that would otherwise be contrary to the international obligations of an injured state vis-à-vis the responsible State" which are carried out in a response to prior violation of international law by another state (ILC, 2001, 128).

Certain condition must be met to adopt countermeasures in response to cyber- attack below the level of armed attack. Firstly, countermeasures concern only non-forcible one and must be proportionate with the injury suffered. Secondly, they must be directed at the responsible state. Thirdly, they must be taken to procuring cessation of and reparation for the internationally wrongful act and not by way of punishment. Finally, they must comply with international law and the measure must be 'as far as possible' reversible (Ibid 129).

An injured state of a cyber-attack can resort to forcible countermeasures if the attack triggers the right to self-defense or the effects of the low-intensity cyber-attack can be accumulated with those of others to form a composite armed attack. This means that the victim state cannot retaliate by sending malicious code unless the cyber-attack is serious enough to constitute an armed attack. In fact, the foreseeable effects of the counter cyber-attack should be proportionate to those attacks. Achieving this, however, is hard because malware might spread uncontrollably once it is sent through cyberspace (Roscini, 2010, 114).

C. Resorts to an International Court

The victim state of a cyber-attack may bring the responsible state before an international court such as the ICJ so as to obtain reparation to redress the damages caused to its economy and civilians as a result of the violation of Article 2(4) of the UN Charter or the principle of non-intervention. However, it might be hard to quantify the amount of damage caused by a cyber-attack. This is because the private sector might be unwilling to providing the exact data on the kind and size damage occurred due to business confidentiality (Tikk, 2008, 17). Moreover, the ICJ and other international courts cannot hear any cases unless both states agreed to the Court's jurisdiction. In accordance with Article 96 of the UN Charter, the request of an Advisory Opinion of the ICJ on the legality of cyber-attacks would be another option. Such opinions are optional and non-binding, even though they might contribute to the formation of a customary international rule (Conforti, 2005, 276).

VIII. Conclusion

The present study reviews whether cyber-attacks can be regulated under the *jus ad bellum* rules. Some difficult questions arise when attempting to fit cyber-attacks within a warfare regime established well before the event of cyber technologies. Lack of ad hoc rules nevertheless does not mean that states can initiate cyber-attacks without restrictions. This study takes the view that the UN Charter rules on the use of force seem to be flexible enough to be extended to cyber-attacks even though the relevant rules do not expressly contemplate them. Of course, a cyber-attack is a use of armed force and encompassed in the prohibition in article 2(4) when causing physical damage or destruction to property, loss of life or injury to persons, or severe disruption of the functioning of critical infrastructures even if it does not materially damage them. Using the Stuxnet virus against Iran in 2010 is a good example in this regard. However, it is perfectly conceivable that cyber-attacks falls below the use of force if not resulting

in the above consequences, but this does not mean that such attacks are lawful. They may be unlawful intervention in the internal affairs of other states if they are coercive in nature, i.e. if they are accompanied by an intention to coerce the target state in relation to a matter that it is freely entitled to determine. The cyber-attack against Estonia in 2017 is a good example in this regard. By contrast, cyber exploitation to infiltrate information which lacks a coercive element may violate another state's sovereignty. Similarly, it is explained that a cyber-attack which amounts to a use of armed force *per se* is not sufficient to give the victim state the right of self-defense, unless it is serious enough to reach the "scale and effects" threshold of an armed attack.

It is also discussed that several remedies are at the victim state's disposal against a cyber-attack not amounting to an armed attack, including the adoption of acts of retortion, resort to the Security Council and non-forcible countermeasures, unless the attack triggers the right to self-defense or the effects of the low-intensity cyber-attack can be accumulated with those of others to form a composite armed attack. In the end, it can be said that an international cyber convention is truly crucial to govern cyber conflict between states. This is because it fosters international co-operation to counter threats resulting in cyber-attacks and empowers its ratifying parties to cooperate in evidence collection which facilitates identifying and punishing cyber aggressors. Moreover, providing a definition of cyber-attacks in such convention, it limits the cyber-attacks to which states may respond forcibly.

REFERENCES

Accordance with international law of the unilateral declaration of independence in respect of Kosovo [Advisory Opinion] [2010] ICJ Rep. Declaration of Judge Simma

Addicott, J. (2010). "Cyber-terrorism: Legal Policy Issues," in John Moore and Robert Turner (eds,) Legal Issues in the Struggle against Terrorism. Durham, NC: Carolina Academic Press

AIV/CAVV, (2011). Cyber Warfare, No 77, AIV/No 22 CAVV. Retrieved February 09, 2019, from https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

Brownlie, I. (1963). International Law and the Use of Force between States. New York & London: Oxford University Press.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? Journal of Conflict & Security Law, 17(2), 211-227. doi:10.1093/jcsl/krs014

Chairman of the Joint Chiefs of Staff (2006). National Military Strategy for Cyberspace Operations.

Conforti, B. (2005). The Law and Practice of the United Nations. Leiden-Boston: Martinus Nijhoff.

Constantinou, A. (2000). The Right of Self-defense under Customary International Law and Article 51 of the *UN Charter. Brussels: Bruylant.*

Dinstein, Y. (2005). War, aggression and self-defense (4th ed.). Cambridge: Cambridge University Press.

Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua), Judgment 13 July 2009, para 66.

Eriksen, T. (2015). 'When do cyber operations amount to use of force and armed attack, and what response will they justify?'. Retrieved March 15, 2019, fromhttps://www.duo.uio.no/bitstream/handle/10852/50840/723.pdf?sequence=1&isAllowed=y

Garner, B. A. (ed). (2009) Black's Law Dictionary (9th ed). St. Paul, MN: West.

Garraway, C. (2004). 'The Use and Abuse of Military Manuals', in McCormack, T. L., & McDonald, A. (ed) Yearbook of International Humanitarian Law. (Vol. 7). Hague: T.M.C. Asser Press.

Gervais, M. (2012). Cyber Attacks and the Laws of War. Berkeley Journal of International Law,30 (2), 525-579. doi:10.15779/Z38R66C

Hathaway, O. A. & Crootof, R. (2012). The Law of Cyber-Attack. California Law Review, 100, 3852nd ser., 817-885. Retrieved November 27, 2018, from https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4844&context=fss_papers.

Heinegg, W. H. (2013). Territorial Sovereignty and Neutrality in Cyberspace. *International Law Studies*, 89, 123-156. Retrieved January 11, 2019, from https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1027&context=ils.

HM Government, (2010). A Strong Britain in an Age of Uncertainty: The National Security Strategy

Hollis, D. B. (2007). 'Why states need an international law for information operations. LEWIS & CLARK LAW REVIEW, 11(4), 1023-1061. Retrieved October 18, 2018, from https://law.lclark.edu/live/files/9551-lcb114art7hollis.pdf.

Holmberg, E. J. (2015, Spring). Armed Attacks in Cyberspace. Retrieved February 20, 2019, from http://su.diva-portal.org/smash/get/diva2:854660/FULLTEXT01.pdf

International Group of Experts, (2010). Tallinn Manual on the International Law Applicable to Cyber Warfare, in Michael N. Schmitt(ed.) Cambridge: Cambridge University Press.

Janev, M. H., & Aleksoski, S. (2013). Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace. Mediterranean Journal of Social Sciences, 4(14), 115-124. doi:10.5901/mjss.2013.v4n14p115

Kittrich, J. (2008). The Right of Individual Self-Defense in Public International Law. Berlin: Logos Verlag Berlin GmbH.

Kilovaty, I. (2014). Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare. 5 American University National Security Law Brief, 5(1), 91-124. Retrieved January 28, 2019, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2695642.

Klamberg, M. (2017). 'Exploiting legal thresholds, fault-lines and gaps in the context of remote warfare, in Jens Ohlin (ed,) Research Handbook on Remote Warfare. Cheltenham: Edward Elgar.

Koh, H. (2012, September 19). International Law in Cyberspace. Retrieved October 14, 2018, from http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace

Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) [Advisory Opinion] [1971] ICJ Rep

Legality of the Threat or Use of Nuclear Weapons [Advisory Opinion] [1996] ICJ Rep

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. NATIONAL SECURITY LAW & POLICY, 4, 63-86. Retrieved December 09, 2018, from http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf

Melzer, N. (2011). Cyber warfare and International Law. UNDIR Resources

Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands & Directors of the Joint Staff Directorates, (2010). Joint Terminology for Cyberspace Operations

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US*) (Merits) [1986] ICJ Rep 14*

Moore, S. (2013). 'Cyber Attacks and the Beginnings of an International Cyber Treaty. NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW AND COMMERCIAL REGULATION, 39(1), 224-257. Retrieved January 18, 2019, from https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2016&context=ncilj.

Mousavian, S. H. (2012). The Iranian Nuclear Crisis: A Memoir. Washington DC: Brookings Institution Press

NATO, (2010). Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation. Retrieved December 23, 2018, from http://www.nato.int/cps/en/ natolive/official_texts_68580.htm

North Sea Continental Shelf, [1969] ICJ Rep

Oil Platforms (Iran v US) [2003] ICJ Rep

Randelzhofer, A & Nolte, G. (2013) 'Article 51' in Bruno Simma, Hermann Mosler, Andreas Paulus & EleniChaitidou (eds), The Charter of the United Nations: A Commentary (3rd ed.). Oxford: Oxford University Press

Report of the ILC, Fifty-third Session, UN Doc. A/56/10 (2001)

Roscini, M. (2010). "World Wide Warfare – Jus ad bellum and the Use of Cyber Force", in A von Bogdandy & R.Wolfrum (eds,) Max Planck YUNL (Vol. 14). Brill

Roscini, M. (2014). Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press

Ruys, T, (2010). Armed Attack and Article 51 of the UN Charter. Cambridge: Cambridge University Press.

Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, 37, 886-937. Retrieved March 02, 2019, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800.

Silver, D. (2002). 'Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter' International Law Studies, 57, 73-97. Retrieved November 11, 2018, from https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1398&context=ils

Stone, J. (1959). 'Non Liquet and the Function of Law in the International Community', BYIL (Vol. 35)

The Observer (2010), 'Britain fends off flood of foreign cyber-attacks'. Retrieved January 26, 2019, from http://www.theguardian.com/technology/2010/mar/07/britain-fends-off-cyber-attacks

Tikk, E. (2008). 'Cyber Attacks Against Georgia: Legal Lessons Identified' Retrieved December 29, 2018, from http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf

UK Ministry of Defence (2004). The Manual of the Law of Armed Conflict. Oxford: Oxford University Press

UN Charter 1945

UNGA Doc. A/66/152 (2011)

UNGA Doc. A/68/98 (2013)

UNGA Res. 3314 (XXIX) "Definition of Aggression" (14 December 1974)

UNSC Res. 1368 (2001)

UNSC Res. 1373 (2001)

US Department of Defense (1999), 'An Assessment of International Legal Issues in Information Operations'. Retrieved November, 14, 2018 from http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf

US Department of Navy (2017), The Commander's Handbook on the Law of Naval Operations. Retrieved September, 16, 2018 from http://www.jag.navy.mil/distrib/instructions/CDRs_HB_on_Law_of_Naval_Operations_AUG17.pdf

Vienna Convention on the Law of Treaties 1969

Waxman M, 'Cyber-attacks and the Use of Force: Back to the Future of Article 2(4)', 36 (2) Yale Journal of International Law

Waxman, M. C. (2013). 'Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions', International Law Studie, 89, 109-122. Retrieved November, 10, 2018 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2235838

White house (2010). National Security Strategy

Zemanek, K. (2012). 'Armed attack', Max Planck Encyclopedia of Public International Law.(Vol. I). Oxford: Oxford University Press