Scientific Research Publishing

Beijing Law Review, 2021, 12, 631-649
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Cyberattack and the Use of Force in International Law

Joseph N. Madubuike-Ekwe

Department of Public Law, Faculty of Law, Benson Idahosa University, Benin City, Nigeria
Email: jekwe@biu.edu.ng, josefa06@gmail.com

How to cite this paper: Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. *Beijing Law Review, 12,* 631-649.
https://doi.org/10.4236/blr.2021.122034

Received: September 11, 2020
Accepted: June 19, 2021
Published: June 22, 2021

Abstract

This article examines how the existing law of armed conflict may be applied or adapted to meet the challenges posed by cyber-attacks. It begins with a definition of cyber-attacks, cyberexploitation and cyberespionage and their differences. The article discusses how cyber-attacks are regulated by the existing body of laws such as the United Nations Charter, International humanitarian Law (IHL), international treaties and domestic laws. It notes that the existing law addresses only a small fraction of potential cyber-attacks. IHL, for example, provides a useful framework for a very small number of cyber-attack that amounts to an armed attack or that take place within the context of armed conflict. The article concludes that, since cyber-attacks are global in nature, there is need for a new international legal framework to more effectively deal with the challenges posed by cyber-attacks.

Keywords

Cyber-Attack, Cyberspace, IHL, International Law, Armed Conflict

1. Introduction

Most nations, particularly, developed nations are increasingly dependent on information and information technology for both civilian and military purposes. This provides opportunities for adversaries to strike inexpensively, remotely, and effectively with little risk (Gervais, 2012). Because of this, states and non-state actors turn to cyberspace to conduct warfare with greater frequency. Cyberwarfare allows combatants to fight from extreme distances which raise a number of ethical and moral considerations similar to the concerns raised in relation to those operating drones (Alston, 2010). Cyber-attackers are far from the battlefield. Being removed from the horrors of war, cyber-attackers risk becoming emotionally detached from the effects of their attacks, increasing the possibility of unneces-

sary harm, suffering and collateral damage.

The legality of cyber warfare remains unsettled. The International humanitarian law (IHL) has historically interpreted "armed conflict" in the context of conventional military weapons in order to respond proportionately and as necessary to stop the threat. Since modern technology has brought warfare into cyberspace, there is need to adapt international instruments such as the IHL to meet new challenges facing the world. Although opinion is divided as to how to apply IHL to cyber-attacks, recent events confirm that cyber warfare is operational (Gervais, 2012).

The aim of this article is to examine how the existing laws of armed conflict might be applied to cyber-attacks. The article is divided into five parts. Part I introduces the article. Part II discusses the meaning of cyber-attack, cyber espionage and cyber exploitation as well as the capabilities of cyber-attack. In examining the existing laws, Part III discusses cyber-attacks in the context of *jus ad bellum* on when a state may legitimately use force as an instrument of dispute resolution. Part IV examines the relationship between traditional *jus in bello* principles and cyber-attacks employed in the context of armed conflicts. Cyber-attacks pose serious challenges to *jus in bello* principles of military necessity, distinction, proportionality and neutrality. Part V concludes the article by recommending a new comprehensive international legal framework to effectively address cyber-attacks. The focus of this article is on cyber warfare in the context of International armed conflicts as distinguished from non-International armed conflicts. It does not, therefore, generally discuss the issue of cyber warfare in situations of non-international armed conflicts.

2. Defining Cyber Warfare

The term "cyberwar" is not an apt description for all the hostile actions in cyberspace because of the wide range of possible intended effects of an attack. As such, it will be more helpful to distinguish the two forms of hostile actions against a computer system or net work—Cyber-attacks and cyber exploitation (Lin, 2010).

Cyber-attack is destructive in nature. An example of such a hostile action is erasure by a computer virus resident on the hard disk of any infected computer. In this particle, "cyber-attack" refers to the use of deliberate actions and operations—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transmitting these systems or networks (NRC, 2009).

The US Department of defense has not defined cyberwarfare. But one workable definition of cyber-attack by the US Army's DCSINT Handbook NO1.02 is "the premeditated use of destructive activities, or the threat thereof, against computers and/or networks with the intention to cause harm or to further social, ideological, religious, political or similar objectives or to intimidate any person

in furtherance of such objectives" (DCSINT Handbook, 2006).

Such effects on adversary systems and networks may also have indirect effects on entities coupled to or reliant on them. A cyber-attack seeks to cause the adversary's computer systems and networks to be unavailable or untrustworthy and therefore less useful to the adversary.

By comparism, cyber exploitation is nondestructive. An example is a computer virus that searches the hard disk of any infected computer and emails to the hostile party all files containing a credit card number or confidential information. "Cyber exploitation" refers to the use of actions and operations, perhaps over an extended period of time, to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks. Cyber exploitations are usually clandestine and conducted with the smallest possible intervention that still allows extraction of information sought. They do not seek to disturb the normal functioning of a computer system or network from the user's point of view, and the best cyber exploitation is one that a user never notices (Lin, 2010). The goal of cyber exploitation is to obtain information from a computer network without the user's knowledge, which amounts to a modern form of espionage. Espionage is illegal under the domestic laws of most nations, but it is not illegal under international law (Roscini, 2010).

Throughout history, nation states have undertaken espionage by using agents to infiltrate and collect information about adversaries (Gervais, 2012). Cyber espionage is the "unauthorized probing of a target computer's configuration to evaluate its system defenses or the unauthorized viewing and copying of date files." (Ibid) It is a low-cost and low risk tool for State governments. Today, state governments now engage in intelligence and commercial espionage using the same techniques that cyber criminals utilize for gaining confidential information—such as malware, phishing and code injection. (Ibid)

The primary technical difference between cyberattack and cyber exploitation is in the nature of the payload to be executed—a cyber-attack payload is destructive whereas a cyber-exploitation payload acquires information nondestructively. In addition, because a cyber-exploitation should not be detected, the cyber operation involved must only minimally disturb the normal operating state of the computer involved. In other words, the intelligence collectors need to be able to maintain a clandestine presence on the adversary computer or network despite the fact that information exfiltrations provide the adversary with opportunities to discover that presence.

Cyber espionage and cyber exploitation does not rise to the level of warfare because the purpose or outcome of both cyber espionage and exploitation is to monitor information and not to affect a computer system's operation. Nonetheless, cyber espionage, like traditional espionage may violate any number of domestic laws or international agreements it does not violate International humanitarian Law (Gervais, 2012).

The Legal Framework

The International Humanitarian Law provides the primary legal framework within which to understand constraints on the use of offensive cyber operations. The IHL addresses two separate questions. First, when is it legal for one nation to use force against another? This body of law is known as *jus ad bellum*. Second, what are the rules that govern the behavior of combatants who are engaged in armed conflict? This body of law is known as *jus in bello*. It is separate and distinct from *jus ad bellum*.

3. Jus Ad Bellum

The question of how to apply IHL to cyber warfare can be addressed only after it is first determined that a state might legally use "force" in responding to what it perceives to be "cyber-attacks." This determination must be made in the context of *jus ad bellum*, those established "conflict management" norms and procedures that dictate when a state may- and may not—legitimately use force as an instrument of dispute resolution (Moore, 2005).

Jus ad bellum is governed by the United Nations Charter, interpretations of the Charter, and customary international law developed with and sometimes prior to the Charter (United Nations Charter, Arts. 2 (4), 39, and 51).

The terms, "use of force," "threat of force", or "armed attack" are not defined in the United Nations Charter. However, nations understand that certain unfriendly actions, including unfavorable trade decisions, space-based surveillance, boycotts, severance of diplomatic relations, denial of communications, espionage, economic competition or sanctions, and economic and political coercion do not rise to the level of a use of force, regardless of the scale of their effects. Armed attack may include declared war, occupation of territory, naval blockade, and the use of armed force against territory, military forces, or civilian abroad. However, there are no precedents for how offensive cyber operations should be regarded (Lin, 2010).

Although opinion is divided among international lawyers and jurists on the real meaning of Article 2 (4) of the UN Charter, The provision prohibits a state from either threatening or using "force" against another state in the international community. In Articles 39 and 42, the Charter contains only two exceptions to this prohibition on the use of force: actions authorized by the Security Council and acts of self-defense under Article 51 of The UN Charter.

1) Security Council Authorizations

The Security Council has power to authorize United Nations members to engage in both use of force and use of other measures against another state which is or is threatening to become an aggressor (UN Charter, Arts 41 and 42). However it can only do so only if it makes an article 39 determination that the actions of a state constitute a "threat to the peace, breach of the peace, or act of aggression." Extensive experience has shown, that Article 39 determinations and resultant use of force recommendations are exceptionally difficult to achieve (Gra-

ham, 2010). Most such decisions are arrived at only after extensive and time-consuming deliberations, and even then such decisions are subject to the veto of any permanent Security Council member (UN Charter, Art. 27). Accordingly, given the nebulous nature of cyber-attacks, and the uncertainty about whether the Security Council will respond to such attacks in a timely manner, it seems valid to assume that a state will choose to deal with cyber-attacks by exercising its right to self-defense.

2) Right of Self-Defense

A State's right to undertake self-defense measures is not one that was created by Article 51 of the U.N. Charter. The Charter merely reaffirmed this inherent customary international law (CIL) right of states to survive within the international community (ICJ Statute, Art. 38). While an analysis of the right of self-defense must look to both the provisions of Article 51 and CIL, there exists a firm international consensus on this very fundamental issue. Although several theories have always existed as to the types of state actions that actually constitute "armed attacks", a state unmistakably possesses both an inherent and Charter-derived right to engage in an "appropriate" self-defense response to such an attack (Graham, 2010).

The question is what is appropriate self-defense? A response is lawful if it complies with two main principles of CIL—"necessity" and "proportionality" (Wingfield, 2000). A State meets the requirement of necessity when it becomes evident that, under the prevailing circumstances, the state cannot achieve a reasonable settlement of a dispute through peaceful means. "Proportionality" requires that state limit self-defense actions to the amount of force required to defeat an ongoing attack or to deter a future attack. Compliance with this principle obviously depends on the particular factual situation.

Does a right to anticipatory or pre-emptive self-defense exists within the context of cyber-attacks? A long established tenet of customary international law, which dates back to 1836 *Caroline case,* in which a threatened state might lawfully resort to self-defense measures when the "necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment for deliberation" (Shaw, 2010). To exercise this right lawfully, a state needs to show that the anticipated attack was imminent. In the case of cyber-attacks, such a requirement would be difficult to meet, if not impossible (Graham, 2010).

For example, sophisticated cyber-attacks are designed to overwhelm a target state's computer systems instantaneously. There are, of course, cyber-attacks that a state might foresee and counteract. A state might discover evidence of a cyber-attacker's attempted network intrusion, an audit of computer systems might reveal unauthorized backdoors or malware, or targeted states might uncover an online forum that serves as a gathering place for hacktivists to trade information and tools prior to a coordinated attack. In such cases, the target state is previously aware of a planned cyber-attack and may invoke its right to respond in anticipatory self-defense if the *Caroline* test criteria are met (Gervais, 2012).

Where met, a state might lawfully disable the servers that host the online forum where cyber-attackers are gathering, assuming the state has no other means by which to forestall the imminent attack(s).

3) Does Cyber-attack constitute an armed attack?

When there is a conflict between nations, the U.N. Charter requires that members "settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered" (United Nations Charter, art 2 (3)). Thus the authority for a state's use of force originates either from the UN Security Council or by the State's right to act in individual or collective self-defense. The question is whether cyber-attack—or continuous series of cyber-attacks—can reach the threshold of "armed attack" that triggers the right to self-defense under article 51 of the Charter? Is there a difference between an "armed attack" under Article 51 and a "use of force" under Article 2 (4) of the U.N. Charter? The answer to these questions are not easy, because the term "armed attack" is not specifically defined by treaty or any other form of international agreement. However, the international framework for analyzing whether certain state actions constitute armed attacks has evolved over time, and these are the legal principles that must be applied in assessing the nature of cyber-attacks (Graham, 2010).

Generally, the international community agrees that the criteria put forward by Jean Pictet in order to determine the existence of an international armed conflict under common Article 2 of the 1949 Geneva Conventions should serve as a guide for assessing whether a particular use of force has risen to the level of an armed attack (Geneva Convention, 1949). Under this test, a use of force is deemed an armed attack when the force is of "sufficient scope, duration, and intensity" (Graham, 2010).

However, certain international instruments have evolved over the years that have facilitated the application of Pictet's criteria. Particularly the U.N. General Assembly's "Definition of Aggression" resolution in which Aggression is defined as "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" (U. N. Gen Ass Res. 3314 (XXIX), 1974). While this Resolution does not define armed attack, it provides examples of state actions that are deemed to qualify as such, and these have gained extensive international acceptance.

Although, these declarations in international instruments and decisions of the international courts are helpful in the context of assessing conventional uses of force (Nicar v. US), they are of minimal value in determining when cyber-attacks constitute armed attacks (Nicar v. US). This is because cyber weapons are versatile and can be either a supporting actor in the theater of conflict or the main event. They are not monolithic weapons whose use leads to straightforward answers about whether they violate the prohibition on force. Rather, the innumerable harmful effects caused by cyber-attacks makes their categorization both more

complex and more necessary. The effects of a cyber-attack can range from a simple inconvenience (such as a DDoS attack that disrupts web traffic temporarily), to physical destruction (such as changing the commands to an electrical power generator causing it to explode), and even to death (such as disrupting the emergency lines to first responders so that calls cannot be made to police or ambulance services). But treating all forms of cyber-attack as a use of force would require an implausibly broad reading of Article 2 (4) that includes non-physical damage (Gervais, 2012).

Additionally, the intensity and temporal scope of a cyber-attack can transform an event from a low-level aggressive act to a prohibited use of force. In *Armed Activities on the Territory of the Congo, (Dem. Rep. Congo v. Uganda)* the ICJ determined that a violation of Article 2 (4) resulted from the "magnitude and duration" of Uganda's actions. Therefore, the magnitude and duration of an attack are appropriate factors for consideration in any model that analyzes the coercive tactics employed by a state.

Furthermore, three distinct analytic models have recently been put forward to facilitate the application of Pictet's use of force criteria, scope, duration, and intensity, to unconventional force, including cyber-attacks.

Firstly, is an "instrument-based approach". Under this model, an assessment would be made as to whether the damage caused by a cyber-attack could previously have been achieved only by a kinetic attack. For example, using this model, a cyber-attack conducted for the purpose of shutting down a power grid would be deemed an armed attack. Why? Because prior to the development of cyber capabilities, the destruction of a power grid would typically have required bombing a power station or using some other form of kinetic force to achieve such result. Additionally, a cyber-attack is a use of force if the attacker seeks to cause direct physical destruction, injury, or death. This approach removes the need to examine the instrument of delivery, and it allows the international community to adapt the Charter to evolving technology while accounting for nuances in the intensity of a cyber-attack (Brownlie, 2012).

Secondly, is an "effects-based approach," often referred to as a consequence-based model? Under this approach, no attempt would be made to assess whether the damage resulting from a cyber-attack could previously have been achieved only through a kinetic use of force. Here consideration would be the overall effect of the cyber-attack on the victim state (Schmitt, 1999).

Thirdly, is "strict liability" model that would automatically deem any cyber-attack against critical national infrastructure (CNI) to be armed attack, based on the severe consequences that could result from any attack on such infrastructure systems?

Therefore, from the discussions so far, it is clear that cyber-attacks constitute armed attacks. As such, a state may use force in response to a cyber-attack as a legitimate exercise of the right of self-defense. Before exercising this right, there is need to establish the responsibility of another state for the cyber-attack.

4) State Responsibility

Before a state responds in self-defense, several factors must be considered. Firstly, whether the cyber-attack should be treated as a law enforcement matter or a national security matter. Relevant to this determination is whether the level of force used in the cyber-attack rises to that of an armed attack, as discussed above in Section III. Secondly, whether the state where the attack originated is complicit. If the act of self-defense is not in immediate response to an ongoing attack, the state must impute responsibility before launching its cross-border counter attack (Gervais, 2012). Establishing state responsibility in the area of cyber-attacks requires understanding state's duties to one another, particularly regarding non-state actors operating within their jurisdiction.

In 2001, the international law Commission adopted the Draft articles on State Responsibility, which articulates the international jurisprudence on state responsibility (The International Law Commission Commentary, 2001; Wallace & Martin-Ortega, 2013). Article 1 states that "every internationally wrongful act of a state entails the international responsibility of that state." This notion of state responsibility is supported by state practice as well as *opinion juris.* In the *Corfu Channel Case*, (*U.K. v. Albania*), the ICJ examined the threshold to attribute responsibility for actions within a state's borders. The ICJ held that territorial sovereignty is not only an essential foundation of international relations, but also that under customary international law, every state also has an obligation "not to allow knowingly its territory to be used for acts contrary to the rights of other states." This formulation, however does not take into account the subtleties in degree of state responsibility. Should a state be held internationally responsible for a single soldier or patriotic hacker that uses cyber-attack to destroy critical infrastructure of an adversary? (Gervais, 2012) The answer to this question require a brief discussion of state responsibility with regards to state actors and non-state actors.

a) State Actors

There is little controversy that if a state agent attacks another state, then the hostile conduct is attributable to the state. Article 4 of the Draft Articles on State Responsibility declares that "The conduct of any state organ shall be considered an act of that state under international law." A state organ includes all individual or collective entities that make up the organization of the state and act on its behalf.

This principle is a codification of customary international law. It reflects the assumption that a state is fully responsible for its agents—even when those agents act outside the scope of their duties. In *Armed Activities on the territory of the Congo*, (*Dem. Rep. of /Congo v. Uganda*) the ICJ held that "according to a well established rule of a customary nature … a party to an armed conflict shall be responsible for all acts by persons forming part of its armed forces." This rule also applies to a person or entity that is not an organ of the state but nevertheless exercises elements of governmental authority. This extends to private or public entities that a state may charge with elements of authority normally associated

with the government. For example, if the British government employs private defense companies and authorizes them to conduct active defense measures, the conduct of the private defense company is imputed to Britain (Gervais, 2012). As noted in Article 5 of the Draft Articles on State Responsibility, "If it is to be regarded as an act of state for purposes of international responsibility, the conduct of an entity must accordingly concern governmental activity and no other private or commercial activity in which the entity may engage." This position is consistent with the "effective control" test as stated by the ICJ in *Nicaragua v. U.S.* Similarly, a state may not coerce another state to do its bidding without accountability. Article 17 of the Draft Articles on State Responsibility holds a state internationally responsible for wrongful acts that "it directs and controls another state in the commission of," if the state exercising the direction and control does so knowingly. This is a reflection of the decision in the *Corfu Channel case* and its mandate that a state not knowingly allow an attack to originate from its territory. This is particularly important in the area of cyber-attacks because of their surreptitious and uncontrollable nature.

Because of the anonymity of the technology involved, attribution of a cyber-attack to a specific state may be difficult. While a victim state might ultimately succeed in tracing a cyber-attack to a specific server in another state, this can be an exceptionally time consuming process, and, even then, it may be impossible to definitively identify the entity or individual directing the attack (Jensen, 2002). For example the "attacker" might well have hijacked innocent systems and used these as "zombies" in conducting attacks (Graham, 2010). Because of these reasons, states acting on the perceived legal requirement that they must conclusively attribute a cyber-attack to another state or its agents historically have chosen to respond to cross-border cyber-attacks as they would to criminal matters, employing only "passive" (computer security) measures to and urging the states from which the attacks originated to investigate and prosecute those responsible. There is ample evidence, however that even the most sophisticated computer security measures cannot completely protect a state's critical systems (Graham, ibid). As a result, many states have consistently demonstrated a lack of desire to deal with cyber-attacks through effective law enforcement. They have already begun developing cyber units within their military or intelligence apparatuses, States have also delegated some elements of their cyber-attack capabilities to private sector. One state might even consider using another state to launch an attack on its behalf. Although tracing a cyber-attack is a formidable technical challenge, if the targeted state successfully traces a cyber-attack to source state's cyber unit or to an entity acting with the authority or under the control of the source state, the latter ought to be held responsible.

b) Non-State Actors

The question is whether, in both cyberspace and traditional warfare, it is appropriate to attribute state responsibility when non-state actors perpetrate an attack. Article 51 of the U.N. Charter does not provide guidance on whether a

state may respond with force to a non-state actor. Non-state actors usually hacktivists present a complicated issue for targeted states (Gervais, 2012).

Hacktivists are usually private citizens motivated by nationalistic or ideological feelings who possess sufficient skill to participate in a cyber-attack. The nature of cyber space permits hacktivists to launch attacks on another state from anywhere, at will, without government direction. Hacktivists freedom to engage in cyber-attacks from virtually anywhere in the world allows them to operate from the territory of a third party. Any action taken against a hacktivist in the territory of a third party state raises the questions about violating that state's sovereignty, as well as whether the third party state has certain rights and obligations. The Charter does not explicitly address this facet of international conflict, leaving a legal loophole that hacktivists may exploit (Gervais, 2012).

Nevertheless, international custom and practice demonstrate that states can, and do, respond with force to non-state actors. The international response to 9/11 attacks on the United States validated this principle of customary international law. After 9/11, the U.N. Security Council passed Resolution 1368, which reaffirmed the "inherent right" of the United States to respond in self-defense in accordance with article 51 of the U.N. Charter. Several weeks later, when it was clear that non-state actors had committed the 911 attacks, the United States still received nearly universal support, including from the Security Council, when it invoked its right to respond in self-defense (U.N. Security Council Res. 1373).

On what grounds should we attribute responsibility to a state for the actions of its non-state actors? If the state directs or controls the non-state actors regardless of whether the non-state actors are within its jurisdiction, there are several grounds for which to hold the state responsible. However, "lone wolf" hacktivists, those who act without endorsement of the state, present a more complicated problem (Gervais, 2012).

In line with the *Corfu Channel* decision, if a state may not knowingly allow its territory to be used for acts that violate another state's rights, then *mutatis mutandis* a state may not knowingly allow non-state actors within its borders to attack another state. Additionally, the Draft Articles on State responsibility augment the *Corfu Channel test* by imputing responsibility to a state if "the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that state in carrying out the conduct."

Thus in *Nicaragua v. U.S.*, the issue before the ICJ was whether the United Sates was responsible for the actions of the contra guerillas in their rebellion against the Nicaraguan government. The court held that to find the United States responsible would require "effective control" over the non-state actor group and the exercise of that control with respect to the specific operation in which breaches were committed. This implies that state control extends beyond its immediate territory. If a state is in "effective control of non-state actors operating in another territory, it may be held responsible for their actions.

On the other hand the International Criminal Tribunal for the former Yugos-

lavia (ICTY) articulated a lower "overall control "test in *Prosecutor v. Tadic* In that case, the tribunal stated that this standard "to some extent equates the group with state organs proper. The *Tadic* standard was applied only to participants in an organized and hierarchically structured group, such as a military or paramilitary force. An example of such a paramilitary group is the Russian Business Network, which is often associated with Russia's political and military elite, though not a formal participant. The Russian business Network was intimately involved in the cyber-attacks on Estonia and Georgia, attacks for which Russia denied its own involvement. Under the overall control test, the relationship between the Russian Business network and the Russian state should be sufficient to impute state responsibility (Gervais, 2012).

In the case of individuals and unorganized groups, the *Tadic* tribunal accepted a higher "effective control" standard to impute state responsibility. In order to meet the "effective control" test, the *Tadic* tribunal determined that there must be "specific instructions or directives aimed at the commission of specific acts," or in the absence of direction, that there be a public endorsement of the acts *ex post facto*. Thus Article 11 of the Draft articles on State responsibility states that "conduct which is not attributable to a state under the preceding Articles shall nevertheless be considered an act of that state under international law if and to the extent that the state acknowledges and adopts the conduct in question". (Madubuike-Ekwe, 2017). In *U.S Diplomatic and Consular Staff in Tehran* (U.S. v. Iran) the seizure of the US embassy and its personnel by militants was endorsed by the Iranian State. The ICJ held that Iran's approval translated into state responsibility for the actions of the militants. Under this framework, if individuals or unorganized groups of hacktivists use a cyber-attack to destroy a power plant in another state and their host state unequivocally approves the action, the attack will be imputed to that host state.

Given the anonymity of the technology involved, attribution of a cyber-attack to a specific state may be difficult. While a victim state might ultimately succeed in tracing a cyber-attack to a specific server in another state, this can be an exceptionally time-consuming process, and even then, it may be impossible to definitely identify the entity or individual directing the attack. For example the attacker might well have hijacked innocent systems and used them in conducting attacks (Graham, 2010). According to Yoram Dinstein, "in the present state of the art, it is often by no means clear who originated the Cyber-attack." (Dinstein, 2002). The inability to identify the attacker undermines in practice the theoretical entitlement of the victim state to resort to forcible counter-measures in self-defense (Sklerov, 2009).

Because of the difficulties raised by traditional requirement to attribute cyber-attacks to a state—and the increasing vulnerability to continuous attacks to which this concept exposes victim states—there is now a growing effort to formulate acceptable alternatives to the notion of "conclusive attribution" (Jensen, 2002). While all these efforts have merit, our focus here will be on the suggestion that

state responsibility for cyber-attacks may be based on "imputed" responsibility.

Thus the concept of imputed responsibility would apply to not only to cyber-attacks conducted by a state's own citizens, but to all non-state actors who launch such attacks from within a state's territory. It is now generally accepted that non-state actors, such as terrorists, have committed armed attacks against states (Dinstein, 2005). Certain armed attacks can rise to the level of armed attacks. In light of the fact that almost all cyber-attacks are now traced to non-state actors, attention will be focused on the imputed responsibility of states for the actions.

Therefore, the question is what is a state's duty to prevent cyber-attacks? What constitutes state's violation of this duty?

5) Duty to prevent Cyber-attacks

International law requires states to take steps to prevent their territories from being used to launch attacks. This duty comprises of the following state obligations:

a) To enact stringent criminal laws against the commission of international cyber-attacks from within national boundaries.

b) To conduct meaningful, detailed investigations into cyber-attacks.

c) To prosecute those who have engaged in these attacks

d) To cooperate with the victim state' own investigation and prosecution of those responsible for the attacks.

Although these state obligations are derived from all sources of international law, some of the sources are more relevant to cyber-attacks. For example, the European Convention on Cybercrime requires signatories to adopt domestic laws that criminalizes cyber-attacks and confirms the duty of states to prevent their territories from being used by non-state actors to conduct these attacks against other states (Convention on Cybercrime, 2001). Similarly, the *Tallinn Manual* provides that "a state bears International Responsibility for a cyber-operation attributable to it and which constitutes a breach of an international obligation" (Tallinn Manual 2.0).

The United nations have increasingly passed resolutions which focused on cyber-attacks. For example, the U.N. General Assembly has called on states to criminalize such attacks and to prevent their territories from being used as safe havens from which to launch attacks. The General Assembly has also called upon members states to cooperate in the investigation and prosecution of international cyber-attacks (U.N. G.A. Res 45/121; Res 55/63). Finally, some states including United States, and the General Assembly have specifically identified cyber-attacks as a threat to international peace and security.

6) Violation of the duty to prevent Cyber-attacks

To ascertain whether a state is responsible for cyber-attacks depends on a number of factors. The mere fact that a cyber-operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that state but is an indication that the

state in question is associated with the operation (Tallinn Manual 2.0).

In making such an assessment, a victim state must at a minimum examine a sanctuary state's criminal law dealing with cyber-attacks, its enforcement of the law, and its demonstrated record of cooperating with victim state's own investigations and prosecutions of cyber offenders who have acted across borders (Sklerov, 2009). Thus a state that knows of cyber-attackers launching attacks must take reasonable steps to fulfill its duty, by stopping the attacks, bringing the attackers to justice, or preventing further attacks. If a state does not cooperate with the efforts of the victim states to prevent such attacks, the state may be vulnerable to charges of imputed responsibility for these actions. In which case, the victim state may respond unilaterally against the sanctuary state in self-defense under Article 51 (UNSC, Res 1368 and 1373). Therefore if a state knowingly allows, either through action or omission—a non-state actor to commit an attack, the state would be held internationally responsible. But if the state undertakes sufficient measures to protect other states, and a cyber-attack still manages to originate from its territory, the state would be responsible.

Nevertheless, a state may not attribute state responsibility and then immediately respond with force. Rather, the victim state must request the offending state comply with its international obligations. If the offending state does not comply, the victim state may impute state responsibility and act accordingly.

4. Jus in Bello and Cyber-Attacks

Although a stand-alone cyber-attack has never instigated an armed conflict, cyber-attacks have been used in wars in response to traditional provocations or to prepare the way for an imminent conventional attack. However, once a state has entered into a conflict, the use of force is governed by the principles of *jus in bello*. Under *jus in bello*, even states that have the lawful right to use force still have limitations in how they use it. *Jus in bello* is largely derived from the Hague conventions (Hague Conventions, 1907), the Geneva Conventions, and its protocols, much of which is considered customary international law. In this section, this article examines how the law of armed conflict ought to apply to cyber-attacks. It should be noted that the limitations on how a state conducts its use of force is not based on the weaponry used, so adapting the principles of international humanitarian law to the use of cyber-attacks—despite being a new weapon of warfare—is not only possible but also appropriate given its growing popularity as a coercive tactic. Therefore, the applicability of the Law of armed conflict to cyber-attack must center on the traditional principles of *jus in bello*—military necessity, distinction, proportionality, and neutrality.

1) Military Necessity

International Humanitarian law (IHL) restricts the use of force to targets that will accomplish valid military objectives. Article 52 of Protocol 1 limits lawful targets to "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction,

capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage" (Protocol 1), Article 23 of the Fourth Hague Convention forbids destruction or seizure of property "unless such destruction or seizure is imperatively demanded by the necessities of war." The Rome Statute of International Criminal Court (ICC) considers violation of the principle of military necessity a "war crime". Thus, valid targets are limited to the concrete military advantage to be gained from a specific hostile act (Gervais, 2012).

A cyber-attack that targets an adversary's military computer systems satisfies the condition of military necessity because it is associated with the military. Most militaries use computers systems for several types of operations (Ibid.). An individual cyber-attack may be unnecessary if it does not advance the military objective. Although cyber-attacks must be necessary to be lawful, determining whether a target creates a "definite military advantage" is complicated. The complexity of computer systems makes calculating military advantage a challenge. Thus the evaluation of whether a cyber-attack arose from military necessity will rely on a case-by-case analysis similar to evaluation of military necessity in traditional warfare.

2) Distinction

The principle of distinction, which requires that combatants be distinguished from noncombatants and that military objectives be distinguished from protected property or protected places-presents another legal challenge (Graham, 2010). Under this principle, military commanders must employ weapons that can target accurately and must use this capability to distinguish between civilian and military objectives. By extension, the law of armed conflict prohibits cyber-attacks that are uncontrollable, unpredictable, or do not discriminate between civilian and military objectives. Furthermore, Additional protocol I prohibits attacks that deny the civilian population indispensable objects such as food or water supplies (Hathaway & Crootof, 2012).

Cyber-attacks may be easily applied to certain situations. For example, a cyber-attack that targets a military air traffic control system and only causes troop transport to crash would comply with the principle of distinction. However, other cyber-attacks deliberately target objects to kill civilians or destroy civilian objects. Such attacks are clearly unlawful under the law of armed conflict. For example, an attack on the civilian banking sector or hospitals, museums, or places of worship. Cyber-attacks against networks that manage these targets, like any other attack on these objects would be unlawful (Gervais, 2012).

Such cases are easy, but the harder determination to make is whether it is unlawful to attack dual use objects that serve both civilian and military purposes. These includes power generating stations, telecommunications, and bridges, among other civilian infrastructure used by the military during wartime (Green, 2000). Because much of cyberspace is dual-use, upholding the principle of distinction in cyberspace can be more challenging than in a conventional warfare.

However, if the intent of a cyber-attack is to achieve a military advantage by

targeting computer systems used for military objectives, and if the attackers conduct such attacks with reasonable precaution for likely collateral effects, cyber weapons are more precise and adaptable means for attack than traditional weapons (Gervais, 2012).

3) Proportionality

The principle of proportionality is similar to distinction in that it reflects concern with the consequences of an attack on civilian and civilian objects. The principle prohibits "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" (Protocol 1). The Rome Statute of the ICC incorporates proportionality within its enumeration of particular crimes. Article 8 (2) (a) (iv) refers to "excessive destruction… not justified by military necessity" and Article 8 (2) (b) (iv) states that "intentionally launching an attack in the knowledge that such attack will cause incidental loss…or damage… would be clearly excessive in relation to the concrete and direct overall military advantage anticipated" (Gervais, 2012). Thus, a military decision maker must weigh potential civilian casualties, destruction of civilian property, and the loss of indispensable civilian items against the benefit of achieving a military objective.

The principle of proportionality would make attackers prefer cyber-attack to kinetic attack from the standpoint of IHL compliance. For example, the trace-back capabilities of active defense measures—that is electronic countermeasures designed to strike an attacking computer system, shut it down and halt an attack—will ensure that these measures target only the source of the cyber-attack. This would greatly reduce collateral damage relative to that which would result from the use of kinetic weaponry, thus helping to achieve proportionality; distinguish the attacking system (the military objective) from protected places, property, and civilians; and minimize the unnecessary suffering that would be the probable result of a kinetic use of force (Graham, 2010). These traits are desirable for a state that wants to apply a level of proportionality force without causing a disproportionate number of civilian casualties.

However, it is obvious that the use of active defenses to defeat cyber-attacks will also create substantial challenges with regard to IHL compliance. For example, a surgical strike against a computer system ostensibly at the core of a cyber-attack may not be possible to achieve due to technical limitations (Ibid.). It is exceptionally difficult to trace an attack routed through intermediary systems. When such an attack occurs, a trace program not only requires time to carry out its functions, but it becomes more difficult to pinpoint the specific source of the attack once the attacker terminates the electronic connection. This may well cause a failure to identify the attacking system or an incorrect identification of an intermediary system as the source of the attack, with potentially significant IHL implications (Wedgewood, 2002).

Due to the type of harm they inflict, the proportionality of cyber-attacks poses

unique challenges. It can be difficult to evaluate whether an attack would be proportional according to the relevant categories of "loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof," as the typical direct effects of cyber-attacks may be non-lethal or temporary, yet severe (Protocol 1). In particular, how should the temporary incapacity of critical systems be evaluated? A cyber-attack that effectively stops the transmission of information through the internet might inconvenience the populace, but it might also have more severe consequences. For example, it might cause hospitals to be unable to communicate vital information, leading to loss of life. As a result, cyber-attacks may change the weight given to temporary consequences, and may force states to confront more uncertainty than they typically face in making decisions about the legality of planned attacks (Hathaway & Crootof, 2012).

Therefore the proportionality analysis of a cyber-attack must always be considered on a case by case basis. As Gervais notes, "any formula that compares the number of civilians killed to the number of combatants killed is insufficient." However, one must consider the values of the target and whether the attack offered a definite military advantage and showed proper caution vis-à-vis civilian life and property.

4) Neutrality

The principle of neutrality permits a state to declare itself neutral to a conflict and thereby protects it from attack or trespass by belligerents. Neutral states remain protected as long as they do not militarily participate or contribute to belligerent states or allow their territory to be used for such militaristic purposes. The principle of neutrality includes both rights and responsibilities: "The principal right of the neutral nation is that of inviolability; its principal duties are those of abstention and impartiality. Conversely, it is the duty of a belligerent to respect the former and its right to insist upon the latter" (Hathaway & Crootof, 2012).

Cyber-attacks jeopardize these distinct elements of neutrality. Certain characteristics of cyber-attacks make the evaluation of the principle of neutrality usually complex. Cyber-attacks may harness zombie computers located in one country to harm networks in another country, without the knowledge of any individual, much less the government—by masking their origin through a series of servers and computers. This poses challenges to analysis under the principle of neutrality for two reasons. First, a country may not know its computers are being used for a cyber-attack, and it therefore may not know its neutrality is threatened. Second, the principle of neutrality determines lawful responses to attacks based on the identity of the origin country. Thus, the inability to attribute attacks to a certain state affects the neutrality analysis. Nonetheless, it is also possible that political uncertainty about lawful responses to cyber-attack may be masquerading as an inability to attribute attacks; As such further clarity around the legal framework governing cyber-attacks may reduce barriers to attribution.

It is important to maintain the principle of neutrality to prevent warfare from spreading. The infrastructure of the internet presents practical problems for a

state attempting to be neutral under the current international humanitarian law framework. A re-interpretation of neutrality that permits a state to maintain its neutrality despite its cyberspace infrastructure "facilitating" attacks is necessary to preserve the spirit of neutrality (Gervais, 2012). A state ought to be able to maintain its neutrality as long as it upholds its duty "not to allow knowingly its territory to be used for acts contrary to the rights of other states."

5. Conclusion

Finally, this article has examined to what extent cyber-attack can be regulated under the existing regime of the laws of armed conflict. The existing Law of armed conflict framework—both *jus ad bellum* and *jus in bello*—provides some guidance, although incomplete and imperfect, for states seeking to determine the scope of permissible offensive and defensive cyber-attacks. It does not regulate the vast majority of cyber-attacks. Most cyber-attacks do not rise to the level of armed attack or take place in the context of an armed conflict. Consequently, they are not covered by the existing law of armed conflict. This does not mean that these cyber-attacks are unregulated. There are a variety of other legal frameworks such as the international law of countermeasures, domestic laws etc., that fill the gaps left by the law of armed conflict.

Cyber-attacks are global in nature. Changes to domestic law and policy criminalizing cyber-attacks while valuable legal responses cannot adequately and effectively curb an action that is truly an international concept. This global threat may only be effectively met by a global solution by the international community working together to design a new law for cyber-attacks. This must begin with an agreement on the problem—which means agreement on the definition of terms such as "cyber-attack", "cyberwarfare", "damage", "use of force" and "armed conflict" as well as "distinction" and proportionality as applied to cyberwarfare.

Thus given the global ubiquity of cyber space, it is commendable that 78 states support the "Paris call" (Paris Call, 2018) which reaffirms that "international humanitarian law and customary international law are applicable to the use of information and communication technologies (ICT) by states (Horowitz, 2020). This position is supported by some international organizations such as the European Union and the NATO. However some states refrain from, or even draw caution against taking such position.

In conclusion, it is inevitable that some conflict will have a cyber-component to it and it behooves policy makers to understand the legal landscape before such a conflict occurs. It is recommended that analysts develop the requisite knowledge and expertise now so that they are prepared to help policy makers when the need arises. By examining some of these relevant questions, this article takes one small step in this direction.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

(2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press (Hereinafter Tallinn Manual 2.0).

Alston, P. (2010). *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Addendum: Study on Targetted Killings. A/HRC/14/24/Add.6*. https://www.refworld.org/docid/4c0767ff2.html

Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda) 2005 I.C.J. 116, 165 (Dec. 19).

Brownlie, I. (2012). *International Law and the Use of Force by States* (p. 362). Oxford: Oxford University Press.

Convention on Cybercrime, Council of Europe, Nov. 23, 2001, 41 I.L.M. 282.

Dinstein, Y. (2002). Computer Network Attacks and Self Defense. In M. N. Schmitt, & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law* (p. 99). International Law Series, Vol. 76, Newport, RI: Naval War College.

Dinstein, Y. (2005). *War, Aggression and Self Defence (*4th ed.). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511841019

Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.S.T.S. 135.

Gervais, M. (2012). Cyber-Attacks and the Laws of War. *Berkeley Journal of International Law, 30,* 525-531. https://doi.org/10.2139/ssrn.1939615

Graham, D. E. (2010). Cyber Threats and the Law of War. *Journal of National Security Law and Policy, 4,* 89.

Green, L. C. (2000). *The Contemporary Law of Armed Conflict* (2nd ed.). Manchester: Manchester University Press.

Hague Conventions IV Respecting the Laws and Customs of War on Land, Annex, Oct. 18, 1907, 36 Stat. 2277, 205 consol. T.S. 277.

Hathaway, O. A., & Crootof, R. (2012). *The Law of Cyber Attack* (p. 850). Faculty Scholarship Series, Paper 3852. https://digitalcommons.law.yale.edu/fss_papers/3852

Horowitz, J. (2020). Cyber Operations under International Humanitarian Law: Perspectives from the ICRC. *ASIL Insights, 24*. https://asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law

Jensen, E. (2002). Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. *Stanford Journal of International Law, 38,* 207.

Lin, H. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy, 4,* 63.

Madubuike-Ekwe, N. J. (2017). The Applicability of the Law of Armed Conflict to Cyberwarfare: An Overview of Issues. I BUA L. J., 149.

Military and Paramilitary Activities in and against Nicaragua (Nicar V. US) 1986 I.C.J. 14 (June 27).

Moore, J. N. (2005). Development of International Law of Conflict Management. In J. N. Moore, & R. F. Turner (Eds.), *National Security Law (*2nd ed.). Durham, NC: Carolina Academic Press.

National Research Council (NRC) (2009). *Technology, Policy, Law and Ethics regarding U.S. Acquisition and Use of Cyberattack Capabilities*.

Prosecutor v. Tadic, Case No. IT-94-1-T, Sentencing Judgement 120 (July 14, 2007).

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts. (Hereinafter Protocol 1).

Roscini, M. (2010). World Wide Warfare-Jus Ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law, 14,* 85-130. https://doi.org/10.1163/18757413-90000050

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,* 885-937. https://doi.org/10.21236/ADA471993

Shaw, M. (2010). *International Law* (6th ed.). Cambridge: Cambridge University Press.

Sklerov, M. J. (2009). Solving the Dilemma of State Responses to Cyber-Attacks: A Justification for the Use of Active Defenses against States Which Neglect Their Duty to Prevent. *Military Law Review, 201,* 1-85.

The International Law Commission Commentary, Official Records of the G.A. 53rd Session, December 10, 2001, Supplement No. 10 (A/56/10 Ch.IV. E.1).

The Paris Call for Trust and Security in Cyberspace, November 12, 2018. https://pariscall.international/en

U. N. Gen Ass Res. 3314 (XXIX) 1974.

U.N. G.A. Res 45/121, 3, U.N. Doc /A/RES/45/121 (Dec. 14, 1990).

U.N. G.A. Res. 55/63, 1, U.N. Doc. A/RES/55/63 (Jan. 22, 2001)

U.N. Security Council Res. 1373 U.N. doc. S/Res/1373 (Sept. 28, 2001)

U.S. Diplomatic and Consular Staff in Tehran (U.S. v. Iran) 1980 I.C.J. 3 (May 24).

U.S. Training & Doctrine Command, DCSINT Handbook No. 1.02 Critical Infrastructure Threats and Terrorism at VII-2 (2006).

UN Charter, arts 2, 27, 41, 42, 51.

United Nations Charter, Articles 2(3), 2(4), 41, 42, 51.

Wallace, R. M. M., & Martin-Ortega, O. (2013). *International Law* (7th ed.). Mytholmroyd: Sweet & Maxwell.

Wedgewood, R. (2002). Proportionality, Cyberwar and the Law of War. In M. N. Schmitt, & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law* (pp. 219, 227-230).

Wingfield, T. (2000). *The Law of Information Conflict: National Security Law in Cyberspace*. Falls Church, VA: Aegis Research Corp.