Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security that Redefines the Law of State Responsibility

NICOLAS JUPILLAT

INTRODUCTION

Cyberspace is the theoretical environment “formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks.”¹ As our dependence on computer networks grows, so does our vulnerability. As early as 2013, United States Director of National Intelligence James Clapper told the Senate Intelligence Committee “that cyber attacks and cyber espionage [had] supplanted terrorism as the top security threat facing the country.”² On April 1, 2015 President Obama issued an ambitious executive order in which he declared malicious cyber-enabled activities “an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States”, and “a national emergency”.³ The international community at large shares the same concern. The United Nations General Assembly has adopted several resolutions expressing the need to collectively address the impact of information and communication technology on international security since 1998.⁴

Cyber Defense Center of Excellence\(^5\) convened a group of international experts to discuss the applicability of international law to cyber warfare.\(^6\) Their final work, known as the Tallinn Manual, provides a series of draft rules that are a strong indication of how international law will be applied to cyber conflict in the future. Even though these rules are non-binding as such, the International Court of Justice, whose function is to settle disputes in accordance with international law, recognizes academic work as a subsidiary source of the law.\(^7\) Continuing the discussion initiated by the Tallinn Manual is therefore of paramount importance.

As the international and academic communities address the rising legal issues of cyber conflict, the temptation to reconsider previously agreed upon interpretations of the rules governing self-defense is greater than ever before. While the new threats and actors arising in cyberspace do require a certain clarification of the law,\(^8\) they do not render existing norms obsolete.\(^9\) The development of specific norms for State conduct in cyberspace should therefore be carefully considered. Consequences of cyber operations are far more difficult to predict and assess, not to mention that cyberspace is an equalizing factor that empowers non-State actors to cause heavier damage than they would in conventional war fighting domains, at considerably lower costs.\(^10\) In sum, the complex nature of cyberspace means we can no longer afford imprecision in the law, especially when it comes to the right of self-defense, which allows States to use force in response to an armed attack without having to seek prior approval from the United Nations Security Council.\(^11\) Self-defense in cyberspace not only comes with its own set of challenges (the question of whether there is such a thing as an armed attack causing no physical consequences of cyber operations is particularly challenging) but also presents unique legal issues due to the nature of cyberspace.

\(5\). Center of Excellence created in 2008. Participating nations include Estonia, Germany, Italy, Latvia, Lithuania, Slovak Republic, Spain, Hungary, Poland, the United States, the Netherlands, Austria (non-NATO), the Czech republic, the United Kingdom, and France.


\(7\). Statute of the Court, 1945 I.C.J. (art. 38 § 1(d)): “The teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.”


\(9\). Id.


In the near future, advancements in the fields of robotics, nano- and biotechnology, as well as artificial intelligence will further increase the complexity of cyber operations and their impact on international peace and security. This Article focuses on *ius ad bellum*, and provides an overview of the questions raised by use of force in general, self-defense in particular, and the plea of necessity as a potential alternative course of action against threats to peace and security in cyberspace.

I. USE OF FORCE GENERALLY

As a matter of principle, the United Nations Charter prohibits the threat and use of force in international relations. Only two exceptions are recognized: use of force mandated by the United Nations Security Council, and self-defense in response to an armed attack, which refers to the most severe form of the use of force. More than mere exceptions, these two recourses are but a continuation of the prohibition of use of force, which they aim to remedy.

The idea of cyber use of force is commonly admitted. The International Court of Justice has ruled that the prohibition of use of force applies regardless of the weapon used. For a cyber instrument to qualify as a weapon, it needs not be a weapon by design. Virtually any object can become a weapon depending on its use or intended use. Therefore, in order to qualify as a use of force, a cyber operation attributable to a State would most likely have to result in death, injury or significant material damage. Though the history of cyber conflict can be traced back to 1986, there are no examples of a cyber operation being qualified as a use of force to-date. The likelihood of computer networks being used to

12. *Id.* at art. 2, para. 4: “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.”


16. *Id.* at Rule 11(8).


18. *Infra* note 94. See release of the Stuxnet worm that was designed to force Iran’s nuclear plants’ centrifuges to spin uncontrollably while still making it appear as if they were operating normally. The aim was not to cause a nuclear disaster but to have Iranian authorities doubt their own capacity to have a functional nuclear program. Once the nature of the problem was identified, the Iranian government still avoided calling it an example of use of force.
effectively cause death, injury or material damage has, however, dramatically increased. Possible examples include interfering with the cooling system of a nuclear plant, opening a dam with the intent of flooding inhabited areas, or interfering with air or road traffic control systems. As for cyber operations that do not cause physical damage, the qualification of use of force cannot be entirely ruled out but no consensus on a possible threshold has yet emerged. The so-called Schmitt Analysis provides a test that helps determine whether or not a cyber operation amounts to a use of force.\(^{19}\)

As previously mentioned, one of cyberspace’s distinctive aspects is its propensity to empower non-State actors to participate in conventional as well as cyber conflicts to a much larger extent than in the past. Some of them do so on their own initiative (hacktivists, cyber terrorists) while certain States that seek to escape responsibility will resort to non-State actors as proxies. The International Court of Justice has ruled that while financing an armed group conducting hostilities against another State constitutes a prohibited act of intervention in the internal affairs of that State, it does not constitute a use of force.\(^{20}\) But arming or training them would indeed qualify as such.\(^{21}\) Following the same rationale, the Tallinn group of experts has considered that the provision by a State of malicious code to a non-State actor using it against the cyber infrastructure of another State would be a form of use of force.\(^{22}\)

When the instance of use of force is not severe enough to qualify as an armed attack, it is up to the Security Council to take the measures necessary to maintain international peace and security. Among them, the United Nations Charter provides for the possibility of “complete or partial interruption of ... telegraphic, radio, and other means of communication” as a peaceful response to a threat against peace.\(^{23}\)

II. SELF-DEFENSE GENERALLY

Article 51 of the United Nations Charter reaffirms the inherent right of self-defense, individual or collective, in the event of an armed attack. A cyber operation whose scale and effects\(^{24}\) amount to an armed attack would provide the State thus harmed with the right to use force in self-defense

\(^{19}\) MICHAEL SCHMITT ET AL., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE Rule 11(9) (Cambridge University Press 2013). The test includes assessment of Severity, Immediacy, Directness, Invasiveness, Measurability, Military character, Presumptive legitimacy, and Responsibility.

\(^{20}\) Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) 1986 I.C.J. § 228 (June 27).

\(^{21}\) Id.

\(^{22}\) MICHAEL SCHMITT ET AL., at Rule 11(4).

\(^{23}\) U. N. Charter, art. 41.

without requiring prior permission from the United Nations Security Council. According to the theory of accumulation of effects, multiple cyber operations conducted by one or more actors acting together, which would not individually reach the threshold of an armed attack, could cumulatively amount to an armed attack depending on their overall scale and effects.\footnote{25. Michael Schmitt et al., at Rule 13(8).}

The response in the context of self-defense against a cyber attack is subject to the same principles of necessity, proportionality, and immediacy as conventional attacks.\footnote{26. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) 1986 I.C.J., §176, 194 (June 27); Oil Platforms Case (Iran vs. U.S.), § 43, 73–74, 76 2003 I.C.J. (Nov. 6).} These criteria will prove difficult to evaluate in cyberspace given, on the one hand, the time required for attribution of the attack, and on the other, the difficulty for the attacker to predict, and for the target to assess, damages directly caused by the cyber operation.

The Tallinn experts have unanimously rejected the concept of preventive self-defense,\footnote{27. Michael Schmitt et al., at Rule 15(7).} which pertains to the use of force against a State that is deemed dangerous in and of itself regardless of the existence of a tangible threat. Conversely, international law does not object to preemptive self-defense\footnote{28. Also referred to as anticipatory self-defense.} in principle. The Tallinn group of experts is divided, however, on the way to justify the lawfulness of a preemptive strike.\footnote{29. Michael Schmitt et al., at Rule 15(4).} For a minority, only temporal proximity of the attack may justify it. For a majority, a State may exercise its right of self-defense preemptively when an attack is being prepared and the target State would risk losing its ability to respond effectively unless it acted first, whatever the relative imminence of the attack may be. But since it is particularly difficult to quickly and reliably trace a cyber operation back to its perpetrator, will it be possible to predict with a sufficient degree of certainty that a cyber attack is about to be committed in order to justify a preemptive strike? Unlike conventional domains where technology such as remote sensing can be used to ascertain the adversary is preparing to launch an attack, cyber operations are more difficult to detect as they blend into the considerable flow of information packets exchanged through computer networks on a daily basis.

The Tallinn group of experts was divided on the question of whether the nature or the scale of the effects should prevail in the characterization of an armed attack.\footnote{30. Id. at Rule 13(9).} Though the Tallinn experts rejected the idea that intelligence gathering or cyber theft could amount to an armed attack,\footnote{31. Michael Schmitt et al., at Rule 13(6).} it is
still uncertain whether there needs to be physical damage for an attack to qualify as an armed attack or if sufficiently serious immaterial effects would also qualify as such (attacks causing malfunction of a nation’s critical infrastructures such as its power grid, banking, telecommunication or transportation systems, financial markets). The difficulty here lies in ensuring that the necessity requirement is met, especially in the case of one-shot cyber attacks. Whether the effects are short-lived or long lasting, the initial cause of the injury may sometimes be the punctual introduction of malicious code into a system. Yet, the right to resort to force in self-defense can only be exercised if it is the only course of action available to defeat an imminent or ongoing strike. It is by no means meant to be a punitive measure against the perpetrator. At the other end of the spectrum of possible non-kinetic armed attacks, China and Russia, among others, have expressed that any information inciting terrorism, secessionism, extremism or undermining the political, economic and social stability of other countries, as well as their spiritual and cultural structures constitutes a major threat to peace and security, alluding to the possibility of considering certain types of content or so-called “psychological wars” as a justification for self-defense, a view that Western powers oppose.

The question of the role of non-State actors, whose disruptive potential is significantly larger in cyberspace than it is in conventional domains, is particularly delicate when it comes to self-defense. First and foremost, it is necessary to distinguish between situations where State involvement, regardless of its extent, can be established, and those where it cannot.

III. THE NECESSARILY STATE-SPONSORED NATURE OF ARMED ATTACKS

For a State to exercise its right of self-defense, it must have been the target of an “armed attack”, which, as stated above, is the most severe form of the use of force under international law. Although the United Nations Charter does not specifically mention that an armed attack must be understood as an act performed by a State, the Charter’s purpose is to govern State relations exclusively, which necessarily implicates State involvement. At any rate, it is highly unlikely that the drafters of the Charter could have imagined at the time it was written that a non-State

33. MICHAEL SCHMITT ET AL., at Rule 14(2).
35. MICHAEL SCHMITT ET AL., at Rule 11(3).
36. The doctrine of the United States does not distinguish between mere uses of force and armed attacks. See MICHAEL SCHMITT ET AL., at Rule 11(7).
armed group would one day acquire the capacity to rival nation-States and be able to carry out an armed attack on their own. United Nations General Assembly Resolution 3314 additionally provides a definition for the qualification of the armed attack that only refers to States. While United Nations General Assembly Resolutions are not binding and cannot impose on the Security Council, the International Court of Justice held that General Assembly Resolutions are an expression of international customary law. Furthermore, the Kampala conference held in 2010 to review the Rome Statute establishing the International Criminal Court reaffirmed resolution 3314 as the basis of its definition of the crime of aggression. The amendment currently pending ratification defines the crime of aggression as “the planning, preparation, initiation or execution by a person in a leadership position of an act of aggression,” which presumes the person’s ability to control or direct the political or military action of a State. This reaffirmation of resolution 3314 as the authoritative reference for the definition of an armed attack reinforces its customary nature. It is at the very least the expression of the opinio iuris of States Parties to the Rome Statute.

According to the law of State responsibility, any acts committed by organs of a State are attributable to that State. Organs of a State refer to any persons or entities that are characterized as such under the State’s internal legislation, regardless of their function or place in the hierarchy, whether or not they were acting in compliance with, beyond or without any instructions. Private sector persons or entities specifically empowered by domestic law to exercise governmental authority are also to be equated to State organs. This would apply to situations where States have legislation authorizing private sector Computer Emergency Response Teams to conduct cyber defense of governmental networks. More generally, an act

39. Aggression is the counterpart of armed attack in international criminal law ("agression armée" is French for "armed attack").
40. Rome Statute of the I. C. C., part 2, art. 8 bis (2001). The 2010 Kampala Amendments on the definition of aggression will have to be ratified by at least 30 States (23 as of March 12, 2015) and the jurisdiction of the Court activated by two thirds of the States Parties to the Rome Statute any time after 2017.
41. The belief that one’s conduct is executed in furtherance of a legal obligation.
43. Id. at commentary 2.
45. International Law Commission, at art. 5.
46. Michael Schmitt et al., at Rule 6(8).
perpetrated by a non-State actor under the direction or control of a State will also engage the responsibility of that State.\textsuperscript{47}

While noting the controversial nature of the possible characterization of acts by non-State actors as armed attacks, a majority of the Tallinn group of experts goes as far as to argue that the right to self-defense extends to any act perpetrated by non-State actors in cyberspace, regardless of State involvement.\textsuperscript{48} The same majority argues that the uncertainty of the question only lies in the degree of organization a group must have to be capable of mounting an armed attack as a matter of law.\textsuperscript{49} This argument in favor of self-defense in the face of armed attacks by non-State actors is based on Resolutions 1368 and 1373,\textsuperscript{50} unanimously adopted by the United Nations Security Council after the terrorist attacks of September 11, 2001. Both the preamble to Resolution 1368 and the body of Resolution 1373 include a reaffirmation of the “inherent right of individual and collective self-defense” contained in the United Nations Charter.\textsuperscript{51} While these two resolutions may appear to mark the recognition by the international community that the concept of armed attack extends to uses of force perpetrated by non-State actors regardless of State involvement, such an interpretation remains questionable on multiple grounds.

Firstly, these two resolutions mostly fall under the category of political declarations. The Council hardly ever mentions self-defense in its resolutions\textsuperscript{52} since it is not required for the right to self-defense to be recognized. The very idea of self-defense is to allow States to defend themselves when they are faced with a threat that requires immediate action. Article 51 of the Charter states that “nothing... shall impair the inherent right of individual or collective self-defense”, therefore not even Article 39, which charges the Security Council with determining the existence of an act of aggression. As a matter of fact, the right to self-defense is not only a provision of the Charter but also a rule of international customary law.\textsuperscript{53} Therefore, a State is the sole judge of whether it should use force in self-defense, provided an armed attack occurred. All that is required of the injured State is to inform the Security Council of the measures taken.\textsuperscript{54} But if these resolutions were not necessary for the United States to resort to self-defense, why then were they adopted? Both

\textsuperscript{47} International Law Commission, at art. 8.
\textsuperscript{48} \textsc{Michael Schmitt et al.}, at Rule 13(16).
\textsuperscript{49} \textit{Id.} at Rule 13(18).
\textsuperscript{50} S.C. Res. 1368, S/RES/1368 (Sept. 12, 2001); S.C. Res. 1373, S/RES/1373 (Sept. 28, 2001).
\textsuperscript{51} \textit{Id.}
\textsuperscript{52} \textsc{Michael J. Glennon & Serge Sur}, \textit{Terrorism and International Law}, (Brill 2006).
\textsuperscript{53} Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) 1986 I.C.J. §195 (June).
\textsuperscript{54} U. N. Charter, at art. 51.
resolutions can only be understood in the context of the terror attacks of September 11, 2001. The Security Council could easily predict the nature of the American response to what constituted the first modern physical strike that the United States suffered on its mainland. In view of past instances of strikes against U.S. interests abroad, it was highly likely that the American response would involve use of force. Faced with this perspective, Resolutions 1368 and 1373 presented the Council with three benefits: keeping the U.S. response within the pre-established international legal framework of collective self defense; ensuring its right to information about measures taken; and finally, making these measures comply with the customary law of self-defense (in particular the principles of necessity and proportionality).

Beyond the political context surrounding the adoption of these resolutions, their legal authority should not be overstated. First, the International Court of Justice had the opportunity to clarify that an armed attack could only be carried out by a State, and implicitly confirmed that view in a judgment the following year. Secondly, Resolutions 1368 and 1373 are more of an exception in the jurisprudence of the Council. These did not set a precedent in the later practice of the Council, which turned out to be much more cautious when it addressed the Israeli strikes in Lebanon that followed terror attacks by Hezbollah in 2006. At the time, Israel had asserted its right to self-defense, stating that it was not fighting Lebanon but merely replying to terrorists’ actions that originated in Lebanon. However, the Security Council, while stressing the “violence” and “the continuing escalation of hostilities” as well as “the need to address urgently the causes that have given rise to the current crisis,” did not mention self-defense. Finally, Resolutions 1368 and 1373 are incomplete decisions because of their (intended) ambiguity. A close reading of the two texts shows a failure to provide any kind of distinction between terrorist attacks

55. Car bomb attacks against U.S. Embassies in Kenya and Tanzania on August 7, 1998 were followed by military strikes against presumed bases in Sudan and Afghanistan on August 21, 1998.
58. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion 9, para. 139 (July 2004) (“Article 51 of the Charter thus recognizes the existence of an inherent right of self-defense in the case of armed attack by one State against another State.”).
60. Hezbollah cross-border raid of July 12, 2006.
potentially supported by a State and those that are not. It therefore does not lead to a general conclusion about the extent to which a State must be involved in a non-State actor’s attack for an armed attack to be constituted, much less does it open the possibility of armed attacks executed by non-State actors in the absence of State involvement. Resolutions 1368 and 1373 both mention, in passing, the right of self-defense in their introductions but only qualify the attacks as terrorist attacks, not armed attacks. These were adopted at a time when the hypothesis of State involvement in the terror attacks was not yet ruled out. The mention of the right of self-defense was more of a political reminder that, should there be any State involvement established, the United States would likely be entitled to use force to preserve its security.

As a result of these observations, there seems to be little legal grounding for the existence of non-State-sponsored armed attacks. In cyberspace, the multitude of non-State actors potentially capable of causing serious harm outside of any State support, in complete anonymity, calls for greater caution in order to preserve the viability of the international peace and security system, especially if the Council is to effectively promote the principles of peaceful settlement of disputes and the respect for State sovereignty.

IV. TOWARDS A LOWER STANDARD OF ATTRIBUTION OF STATE RESPONSIBILITY FOR ACTS PERFORMED BY NON-STATE ACTORS

These previous observations do not preclude the possibility of an armed attack being carried out by a State through a proxy. In the Nicaragua case, the International Court of Justice, citing resolution 3314, determined that an “armed attack must be understood as including not merely action by regular armed forces across an international border, but also the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to an actual armed attack conducted by regular forces or its substantial involvement therein.” It is the relationship that the State establishes with its proxies that must be

63. International Law does not provide a clear definition for terrorism as we know it today. Article 51(2) of Additional Protocol I and Article 13(2) of Additional Protocol II to the Geneva Conventions of 1949 only prohibit acts of violence by States the primary purpose of which is to spread terror among the civilian population in times of war without offering substantial military advantage.
65. U.N. Charter, art. 33.
66. Id. at art. 2, para. 4.
67. Id. at § 195.
placed under scrutiny to determine whether it should incur responsibility for acts performed by them. In the same judgment, the Court stated that training and arming the contras did give rise to the United States’ legal responsibility for breaching the principle of non-intervention in the internal affairs of Nicaragua, as well as the prohibition of use of force against that State (which includes prohibition of armed attacks).\textsuperscript{69}

While a State cannot be held responsible for all actions of non-State actors operating from within its territory, the international community can encourage it to stop facilitating their operations by lowering the training and arming threshold of State responsibility. To this end, the concept of “harbor and support” might emerge as a rampart against States that do not directly use armed groups as proxies but encourage activities by non-State actors whose interests converge with their own. The doctrine originates in former United States Secretary of State George Shultz’s statement that “it is absurd to argue that international law prohibits us from . . . using force against States that support, train, and harbor terrorists or guerillas.”\textsuperscript{70} This claim received little support at the time. However, the use of increasingly disruptive non-State actors in cyber (and conventional) conflicts by States tends to make it a more plausible option to justify intervention. Operation Enduring Freedom in Afghanistan, launched by the United States on the grounds of the right to self-defense, targeted the Taliban regime accused of “harboring and supporting” the leaders of the Al-Qaeda terrorist network.\textsuperscript{71,72}

The legal grounding of such a standard of State responsibility for use of force executed by non-State actors is still uncertain but the political claim might gain more support as States try to find new ways to address the rising threat posed by non-State actors, including in cases of minimal State involvement. The International Court of Justice may have provided the first step towards legal justification for a similar threshold when it stated that “intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State . . . equates with the use of force by the assisting State when the acts committed in another State involve a threat or use of force.”\textsuperscript{73} The Tallinn experts also came to the conclusion that the

\textsuperscript{69}. Id. at §228.
provision of sanctuary (safe haven) to non-State actors “coupled with other acts, such as substantial support or providing cyber defenses . . . could, in certain circumstances, be a use of force.”74

V. ALTERNATIVES TO SELF-DEFENSE IN THE ABSENCE OF STATE INVOLVEMENT

What if the actions of a non-State actor causing a serious breach of a State’s national security did not benefit from any sort of State support? The United States has tried to justify intervention against non-State actors on the territory of weak States by claiming they are either “unwilling or unable” to stop the perpetrators of an imminent attack.75 A majority of the Tallinn experts supports the same idea.76 Several other States including the United Kingdom, Israel, Pakistan, Kenya, and Ethiopia seem to have put in practice a similar approach in past operations.77 Each State does have an obligation to put an end to harm caused by non-State actors from within its territory. Customary law, as codified in General Assembly Resolution 2625, supports the idea that States have a duty to refrain from unfriendly acts and must cooperate with one another.78 The International Court of Justice has ruled in the Corfu Channel case that a state must “not allow knowingly its territory to be used for acts contrary to the rights of other states.”79 The Arbitral Award in the Smelter Trail case notes: “[a] State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction.”80 Being “unwilling” to apprehend the perpetrators of an attack against another State is therefore a serious violation of international law. It does not, however, necessarily entail the right to self-defense. First, countermeasures may be taken by the injured State to encourage the “unwilling” State to put an end to the situation.81 If such measures do not suffice, and use of force appears as the only way to stop an attack, it is up to the Security Council to authorize a possible

76. MICHAEL SCHMITT ET AL., at RULE 13(23).
intervention in order to restore peace and security, unless the attack poses a sufficiently grave and imminent peril to an essential interest of the target State, in which case the injured State may invoke the plea of necessity. As far as “unable” States are concerned (because they lack the expertise or the technology), bilateral cooperation or consented intervention offers the best chances of obtaining resolution without violating State sovereignty. After all, a weak State that, in all good faith, is unable to neutralize the armed group operating from within its territory could quite possibly authorize intervention by the injured State on its soil in a cooperative framework that would not involve self-defense. If, however, the weak State, while still in all good faith, fails to react quickly enough in spite of the aggrieved State’s repeated requests, the plea of necessity would then again offer a plausible alternative to self-defense to preclude the wrongfulness of an intervention. The advantage of the plea of necessity lies in the fact that it is not directed against any State, and therefore an alternative course of action to self-defense in the absence of State involvement in an attack.

According to the International Law Commission, necessity may be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation if it is the only way for the State to safeguard an essential interest against a grave and imminent peril. It does not depend on prior conduct of the State against which intervention is conducted, and does not seek to attribute responsibility to that State. As a result, the State invoking the plea of necessity must ensure that its intervention does not seriously impair an essential interest of the State on the territory of which intervention occurs. The “Caroline” incident of 1837, though frequently referred to as an instance of self-defense, really involved the plea of necessity. In that case, British armed forces entered United States territory and destroyed a vessel owned by United States citizens which was carrying recruits and military and other material to Canadian insurgents. At the time, the British Government referred to the “necessity of self-defense and self-preservation”. While objecting the right of the British Government to intervene within the territory of the United States, Secretary of State Webster did, however, allude to the possibility of such an intervention being possibly justified by

82. U. N. Charter, art. 39.
83. See further developments on plea of necessity below.
84. International Law Commission, at art. 25.
85. Id.
88. Id.
89. Id.
“a clear and absolute necessity,” 90 one that is “instant, overwhelming, leaving no choice of means, and no moment for deliberation.” 91 In his message to Congress of 7 December 1841, President Tyler declared that: “This Government can never concede to any foreign Government the power, except in a case of the most urgent and extreme necessity, of invading its territory, either to arrest the persons or destroy the property of those who may have violated the municipal laws of such foreign Government.” 92 In an exchange of letters of 1842, the United States and British Governments agreed that “a strong overpowering necessity may arise when this great principle 93 may and must be suspended . . . for the shortest possible period during the continuance of an admitted overruling necessity, and strictly confined within the narrowest limits imposed by that necessity”. 94 In cyberspace, if cyber infrastructure located within the territory of State A is used by non-State actors located in State B to conduct an attack on State C, the latter could potentially invoke the plea of necessity to intervene in State A and B to put an end to the threat it is faced with, provided the attack constitutes a grave and imminent peril to an essential interest of State C, that State A and B are unable or unwilling to react quickly enough, and that none of either State A or B’s essential interests be harmed by State C’s intervention.

The plea of necessity offers a credible alternative to self-defense in the absence of State involvement, 95 especially given the interconnected nature of cyberspace whereby a State’s failure to act can be detrimental to the entire international community. It is preferable to self-defense in that its justification requirements are more restrictive, and it does not seek the weak State’s responsibility.

CONCLUSION

The right to self-defense, while being a long-established prerogative of nation-States under international law, implies a series of questions whose complexity is only reinforced by the intricate nature of cyberspace and cyber operations. Preemptive self-defense becomes more challenging, as perpetrators can remain unseen and direct consequences turn out to be difficult to assess. It may even take years until a cyber attack can be

---

90. Id.
91. Id.
92. Id.
93. Principle of non-intervention within the territory of a sovereign power at peace.
identified as the cause of any malfunctioning of cyber infrastructure. Meanwhile, the very definition of armed attack may evolve to encompass immaterial damage as our societies become more dependent on the uninterrupted functioning of computer networks. In order to preserve international peace and security, the temptation of unilateralism should be avoided by all means. Self-defense must remain an answer to armed attacks carried out by States only, whether through regular or delegated force. However, the tendency for States to resort to proxies, particularly in cyberspace, should be deterred by lowering the threshold of State responsibility for armed attacks performed by non-State actors. Finally, if no State support whatsoever can be established, international cooperation between the injured State and the State from whose territory the operation was conducted should prevail. If, for whatever reason, cooperation does not appear to be effective at addressing a major cyber attack, the plea of necessity might offer, in the last resort, the possibility to preclude unlawfulness of an intervention in the internal affairs of another State in order to put an end to a cyber operation gravely undermining the injured State’s essential interests. More generally, cyber threats to security can only be effectively and peacefully addressed through international cooperation and trust-building measures, which require further harmonization of domestic cyber legislations, and the implementation of a multi-stakeholder Internet governance model involving both the public and private sectors.
