View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by U.S. Naval War College Digital Commons

INTERNATIONAL LAW STUDIES

PUBLISHED SINCE 1895

U.S. NAVAL WAR COLLEGE

Anticipatory Self-Defense in the Cyber Context

Terry D. Gill and Paul A. L. Ducheine

89 INT'L L. STUD. 438 (2013)

Volume 89 2013

Anticipatory Self-Defense in the Cyber Context

Terry D. Gill and Paul A. L. Ducheine[*]

I. INTRODUCTION

This article will examine the question of whether the right of self-defense under contemporary international law permits a State to react to an imminent or potential armed attack carried out by digital means in two circumstances. First, as an attack occurring in conjunction with, or as an adjunct to, a conventional kinetic armed attack intended to neutralize the target State's defensive and command and control systems. Second, as an attack—independent of any use of kinetic force—intended to cause significant human casualties, physical damage or large-scale disruption in the target State. While the former scenario is probably considerably more likely than the latter scenario, both will receive attention. The applicable law is the same in either scenario, although there are some potentially significant differences in the modalities of its application, primarily in the identification of the attacking party and in gauging the level of the response if an attack was conducted wholly in the digital domain.

* Terry D. Gill is Professor of Military Law, University of Amsterdam and Netherlands Defence Academy. Paul A. L. Ducheine is Associate Professor of Cyber Operations, Netherlands Defence Academy, and Senior Guest Lecturer and Research Associate, University of Amsterdam. © 2013 by Terry D. Gill and Paul A. L. Ducheine.

A. Starting Points

This article assumes a number of issues are "givens" for the purposes of this discussion.

First, that any use of force at the international level is, as a matter of law, governed by the international law on the use of force, irrespective of the manner in which the force is conducted and carried out.[1]

Second, while the use of force in the cyber context poses certain challenges in *how* and *when* the existing legal framework regulating the use of force can be applied, it is capable, in principle, of being applied to any type of force that can be qualified as such. Consequently, that it can be applied to computer-based attacks just as it can be applied to other forms of both kinetic and non-kinetic force, such as bacteriological, radiological and chemical weapons, whether used in conventional warfare or in terrorist assaults.[2] While the specific characteristics of cyber attack differ in some important respects from conventional kinetic attack and most forms of what is loosely referred to as "cyber attack" do not qualify as either a use of force or armed attack, those that do cause—or are intended to cause—significant loss of life, physical destruction or long-term disruption of a State's vital infrastructure could constitute an armed attack. Hence, the contemporary legal framework is applicable as a matter of law and potentially relevant in the cyber context. There are neither legal nor practical reasons to assume that the existing international legal framework governing the use of force in the cyber realm is irrelevant, inadequate or incapable of being applied without clear and convincing evidence so indicating.

Third, there are no separate rules and legal principles for the use of force in the cyber context. Therefore, notions such as "use of force," "armed attack," "necessity," "immediacy" and "proportionality" are no different in the cyber context than in the physical world, although the modalities of their application might well differ to some extent. Likewise, the rules relating to attribution of an attack to a particular State or non-State entity

1. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8).

2. Paul Ducheine, Joop Voetelink, Jan Stinissen & Terry Gill, *Towards a Legal Framework for Military Cyber Operations*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES 101 (Paul Ducheine, Frans Osinga & Joseph Soeters eds., 2012).

do not cease to be applicable when the attack is carried out by cyber means.[3]

Fourth, self-defense of States at the international level is relevant only to unlawful uses of force originating outside a State's territory that rise to the level of an armed attack. This means that any other type of activity, whether it involves a degree of force below this threshold or constitutes criminal conduct or a violation of other national or international legal rules not related to the use of force, falls outside the scope of those actions to which States may respond in self-defense. Therefore, cyber criminal activity, cyber (corporate) espionage and various other forms of unauthorized penetration, theft of data and sabotage of computer systems, whether public or private, that do not fit within the definition of armed attack are not subject to the law relating to self-defense and will not be addressed in this article. Such activities may well constitute unlawful intervention or other violations of international and national law, but the violations do not give rise to the right of self-defense when carried out in the physical world. There are no compelling reasons why this should be different in the cyber domain.

B. Structure

Section II will set out the essential nature and purpose of the right of self-defense, and examine its scope and the legal conditions governing its exercise under both the UN Charter and customary international law. Since the law regulating the use of force and the exercise of the right of self-defense are taken to be applicable, relevant and based upon the same rules, conditions and principles in the cyber context as in the physical domain, it is essential to set out this legal framework as clearly and succinctly as possible in order to determine the conditions and modalities of the exercise of self-defense. In particular the legality of anticipatory self-defense under contemporary international law is reviewed. To the extent that anticipatory self-defense is permitted or, alternatively, seen as lacking a legal basis within the right of self-defense in general, this will be relevant to its possible application in responding to an imminent cyber armed attack.

---

3. This is the approach taken by the International Court of Justice (ICJ) in its *Nuclear Weapons* advisory opinion, *supra* note 1, ¶¶ 37–50, 244–47, and unanimously by the Group of Experts responsible for the TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

Following this summary of the current legal framework regulating the use of force and the exercise of self-defense, we turn in Section III to its application in the cyber context. The modalities of a cyber armed attack will first be examined. We will then look into the particular challenges of applying the legal framework governing the exercise of self-defense, in particular anticipatory self-defense, in the cyber context. While the applicable law is the same, there are specific challenges and modalities involved in applying it to the cyber context, principally, in situations when cyber weapons are employed in the absence of more traditional kinetic force. In such situations, the challenges posed include ascertaining the source of the attack and identity of the attacker, determining potential consequences of the attack and gauging the response in terms of necessity, immediacy and proportionality.

In Section IV, we draw a number of conclusions and provide a clear answer to the question of whether anticipatory action in self-defense would be a legal response, and, to the extent it is, what conditions and limitations of a general and specific nature are relevant.

II. THE LEGAL FRAMEWORK GOVERNING THE EXERCISE OF THE RIGHT OF SELF-DEFENSE.

This section will first deal with the essence and legal basis of self-defense and then discuss the criteria pertaining to it as found in the UN Charter and customary international law.

A. Essence and Dual-Legal Basis of Self-Defense

The right of self-defense under international law is the right of a State to repel or, if necessary, overcome an unlawful use of force amounting to an armed attack.[4] That is what characterizes it and sets it apart from other uses of force, whether lawful (e.g., action undertaken by or with the authorization of the UN Security Council to maintain or restore international peace and security or as a law enforcement measure in the domestic legal con-

4. *See* Terry D. Gill, *Legal Basis of the Right of Self-Defence under the UN Charter and under Customary International Law*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS 187, 187–88 (Terry D. Gill & Dieter Fleck eds., 2010).

text), or unlawful (e.g., uses of force that do not have a recognized legal basis).[5]

Self-defense is both an *inherent* right of States under customary international law and an exception to the prohibition on the use of force as laid out in Article 2(4) of the UN Charter. The inclusion of the right of self-defense within the Charter had and has a dual purpose: recognition of the preexisting right of States under customary international law and integration of the right of self-defense into the Charter system of collective security in order to provide an unequivocal basis for collective self-defense.[6] Any legal assessment of self-defense must take into account the Charter's substantive and procedural requirements, as well as the criteria for the exercise of this right under customary international law.

The two sources are complementary, and in no way conflict with each other when applied with this understanding. The starting point for any interpretation of how they interact is to examine the Charter text, considering, when necessary, the intentions of the drafters, as well as the object and purpose of the entirety of Charter provisions related to the use of force and the maintenance of international peace and security. Additionally, the nature and conditions of self-defense under customary international law are crucial to a correct interpretation and application of the right, since the Charter both recognizes its customary nature and does not seek to supplant or override the conditions laid down in customary law, except in so far as explicitly provided for in the Charter. The Charter drafters did not set out to recast the right of self-defense from scratch; instead they recognized the existence of the right and embedded it in the Charter system. This means that the right as it existed at the time the Charter came into force is the

5. The legal character of self-defense is set out and analyzed in D. W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW 3–25 (1958); IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 251 (1963); YORAM DINSTEIN, WAR, AGGRESSION AND SELF- DEFENCE 187–93 (5th ed. 2012); and C.H.M. Waldock, *The Regulation of the Use of Force by Individual States in International Law*, 41 RECUEIL DES COURS 455, 455–68 (1952). With regard to the premise that self-defense is a lawful response to unlawful force, see DINSTEIN, *supra* note 5, at 190 (quoting the decision of the U.S. Military Tribunal in United States v. Ernst von Weizsäcker et al., 14 TRIALS OF WAR CRIMINALS BEFORE THE NUERNBERG MILITARY TRIBUNALS 329 (1949)).

6. The inclusion of Article 51 in the UN Charter came at a relatively late stage in the negotiations leading to the Charter's adoption. It was added at the behest of Latin American States, which wanted to safeguard the right of mutual assistance arrangements in the event of attack. *See* BOWETT, *supra* note 5, at 182–83; LELAND GOODRICH, EDVARD HAMBRO & ANNE SIMONS, CHARTER OF THE UNITED NATIONS 342–44 (1969); Waldock, *supra* note 5, at 503–4.

right that is referred to as "inherent" in Article 51. In the absence of clear evidence to the contrary, there is no reason to assume that there was any intention to substantially alter the content of the right of self-defense in either the text of the Charter itself or in the negotiations leading to the incorporation of the right into the Charter. Therefore, since the Charter is silent on many aspects of the content of the right, an assessment of an invocation of self-defense must take into account the conditions contained in the Charter and customary law, as well as the factual considerations surrounding its invocation.[7]

B. Conditions Laid Out in the Charter

1. Armed Attack

The Charter predicates the exercise of the right of self-defense on the occurrence of an "armed attack." We will also examine the temporal dimension of an armed attack (that is, at what point in time does it occur), but for now we will concentrate on the question of what is an armed attack.

The Charter provides little or no guidance as to what constitutes an armed attack. To ascertain its meaning, we must look for guidance to customary law and supplementary sources, such as international jurisprudence. Based on these, an armed attack is considered to be a use of force originating outside the target State's territory that rises above the level of a small-scale, isolated armed incident or criminal activity, and which is directed against a State's territory, its military vessels or aircraft in international waters or airspace or lawfully present in another State's territory, or, in certain situations directed against its nationals located abroad.[8] It could also in-

---

7. The dual-legal basis of self-defense and the complementary relationship of the Charter and customary law were acknowledged by the ICJ in its *Nicaragua* decision. *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S), 1986 I.C.J. 14, ¶ 94 (June 27) [hereinafter *Nicaragua Judgment*]. The continued relevance of a preexisting rule of customary law in the absence of evidence of the emergence of a newer one regulating the same issue follows from general legal methodology and the doctrine of interpretation of legal sources. *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 3–4 (4th ed. 1990); 1 R.Y. JENNINGS & ARTHUR WATTS, OPPENHEIMS'S INTERNATIONAL LAW 25–26 (9th ed. 1992); Rudolf Bernhardt, *Customary International Law*, *in* 7 ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 61–62 (Rudolf Bernhardt ed., 2003).

8. The requirement that an armed attack originate from a source located or controlled outside a State's territory is generally acknowledged and non-controversial, as are the listed objects, which, if attacked, would constitute an armed attack, with the exception of a

clude a non-kinetic attack involving a use of force that resulted in more than nominal human casualties, or significant physical damage or destruction to either military or civilian objects.

Additionally, an armed attack could arguably include a cyber attack directed against a State's critical infrastructure, provided the cyber attack had the potential to severely cripple a State's ability to carry out and ensure the conducting of essential State functions or severely undermine its economic, political and social stability for a prolonged period of time. A number of States have adopted this position in their national cyber security strategies and many experts concur that an attack of this nature could potentially amount to a use of force rising to the level of an armed attack, although opinion is sharply divided.[9]

State´s nationals located abroad. The latter is controversial, with some authorities rejecting the position that an attack against a State's nationals abroad constitutes an armed attack, while others take the view that protection of nationals falls within the customary right of self-defense. There is a middle view which accepts that if nationals of a State are the target of threats to their lives or physical safety in order to obtain concessions or a change of policy from their parent State, this can constitute an armed attack. These views and the present authors' position are set out in Terry D. Gill & P.A.L. Ducheine, *Rescue of Nationals Abroad*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 4, at 217–19. On armed attack generally, see TOM RUYS, "ARMED ATTACK" AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE (2010).

9. The cyber strategies of several nations acknowledge the possibility of treating an attack that results in human casualties and/or significant physical damage as an armed attack justifying the exercise of self-defense. *See, e.g.,* U.S. Department of Defense, Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, at 4, 9 (2011), *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAASection 934Report_Forwebpage.pdf. The Advisory Council on International Affairs and the Committee on Issues of Public International Law in the Netherlands issued a 2011 joint report, "Cyber Warfare," that was adopted by the Netherlands Government. In this report, both a digital attack with comparable effects to those of a traditional kinetic attack and an attack upon critical infrastructure that produces severe and long-term effects were deemed as potentially triggering the right of self-defense. *See* ADVISORY COUNCIL ON INTERNATIONAL AFFAIRS & ADVISORY COMMITTEE ON ISSUES OF PUBLIC INTERNATIONAL LAW, CYBER WARFARE 21 (2011), *available at* http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf. In the Group of Experts that prepared the *Tallinn Manual,* there was unanimity that a cyber attack with comparable scale and effects to that of a kinetic attack which results in human casualties and physical damage or destruction could constitute an armed attack. The experts were divided, however, on the question whether a cyber attack without such physical

In that regard, it must be pointed out that there is currently insufficient State practice and official policy statements to conclude with certainty that an attack of this nature would amount to an armed attack in the absence of potential loss of life, physical injury or property damage. In the opinion of the authors, such an attack could so qualify under certain conditions. If the attack caused either physical damage or human injury of any significance, it would definitely so qualify. Additionally, even in the absence of physical injury or damage it could, in our opinion, constitute an armed attack, provided the potential disruption of a State's essential functions or stability was severe, long-term and incapable of being remedied within a reasonable time period.

An armed attack can be conducted in various ways, ranging from full-scale invasion to a series of small-scale uses of force conducted by the same author against the same target State that are reasonably connected in geographic and temporal terms and constitute what is, in effect, a phased armed attack.[10]

Some of these modes of attack are more relevant in the cyber context than others. This will receive further attention in a subsequent section.

2. Authorship of Armed Attack

There is general agreement that the potential authors of an armed attack include a State's armed forces and organized armed groups acting under the control of a State. Mere political or ideological sympathy, or diplomatic, logistical or material support for the organized armed group would not, in principle, constitute the requisite level of State involvement to be considered participation in the attack. If, however, a State's material or logistical support was substantial, it could potentially reach that level.[11]

---

effects, even one resulting in severe long-term disruption to critical infrastructure, could constitute an armed attack. TALLINN MANUAL, *supra* note 3, cmt. to rule 13, ¶¶ 6–9.

10. This is often referred to as the "accumulation of events" theory. It is also referred to as a "pin-prick" armed attack or "*Nadelstichtaktik*." *See, e.g.*, Yehuda Z. Blum, *State Response to Acts of Terrorism*, 19 GERMAN YEARBOOK OF INTERNATIONAL LAW 223 (1976); Paul Ducheine & Eric Pouw, *Operation Change of Direction: A Short Survey of the Legal Basis and the Applicable Legal Regimes*, *in* NETHERLANDS ANNUAL REVIEW OF MILITARY STUDIES—COMPLEX OPERATIONS: STUDIES ON LEBANON (2006) AND AFGHANISTAN (2006–PRESENT) 51, 61–63 nn. 49–82 (Michiel de Weger et al. eds., 2009).

11. *Nicaragua Judgment*, *supra* note 7, ¶¶ 195, 103. The views of one of the present authors on substantial involvement are set out in P.A.L. Ducheine & E.H. Pouw, *Legitimizing the Use of Force*, *in* MISSION URUZGAN—COLLABORATING IN MULTIPLE COALITIONS FOR

In addition to these two uncontroversial categories, there is increasing acceptance that an armed attack is capable of being carried out by an armed group not under the control of a State, but which instead acts autonomously with greater or lesser degrees of State tolerance and support that fall short of control or even influence.[12] Although some legal experts and court decisions cast doubt on whether such a group could carry out an armed attack, the better opinion in our view is that there are good grounds for not ruling out this possibility. Nothing in the Charter text relating to self-defense excludes it and this possibility has long been recognized in customary international law. There is also considerable recent State and international practice supporting this proposition and a wide degree of acceptance on the part of legal experts. More to the point is the fundamental consideration that the basic purpose of self-defense is to ward off armed attack. There are no compelling reasons to rule out the right of a State to exercise self-defense in the face of the clear ability of a number of armed groups to conduct an armed attack that is comparable in scale and effects to attacks conducted directly or indirectly by States.[13]

AFGHANISTAN 33, 40 (Rober Beeres et al. eds., 2012) and Ducheine & Pouw, *supra* note 10, at 67–69.

12. *See* Ducheine & Pouw, *Legitimizing the Use of Force*, *supra* note 11, at 39.

13. The UN Security Council implicitly recognized this possibility in Resolutions 1368 and 1373 by referring to "the inherent right of self-defense." S.C. Res. 1368, pmbl., U.N. Doc. S/RES/1368 (Sept. 12, 2001); S.C. Res. 1373, para. 4, U.N. Doc. S/RES/1373 (Sept. 28, 2001). Following the 9-11 attacks, NATO and the Organization of American States also recognized that attacks by armed groups could give rise to the right of self-defense. *See* Press Release, North Atlantic Treaty Organization, Statement by the North Atlantic Council (Sept. 12, 2001), *available at* http://www.nato.int/docu/pr/2001/p01-124e.htm; Terrorist Threat to the Americas, Res. 1, Twenty-Fourth Meeting of Consultation of Ministers of Foreign Affairs Acting as Organ of Consultation In Application of the Inter-American Treaty of Reciprocal Assistance, OEA/Ser.F/II.24, RC.24/RES.1/01 (Sept. 21, 2001). The ICJ cast doubt on whether an armed attack conducted by an armed group gave rise to the right of self-defense in the absence of State support in its advisory opinion on the *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J. 136, 194 (July 9), and its judgment in *Armed Activities on the Territory of the Congo* (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116 (Dec. 19). The latter decision was met, however, with vigorous criticism by a number of the judges in their separate opinions. A large number of recognized authorities believe an armed attack being conducted by a non-State entity in the absence of State control can give rise to the right of self-defense. *See, e.g.*, DINSTEIN, *supra* note 5, at 227–30; Michael N. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES—ESSAYS IN HONOUR OF YORAM DINSTEIN 157 (Michael N. Schmitt & Jelena Pejic eds., 2007). The views of one of the present authors

3. Requirements Related to the Security Council

In addition to the requirement of an armed attack, the Charter stipulates that actions of self-defense may only be carried out until such time as the Security Council has undertaken the measures necessary to restore international peace and security. This is the concrete manifestation of the primary purpose for including the right of self-defense in the Charter. It was not to definitively codify—much less invent—this long existing right, but rather to integrate it into the Charter system of collective security and provide a secure legal basis for collective self-defense treaty arrangements. The Council exercises primacy in the realm of the maintenance and restoration of international peace and security as reflected in, *inter alia*, Article 51 of the Charter.

Additionally, a procedural requirement to report measures of self-defense to the Council at the earliest possible opportunity is incorporated into this provision. It should be stressed that the requirement of reporting to the Council does not translate into a requirement to obtain prior authorization to exercise the right. Likewise, not just any action undertaken by the Security Council has the effect of terminating the right of a State to exercise self-defense. Only measures that are necessary (implying effectiveness when read in conjunction with Article 1(1) of the Charter) to restore peace and security and that are explicitly intended to terminate the exercise of the right by a State will have such effect.[14] It is the Council that decides whether the measures it has taken are sufficient to remove the necessity of exercising self-defense, but in the absence of an explicit intention expressed by the Council, for example, in the form of a cease and desist order, there is

---

are set out in more detail in Terry D. Gill, *The Temporal Dimension of Self-Defense Anticipation, Pre-emption, Prevention and Immediacy*, *in id.* at 113, 118. The essential reason giving rise to the possibility of responding in self-defense to an armed attack conducted by a non-State entity operating from the territory of a host State lies in the duty of States under international law to prevent their territory from being used to carry out actions that violate the rights of other States, including, in particular, the right to territorial inviolability and integrity. This duty of due diligence is part of customary law and was recognized, *inter alia*, in the *Island of Palmas* arbitral award (Island of Palmas (Neth. v. U.S.), 2 R.I.I.A. 829 (Perm. Ct. Arb. 1928)) and by the ICJ in the *Corfu Channel* judgment. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22–23 (Apr. 9).

14. *See* Gill, *supra* note 4, at 195–96.

no presumption that measures taken by the Council have the effect of terminating the right of self-defense in and of themselves.[15]

C. Conditions Laid Out in Customary International Law

Because self-defense has, as we have seen, a dual-legal basis, it is clear that it must conform to the conditions laid out in both sources. Under customary law, any exercise of self-defense must be carried out in a manner consistent with the principles of necessity, proportionality and immediacy. These were formulated in the diplomatic exchanges following the well-known 1837 *Caroline* incident, which has been described by Jennings as the *locus classicus* of the law of self-defense.[16] There is no mention of these principles in Article 51 for the simple reason that, as previously noted, it was not intended to comprehensively codify the law relating to self-defense. These criteria are of a customary nature and complement the requirements flowing from the Charter.

15. The primacy of the Council is evident from the text of Article 51, which, when read in conjunction with Articles 24 and 1, sets out the Council's authority in the maintenance of peace and the fundamental purpose of the Charter—the maintenance and restoration of international peace and security through effective collective measures. *See* DINSTEIN, *supra* note 5, at 238–39; Waldock, *supra* note 5, at 495–96; ROSALYN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 239–40 (1994). In Security Council Resolution 598, the Council ordered both parties to the Iran-Iraq War to stand down. S.C. Res. 598, ¶ 1, U.N. Doc. S/RES/598 (July 20, 1987). In contrast, in Resolution 1373, *supra* note 13, the Council adopted a whole range of mandatory measures not involving the use of force aimed at combating international terrorism, while at the same time affirming the right of self-defense in connection with the armed attack of 9-11. In the Desert Shield/Desert Storm operations of 1990–91, the right of self-defense continued to operate alongside—and was ultimately subsumed into—the collective measures adopted by the Security Council in Resolutions 660–678 (1990).

16. R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AMERICAN JOURNAL OF INTERNATIONAL LAW 82, 92 (1938). For a discussion of the principles of necessity and proportionality and their distinct meanings in the *ius ad bellum*, as opposed to their meaning in the context of other branches of the law, such as the law of armed conflict, see, e.g., JUDITH GARDAM, NECESSITY, PROPORTIONALITY AND THE USE OF FORCE BY STATES 10 (2004). *See also* DINSTEIN, *supra* note 5, at 231–33; OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 152–55 (1991).

1. Necessity

Necessity in the context of self-defense requires the existence of an armed attack that is ongoing or imminent and for which no other feasible alternative response exists.

An attack can be a single large-scale attack or a series of related small-scale attacks from the same source, which together form a single attack. It can also be a manifestly imminent attack in the proximate future, a point to which we will return below.

Alternatives can include measures short of self-defense when these are available. In the context of attacks by non-State actors, this includes exercising law enforcement measures whenever this is feasible and provides an adequate response. This is of particular importance with regard to a possible cyber armed attack conducted by a non-State actor with a greater or lesser degree of organization operating from a territory where the government is both willing and able to conduct or permit an effective law enforcement response. When the Security Council implements effective collective measures, the right of self-defense can be complemented by such measures, subsumed into them, or the right can be terminated when the Council so directs. A clearly expressed willingness to cease an attack, including compliance with ceasefire/withdrawal orders by the Security Council, coupled with adequate measures to ensure non-repetition and a willingness to conclude a comprehensive settlement of outstanding issues by peaceful means can also constitute an alternative to continued exercise of the right of self-defense.[17]

It should be emphasized that seeking or obtaining prior consent does not in general or as a matter of law form part of the principle of necessity. If an attack is ongoing (or as we will argue more extensively below is imminent), there is no requirement to obtain prior consent to exercise the right of self-defense. If an attack has not yet materialized, there is no necessity and, therefore, no right to exercise self-defense.

When armed attacks are being conducted by a non-State actor operating from one State's territory against another State and the non-State actor

17. Law enforcement measures are specifically and uniquely responses to attacks conducted by non-State groups. They can provide a feasible alternative in situations where the State from which the attack originated has control over its territory and is willing to undertake effective law means to address the threat. This would be the logical alternative to the use of trans-boundary armed force in self-defense. See the views of one of the present authors in Ducheine & Pouw, *Legitimizing the Use of Force, supra* note 11, at 64–65.

is neither under the control of the territorial State nor acting with its complicity, remedial action should be taken by the State where the non-State actor is located. This may take the form of adequate law enforcement measures or a proportionate recourse to armed force (either unilateral force or force used with the consent of the territorial State). If the territorial State consented, that consent would serve as a legal basis, in addition to or in place of self-defense, for the taking of action by the target State to forestall the attack.

2. Proportionality

Proportionality in the context of self-defense refers to the requirement that measures of self-defense must not exceed those required under the circumstances to repel the attack and prevent further attacks from the same source in the proximate future and that they must be roughly commensurate to the scale and aims of the overall attack. Hence, the scale and nature of the attack will determine what is required to repel or, if necessary, overcome it and prevent a continuation. A proportionate response to a single isolated armed attack would be measures to ward off the attack and prevent any direct and immediate threat of repetition. For example, a warship targeted by an anti-ship missile fired from a shore-based installation could take measures to ward off the attack and neutralize the immediate source of the attack. A more substantial, but still relatively limited, attack against a State's territory or military forces abroad would permit a response that warded off the immediate attack and forestalled repetition in the proximate future. A proportionate response to a full-scale armed attack, e.g., an invasion or large-scale offensive strike, would be a defensive war aimed at defeating the attacking party and removing the threat of further aggression.

Proportionality requires neither exact mathematical equivalency nor does it dictate the modality of exercising self-defense. If a digital attack rises above the threshold of armed attack, the response may be to employ cyber weapons or kinetic force or a combination of the two to neutralize the attack, as long as the response did not exceed that required to repel the attack. Proportionality does not permit measures that would needlessly prolong or exacerbate the conflict.[18]

18. See the authorities cited *supra* note 16. With regard to proportionality and the "accumulation of events" theory, discussed *supra* note 10 and accompanying text, see the report by Roberto Ago in his capacity as Special Rapporteur to the International Law Commission. Robert Ago, *Addendum to the Eighth Report on State Responsibility,* [1980] 2

3. Immediacy

Immediacy as a separate criterion for the exercise of self-defense refers to the requirement that self-defense measures, after taking the relevant circumstances into account, must not be unduly delayed. This requirement relates to the distinction between self-defense, which is a recognized legal basis for the use of force, and armed reprisal, which is unlawful under contemporary international law. Once an armed attack has occurred and the source of the attack determined, the defending State must proceed with its defensive measures as soon as it is capable of mounting a defense. This does not mean, however, that a response must necessarily be instantaneous to be lawful. A State will need to explore whether there are feasible alternatives to the use of force in instances when it is not readily apparent that there are none. It may need to deploy forces to the source of the attack, mobilize forces that are not in a state of instant readiness, consult with allies and receive assistance in order to be able to respond, identify the attacker when this is not readily evident. The latter requirement is particularly relevant in the cyber context, as well as in certain other types and modes of attack. The important point is that self-defense is exercised within a reasonable timeframe in response to an ongoing attack or, as we will demonstrate below, a clear threat of attack in the proximate future. It is not a punitive measure to be undertaken long after the attack has been carried out. A State does not, however, forfeit its right of self-defense because it is incapable of instantly responding or is uncertain of who is responsible for the attack or from where the attack originated.[19]

4. Evidence

In addition to the necessity, proportionality and immediacy principles, there must be credible evidence as to the identity of the attacking party and the source of the armed attack before measures in self-defense can be taken. International law does not have a comprehensive set of universally recognized evidentiary standards to apply in determining whether a defensive

---

YEARBOOK OF THE INTERNATIONAL LAW COMMISSION pt. 1, 13, 69–70, U.N. Doc. A/CN.4/318/ADD.5-7 (1980).

19. With respect to immediacy as a general criterion for the exercise of self-defense, see Gill, *supra* note 13, at 151–54.

response is permitted in situations where the identity and source of the attack is not readily apparent.[20]

In traditional attacks involving the armed forces of one State attacking the forces or territory of another State, the identity of the attacking party will usually be readily apparent. There was clearly no doubt of the identity of the attacking State at Pearl Harbor in 1941 and the invading State in Kuwait in 1990. However, in situations where an armed group acts as either a proxy of a State or on its own to carry out an armed attack or series of attacks, it may be less than clear who or what is behind the attack, particularly when the author of the attack denies involvement. The case law of the International Court of Justice in rejecting "suggestive" and "highly suggestive" evidence seems to point to a stringent level of proof, but there is less than full agreement within the Court and the international community at large as to the accuracy of the standard it employs.[21]

The requirements for evidence in the criminal justice system of most States and before international criminal tribunals would hardly be feasible or realistic when acting in self-defense.[22] Nevertheless, there must be reasonably credible and convincing evidence of involvement before a State can take measures in self-defense against a particular State or entity such as an armed group suspected of perpetrating an armed attack in instances where the identity of the attacker is not readily apparent.

D. The Temporal Dimension: Anticipatory Self-Defense

We will now turn to the question whether international law permits the exercise of measures of self-defense in response to an imminent or potential armed attack.

Before presenting our views, it is necessary to clarify some terminology. In this article, the term "anticipatory self-defense" denotes defensive

---

20. The ICJ employed a stringent standard that rejected "suggestive" and "highly suggestive" evidence of Iranian involvement in attacks on international shipping in the Persian Gulf. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 59, 71 (Nov. 6). This and other aspects of the judgment were vigorously criticized by a number of judges in their individual opinions. *See id.*, ¶¶ 30–39 (separate opinion of Judge Higgins); *id.*, ¶¶ 21–30 (separate opinion of Judge Kooijmans); *id.*, ¶¶ 33–46 (separate opinion of Judge Buergenthal); *id.*, ¶¶ 33–40 (separate opinion of Judge Owada).

21. *Id.*

22. There is no generally accepted "law of evidence" in international law. Standards differ between criminal tribunals and other international decision making bodies, e.g., arbitrations.

measures undertaken in response to a manifest and unequivocal threat of attack in the proximate future. The term "*preemptive* self-defense" is synonymous. The term "*preventive* self-defense" signifies a defensive response to an inchoate or potential threat of attack at some indeterminate point in the future.

There is at present no universal consensus on the legality of either of these modes of exercising self-defense in advance of an actual attack.[23] It is nevertheless fair to say that the former mode (anticipatory or preemptive self-defense) enjoys widespread support among a significant number of States and in juridical opinion, while preventive self-defense is much more controversial.[24]

In our view, anticipatory self-defense has long been recognized in customary international law. The existence of an anticipatory element in self-defense is, moreover, part of the essence of the right of self-defense in that forestalling continued attack, in addition to responding to an ongoing attack, is part of the necessity and proportionality criteria that are integral elements of self-defense. In that sense, self-defense is both forward looking, by securing the defending State from future attack, as well as reactive, by repelling an attack in progress. Any other rendition would leave a defending State in an untenable and highly vulnerable position; one which, would put it in an unequal position *vis-à-vis* the attacking party. This neither makes sense nor does justice to the purpose underlying the right of self-defense.

The recognition of this anticipatory element can be traced back to the previously mentioned *Caroline* incident. In the diplomatic correspondence following that incident, the general conditions for the exercise of self-defense, including its temporal dimension were set out. These were, in nineteenth century prose, "a necessity of self-defense, instant, overwhelming and leaving no choice of means and no moment for deliberation."[25]

---

23. For a clear discussion of the controversy concerning the temporal aspect of self-defense, see KINGA T. SZABO, ANTICIPATORY ACTION IN SELF-DEFENCE 6–8 (2011).

24. On the legality of preventive self-defense, see High-Level Panel on Threats, Challenges and Change, *A More Secure World: Our Responsibility*, U.N. Doc. A/59/565 (Dec. 2, 2004); U.N. Secretary-General, *In Larger Freedom: Towards Development, Security and Human Rights for All*, U.N Doc. A/59/2005, 59th Sess., (Mar. 21, 2005).

25. On the *Caroline* incident, see MICHAEL BYERS, WAR LAW 53–54 (2003); BROWNLIE, *supra*, note 5, at 42–43; DINSTEIN, *supra* note 5, at 197–98; THOMAS FRANCK, RECOURSE TO FORCE 97–98 (2002). The most authoritative article on the *Caroline* incident remains without doubt that by R.Y. Jennings, *supra* note 16. The primary source for information on the *Caroline* incident and the exchange of correspondence between Webster

This formulation of the general conditions for the exercise of anticipatory self-defense is widely regarded as authoritative and has had a lasting influence, although not without a certain degree of divergence of opinion as to how literally the wording used should be taken. There is also disagreement among authorities and States as to whether it is a valid precedent and, even if it is, whether anticipatory self-defense is still lawful under the UN Charter regime.

This is not the place to delve into the historical value of the *Caroline* incident in depth, but two points deserve attention. First, it is sometimes argued that since *Caroline* took place in an era and under a legal regime in which war was lawful, it is of little relevance under the present day Charter legal regime in which not only war, but the use of force are prohibited, barring strict exceptions. This critique, it is submitted, is incomplete and, therefore, incorrect. While it is true that recourse to war was lawful in the nineteenth century legal order, the attack on the *Caroline* did not constitute a war. The use of trans-boundary force below the threshold of war (often referred to as "measures short of war") required a legal justification in the pre-Charter legal order. Acts involving a use of force that fell outside the legal context of a "state of war," either declared or factual, such as various types of intervention, hot pursuit of armed bands over a frontier, pacific blockade and armed reprisal, were then regulated in international law—as they are now—although many of the legal rules relating to these uses of force were substantially different in the nineteenth century than they are under the Charter. Nevertheless, it is erroneous to conclude that because war was lawful in the international law of the nineteenth century, that legal justifications for using force were irrelevant.

Nor is it convincing to argue that since the British action was directed against a non-State entity (groups of American nationals acting without U.S. sponsorship who sympathized with the rebellion taking place in British North America), it falls under the rubric of "state of necessity" rather than self-defense. The diplomatic correspondence referred to self-defense as the justification, not necessity, and it was viewed as such by both parties to the dispute. More recently, the decisions of the Nuremburg and Tokyo tribunals held following the conclusion of World War II cited the *Caroline* incident in analyzing claims of self-defense by German and Japanese defendants. Moreover, the critique reflects a position that self-defense can

---

and Fox is found in 29 BRITISH AND FOREIGN STATE PAPERS 1129, 1137–38 (1840–41), and between Webster and Ashburton, found in 30 BRITISH AND FOREIGN STATE PAPERS 195, 195–96 (1841-42).

pertain only to attacks conducted by a State or by an armed group under the control of a State: that interpretation was not the law then, nor does it, as discussed above, reflect current practice. Finally, notwithstanding significant divergences between the nineteenth century law on the use of forcible measures short of war and the contemporary legal order, the principles of necessity, proportionality and immediacy, which were agreed to by both States in the *Caroline* incident, have not undergone significant transformation and are still of undisputed relevance today in the context of self-defense, although the circumstances in which they are applied may have altered significantly in some situations.[26]

Second, as regards the precedential value of the *Caroline* formula, it is undisputed that the references made to it in the Nuremburg and Tokyo trials reflect a conviction that it represented customary international law at the very time the Charter was drafted and entering into force.[27] Without

---

26. On the nineteenth century law relating to the use of force short of war, see STEPHEN C. NEFF, WAR AND THE LAW OF NATIONS: A GENERAL HISTORY 156 (2005) and SZABO, *supra* note 23, at 69–77. The right of self-defense in the nineteenth century was related to both the natural law concept of "imperfect war" and the broader notion of self-preservation. Szabo rightly points out that the nineteenth century notion of self-defense referred to in the *Caroline* incident included an intrinsic anticipatory element, therefore, there was no separate category of anticipatory self-defense at that time. *Id.* at 75. The opinions of commentators as to the relevance of customary law and pre-Charter precedents, such as the *Caroline* incident, can be roughly divided into two schools. One, exemplified by such writers as BROWNLIE, *supra* note 5, at 25; DINSTEIN, *supra* note 5, at 188–89; and CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 86–88 (2000), largely or wholly discount the relevance of pre-Charter practice relating to self-defense because it took place in an era when recourse to force was not unlawful. Others, such as BOWETT, *supra* note 5, at 269; FRANCK, *supra* note 25, at 45; and Waldock, *supra* note 5, at 455, take a wider view and consider pre-Charter practice as relevant.

27. For the Nuremburg judgment on the relevance of the *Caroline* criteria to the German plea of preventive self-defense in connection with its invasion of Norway, see 22 TRIAL OF THE MAJOR GERMAN WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL 448–50 (1948), *available at* http://www.loc.gov/rr/frd/ Military_Law/pdf/NT_Vol-XXII.pdf. For the assessment of the declaration of war by the Netherlands on Japan, see JUDGMENT OF THE INTERNATIONAL MILITARY TRIBUNAL FOR THE FAR EAST 379–84 (1946). The Japanese did not commence operations directly against the Netherlands East Indies until January 11, 1942, over a month after the attack on Pearl Harbor, because they first had to deal with American and British forces in the Philippines, Hong Kong and Malaya. The Tribunal pointed out that it was evident from the scale of the Japanese offensive across the Pacific and Southeast Asia that the Netherlands East Indies were going to be attacked as soon as it was practicable, and that, in fact, plans to that effect had been made prior to the attack on Pearl Harbor. Obviously, the plans were not made public so the Netherlands was unaware of them at the time. Nevertheless, the

firm evidence that customary law has evolved in a different direction since then, there is no reason to assume the present legal regime no longer allows for some degree of anticipatory self-defense.[28] Stated differently, if international law relating to the exercise of self-defense in the period in which the Charter was adopted contained an anticipatory element, then the assumption would be that it continues to exist, unless it could be conclusively shown that it had been subsequently altered, with the burden of proof resting on those who hold the law has changed.

Certainly, more is required than simply stating that the wording of Article 51 of the UN Charter, with its phrase "if an armed attack occurs," categorically rules out anticipatory self-defense, since the wording itself sheds no light on either what constitutes an armed attack or when it can be said to have occurred. If one assumes an armed attack only occurs when a particular use of force physically passes an international boundary, there would, indeed, be no scope for anticipatory self-defense. However, this is not the only, nor necessarily the most convincing, interpretation of the meaning of the "occurrence" of an armed attack.

In both the nineteenth century and at the time the Charter was adopted, armed attack was considered to include clear and manifest preparations, even the intention to attack in the proximate future, when their existence was supported by clear evidence. The Nuremburg Tribunal rejected the German defendants' plea of self-defense as justifying the invasion of Norway in April 1940, not because it rejected the possibility of preemption as such, but because the evidence clearly pointed to motives other than self-defense. The Tribunal held that the basis for self-defense was lacking even though the Allies had contemplated a possible intervention in northern Norway to come to the assistance of Finland, which was being attacked by the Soviet Union at the time, and to interdict the shipment of Swedish iron ore to Germany, because Germans were not aware of these contingency plans when they carried out the invasion.

Dutch declaration of war enabled the formation of a joint defensive effort by U.S., British, Australian and Dutch forces in Southeast Asia. The Tribunal deemed it to be defensive in character in accordance with the *Caroline* criteria in response to an aggressive war launched by Japan. For a chronology of the Japanese offensive against the Netherlands East Indies and the formation of the joint defense by the Allies, which culminated in the defeat of Dutch, U.S., Australian and UK naval forces in the Battle of the Java Sea and the completion of the conquest of the Netherlands East Indies by March 1942, see RICHARD E. DUPUY & TREVOR N. DUPUY, THE ENCYCLOPEDIA OF MILITARY HISTORY 1132, 1138 (2d ed. 1986).

28. See sources cited *supra* note 7. *See also* SZABO, *supra* note 23, at 125.

Likewise, the Tokyo Tribunal held the declaration of war by the Netherlands against Japan immediately after the attack on Pearl Harbor, which occurred well before the Japanese commenced military operations against the Dutch East Indies, did not give rise to a right of self-defense by Japan. It so held because it was evident that the scale of the Japanese offensive throughout the Pacific and East Asia was so comprehensive as to include the intention to capture the Dutch colony once it had been reached, after overcoming resistance elsewhere, in order to secure the valuable natural resources located there that were vital to the Japanese war effort. In short, an armed attack was considered to have "occurred" at a time it was evident an attack was going to take place in the near future, even though this was well before any forces ever crossed the frontier, or even concrete measures—as opposed to preparations—had been taken to initiate an attack against Dutch-administered territory. That is the definition of anticipatory self-defense as it comes to current international law from the *Caroline* formula; it is essentially taking action within the last feasible "window of opportunity" once the intention and capability to mount an attack have become clear.[29]

Since the adoption of the Charter, there have been references by States to the existence of the right of anticipatory self-defense on various occasions and in various contexts. While certain invocations have not met with general acceptance, others have. It is particularly noteworthy that no international court or tribunal, nor the Security Council, has ever ruled out recourse to anticipatory self-defense within the general confines of the *Caroline* formula as a matter of law. For that matter, the General Assembly has never made any such pronouncement: neither in the well-known 1970

29. The clear distinction between self-defense, including warding off the manifest danger of impending attack, and preventive self-defense (which is a contradiction in terms since it is based on the mere belief that an attack *might possibly* occur at some indeterminate point in the future and *might possibly* be directed against an indeterminate target State) is the existence of a necessity to act when no feasible sufficient alternatives to defensive force are available. The principles of necessity and immediacy are what set self-defense apart from other uses of force. In this context, necessity and immediacy do not necessarily translate into a specific time period in which a State faced with the clear and present danger of an impending attack must act, but they must be seen in context and are tied to the lack of feasible alternatives. While, in general, the longer the period before an attack is launched the less likely it is that there will be no feasible alternatives, this is not always the case as is demonstrated in, *inter alia*, the Dutch declaration of war against Japan, where the intention and capability to conduct an attack were clear and convincing. For the concept of the "last window of opportunity," see, e.g., TALLINN MANUAL*, supra* note 3, rules 14 & 15 with commentary.

"Friendly Relations" declaration, which restated and interpreted the basic principles of the Charter, nor in the 1974 "Definition of Aggression" declaration, which serves as the basis for the definition of the crime of aggression in the Rome Statute of the International Criminal Court.[30]

In addition, the well-respected *Institut de Droit International* and the High-Level Panel on Threats, Challenges and Change, which advised the UN Secretary-General in 2004, have taken the position that anticipatory self-defense within the parameters of the *Caroline* criteria is permissible under contemporary international law.[31]

In conclusion, there is ample evidence that the right of self-defense contained an anticipatory element at the time the Charter was adopted and that it continues to do so now. In the absence of conclusive evidence that the law has been altered since the Charter entered into force, there is no reason to assume that anticipatory self-defense when exercised within the confines of the *Caroline* criteria has become unlawful.

III. ANTICIPATORY SELF-DEFENSE AND A CYBER ARMED ATTACK

A. Cyber Armed Attack: Likelihood and Possible Modalities

Having set out the applicable legal framework in the previous section, we will now proceed to apply it to a cyber attack that rises to the level of an armed attack in a legal sense. Two things should be pointed out at the outset. First, the term "cyber attack," as it is widely used in the media and by members of the cyber community, is not necessarily synonymous with the notion of armed attack under the international law of self-defense. In the vast majority of cases, incidents referred to as a "cyber attack" have not constituted a use of force, much less one rising to the threshold of an armed attack. The denial-of-service "attack" on Estonia in 2007, which resulted in a few hours of disruption and inconvenience, and numerous examples of cyber break-ins, espionage, sabotage and theft of data and intel-

30. Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. Doc. A/8082 (Oct. 24, 1970); Definition of Aggression, G.A. Res. 3314 (XXIX), U.N. Doc. A/RES/3314 (Dec. 14, 1974), Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90.

31. High-Level Panel, *supra* note 24, ¶¶ 188, 54 (Dec. 2, 2004); W. Michael Reisman, Report, Tenth Commission, *Present Problems of the Use of Armed Force in International Law*, 72 ANNUAIRE DE L'INSTITUT DE DROIT INTERNATIONAL 237 (2007).

lectual property constitute neither a use of force nor an armed attack.[32] Indeed, it is very probable that no breach of cyber security loosely referred to as a "cyber attack" has to date reached the level of an armed attack in a legal sense.[33] That is our position, since, to our knowledge, none has been so regarded in State practice and none has resulted in death, injury or significant long-term material damage to critical infrastructure on which the functioning of a State depends. The only example that might be viewed otherwise is Operation Olympic Games,[34] or Myrtus as it was also known,[35] the Stuxnet cyber attack on the Iranian nuclear weapons program during the period 2008–10 that reportedly caused a measure of physical damage to the centrifuges engaged in the enhancement of nuclear material.[36] While this may be an arguable example of an armed attack, in our view it is better treated as an example of mere sabotage not amounting to an armed attack, since it neither resulted in physical injury or death to persons, and the damage had no wider, long-term or serious secondary effects beyond apparently delaying the progress of the Iranian nuclear program for several months. This could hardly be deemed to constitute critical infrastructure[37] damage seriously impairing the functioning of the State or the stability of Iranian society.

1. Stand-alone Cyber Attack

Second, while the possibility of a stand-alone cyber attack, that is, one not occurring in conjunction with an attack employing traditional kinetic force, rising to the level of an armed attack cannot be ruled out, it is not in our

32. For an overview, see, e.g., Thomas Rid, *Cyber War Will Not Take Place*, 35 JOURNAL OF STRATEGIC STUDIES 1, 5–32 (2012) *reprinted in* CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 2, ch. 4.

33. *Id.* at 75.

34. DAVID SANGER, CONFRONT, & CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER (2012).

35. Rid, *supra* note 32, at 85.

36. *See, e.g.*, David P. Fidler, *Was Stuxnet an Act of War? Decoding a Cyberattack*, 9 IEEE SECURITY AND PRIVACY MAGAZINE 4, 56–59 (2011); Michael.J. Gross, *A Declaration of Cyber-War*, VANITY FAIR, Apr. 2011, at 152, *available at* http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.print.

37. Iran is not dependent on nuclear energy. According to the CIA World Factbook, Iran's electricity consumption is generated from fossil fuels (86.1%) and hydroelectric plants (13.7%). CENTRAL INTELLIGENCE AGENCY, THE WORLD FACTBOOK, https://www.cia.gov/library/publications/the-world-factbook/geos/ir.html (last visited July 30, 2012)

view the most likely form of attack.[38] The majority of potential cyber attacks are not likely to cause physical casualties or significantly degrade a State's critical infrastructure for a significant period of time, although undeniably some could have that capability. The exaggerations of so-called "cyber doom scenarios" have been compared to air-power theorists prior to and during World War II, who took the position that strategic bombing on its own could bring about the complete destruction of a State and its social fabric. They have also been attributed to the psychological aftermath of the 9-11 attack and to longstanding inchoate fears of technology and its potential effects that predate the digital age, but which have gained new adherents as the result of the dependency of contemporary society on digital systems.[39]

Be that as it may, no cyber attack on its own has to date constituted an armed attack. While the possibility of a cyber armed attack can and should not as a matter of prudence be ruled out, it should not be confused with real cyber security threats that do take place on an ongoing and regular basis in the form of cyber espionage, cyber sabotage and cyber criminal activity aimed at both public and private computer systems. However, as serious as these threats may be to a State's national and economic security, they do not constitute armed attacks that would justify the use of force in self-defense.

Only cyber attacks having direct secondary effects resulting in physical casualties, substantial physical damage, or such substantial and long-term damage to critical infrastructure that the carrying out of a State's essential functions or its social and political stability are seriously impaired should, we submit, be treated as armed attack in the sense of the law relating to the exercise of self-defense. While an attack of this magnitude is feasible and

38. In general, a cyber sabotage attack against the supervisory control and data acquisition (SCADA) system of chemical plants, could result in damage, e.g., the leakage of poisonous gasses. There is a potential for a more serious incident when plants are situated closely to densely populated areas, as is the case in the Netherlands where Royal Dutch Shell's chemical installations are close to the port and city of Rotterdam. According to Rose Tsang, however, "it is unlikely such an [intentional] attack [by an individual or small group of individuals] would result in a wide-scale failure of the critical infrastructure." Rose Tsang, *Cyberthreats, Vulnerabilities and Attacks on SCADA Networks* 21 (University of California, Goldman School of Public Policy, Working Paper, 2009).

39. *See* Sean Lawson, *Beyond Cyber Doom—Cyber Attack Scenarios and the Evidence of History*, 10 JOURNAL OF INFORMATION TECHNOLOGY & POLITICS 1, 4 (2013), *reprinted in* CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 2, ch. 13.

cannot be wholly discounted, the unlikelihood of it occurring should be kept in mind.[40]

2. Combined Attack: Cyber Operations and Kinetic Attack

If stand-alone cyber armed attacks are probably less likely to occur than is sometimes conjectured, what other options are there? In our view, the most likely is an armed attack involving cyber operations carried out in conjunction with a traditional use of kinetic armed force. There are two known instances where this has occurred.

One was during the armed conflict between Russia and Georgia in August 2008, when Georgia initiated armed action against South Ossetian separatists and Russia intervened militarily, forcing the Georgian armed forces to withdraw.[41] For purposes of this article, we are not concerned with the legality of the use of force by either side to the conflict, rather our focus is on the cyber operations conducted by Russian State agencies and/or supportive patriotic hackers (there was no clear evidence as to who was responsible). These were limited in effect and duration and did not constitute an armed attack. If, however, they had gone beyond mere defacing of government websites and inconveniencing the public and certain public bodies, to, e.g., support military operations by degrading or neutralizing weapons and military communications systems, in that case they would have constituted armed attacks. If used in such a manner, it would have been part of an overall armed attack involving the use of traditional military force that included the employment of cyber techniques as an adjunct to, or preparation for, the kinetic attack.

That is what apparently occurred in Operation Orchard, when Israel carried out an airstrike against the Al-Kibar nuclear facility in northern Syria in September 2007.[42] The airstrike was seemingly accompanied by the

40. The authors share the view expressed by Tsang, *supra* note 38.

41. *See* ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010); Keir Giles, *"Information Troops"—a Russian Cyber Command?*, *in* 3RD INTERNATIONAL CONFERENCE ON CYBER CONFLICT 45, 46 (Christian Czosseck, Enn Tyugu & Thomas Wingfield eds., 2011).

42. Andrew Garwood-Gowers, *Israel's Airstrike on Syria's Al-Kibar Facility: a Test Case for the Doctrine of Pre-Emptive Self-Defence?*, 16 JOURNAL OF CONFLICT AND SECURITY LAW 263 (2011). Daveed Gartenstein-Ross & Joshua D. Goodman, *The Attack on Syria's al-Kibar Nuclear Facility*, INFOCUS QUARTERLY, Spring 2009, *available at* http://www.jewishpolicycenter.org/826/the-attack-on-syrias-al-kibar-nuclear-facility; *Isra-*

use of cyber electronic warfare that reportedly neutralized the Syrian air defense system and enabled the airstrike to be carried out successfully.[43] Again, without addressing the question of whether this act was a lawful exercise of self-defense, it is a clear illustration of an armed attack in which cyber capabilities were used alongside traditional kinetic armed force as a means of "preparing the battlefield," thereby creating favorable circumstances for the overall success of the operation. This type of cyber operation will almost inevitably become more prevalent as more States obtain the capacity to effectively utilize cyber as an adjunct to traditional kinetic force and integrate it into their operational doctrine and practice.[44] Armed forces will start—as some have already started—to ensure a coherent integration of cyber capabilities across the spectrum of military operations.[45]

In our view, the combination of cyber and kinetic attacks is a far more likely scenario than a stand-alone cyber armed attack. There are several reasons why a stand-alone cyber attack rising to the level of an armed attack is considerably less likely than a combined attack.

On the one hand, if the attack were part of a large-scale offensive comprising a concerted series of attacks, it is unlikely that the attacking State would rely solely on one particular form of attack. A stand-alone "cyber Pearl Harbor" scenario is, therefore, highly unlikely, since an attack on that scale as the opening move in a full-scale war would inevitably trigger a large-scale kinetic response. Thus, it would make little sense to limit the initial attack to a cyber attack. If a State, having decided to go to war, employed cyber in such a large-scale attack that it amounted to the com-

---

el Admits Air Strike on Syria, BBC NEWS (Oct. 2, 2007, 17:12 GMT), http://news.bbc.co.uk/2/hi/7024287.stm.

43. David A. Fulghum & Douglas Barrie, *Israel Used Electronic Attack in Air Strike Against Syrian Mystery Target*, AVIATION WEEK, Oct. 8, 2007, at 28, *available at* http://www.freerepublic.com/focus/f-news/1908050/posts.

44. For national military doctrines, see ENEKEN TIKK, FRAMEWORKS FOR INTERNATIONAL CYBER SECURITY, NATIONAL CYBER SECURITY POLICIES AND STRATEGIES (2011).

45. *See* PRIME MINISTER DAVID CAMERON, SECURING BRITAIN IN AN AGE OF UNCERTAINTY: THE STRATEGIC DEFENCE AND SECURITY REVIEW 27 (2010), *available at* http://www.official-documents.gov.uk/document/cm79/7948/7948.asp ("Future conflict will see cyber operations conducted in parallel with more conventional actions in the maritime, land and air environments.").

mencement of the war, it would most likely be in conjunction with other means of attack to ensure the maximum effect was realized.[46]

If, on the other hand, a cyber operation was employed against a single discrete target, it would more than likely take the form of either an act of cyber espionage or sabotage below the threshold of armed attack, as in the Stuxnet scenario, or be used in support of a kinetic attack if the intention was to destroy the target, as was the case with the 2007 Israeli airstrike on the Al-Kibar nuclear facility. A stand-alone cyber attack that actually caused a significant degree of physical damage to an installation or resulted in human casualties, thereby constituting an armed attack, would not necessarily destroy a target.

Moreover, using cyber alone as a means of inflicting significant physical damage or substantial loss of life would almost certainly increase the risk of miscalculation and escalation, because of the degree of unpredictability and relative anonymity of a cyber attack. Additionally, the probable psychological impact of an attack on one specific target would seem senseless for political and military purposes or in legal terms, assuming these mattered to the actor involved. A more likely course of action in a cyber operation intended to degrade a particular target would be to stay below the threshold of an armed attack, thereby allowing an actor that wished to degrade a particular target to do so with much less risk of a forcible response and to maintain denial of direct involvement, as was the case with Stuxnet. In sum, if the desired end state was destruction of a target, cyber would not be the method of attack most guaranteed to succeed, while if the objective was merely to obtain information or degrade a target without destroying it and risking escalation, it would not require a cyber attack that rose to the level of an armed attack.

3. Rational Actor

Of course, this discussion has assumed the actor is reasonabe and acts with rational motives and objectives, whether they are legal or illegal. The proverbial "genie in the bottle" is, of course, a large-scale act of cyber terrorism that has the potential effect of causing massive loss of life or physical destruction. Examples often used are attacks on a nuclear power plant aimed at shutting down its cooling system and causing a Fukushima-type

46. Some authors refer to Chinese military doctrine in this respect. *See, e.g.*, Han Bouwmeester, Hans Folmer & Paul Ducheine, *Cyber Security and Policy Responses*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 2, at 19, 36.

disaster, on an air traffic control system with the objective of causing a large number of aircraft to crash and on a flood control system triggering a massive and disastrous flood.[47] An attack such as one of those carried out by a nihilistic actor, e.g., Al Qaeda or one of its affiliates that had no regard for the consequences is potentially more plausible than an attack of this nature conducted by a State. Such an attack would undoubtedly rise to the level of an armed attack and it would not necessarily be part of the more comprehensive armed offensive that a State would be likely to employ.

A cyber "Armageddon" is not, however, as likely as sometimes suggested.[48] First, conducting a cyber armed attack on this scale is not readily within the capabilities of non-State organizations and obtaining the capability to do so is not easily accomplished. It would require a major effort, involving considerable time, technical and trained human resources, and probably the support of a State with sophisticated cyber capability for a terrorist organization to develop the capacity to achieve devastating results through the use of cyber alone. Second, the logical question is why a terrorist organization would make that effort when there are other more achievable means to produce similar results. Al Qaeda did not have to take over the air traffic control center at Kennedy International Airport in New York City to achieve the effect it did on 9-11. Instead it seized physical control of four aircraft, a capability more likely for a terrorist organization to possess than that necessary to initiate a major cyber attack. Nevertheless, although not likely, a major attack is feasible and the possibility of a terrorist organization obtaining the necessary capacity to conduct such an attack should not be discounted.

B. Responding to an Anticipated Cyber Armed Attack in Conformity with the Law

Having explored the likelihood of a cyber attack constituting an armed attack when conducted either in conjunction with the use of traditional kinetic military force or as a stand-alone attack, we next turn to an assessment of the manner in which the legal framework governing the exercise of the right of self-defense addressed in Section II would be applied in responding to a clear threat of a such an attack. We will do so on the basis of the conclusion reached previously that anticipatory self-defense is a lawful exercise of the right of self-defense when exercised in response to a manifest and

47. MYRIAM D. CAVELTY, CYBER-SECURITY AND THREAT POLITICS 2 (2007); RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR 64–68 (2010).

48. *See* Lawson, *supra* note 39.

unequivocal imminent threat of attack in the proximate future against a designated target State or States, as these criteria are laid down in the Charter and are contained in customary international law.

1. Combined Cyber and Kinetic Attacks

With regard to what we consider to be the most likely mode of cyber armed attack, namely, that occurring in conjunction with the use of kinetic force, there are no real differences from the manner in which the criteria for the exercise of anticipatory self-defense are applied to traditional means and methods of attack conducted without the use of cyber. The assessment of the likelihood of an imminent attack and the identification of the author of the attack, both based on credible evidence, and the gauging of a proportionate response would not differ in any meaningful way.

For example, if State A was clearly on the point of launching an attack against State B, and State B responded by launching a preemptive airstrike that destroyed a considerable portion of State A's air capability on the ground and command and control functions before the attack was launched, thereby gaining air superiority, it would make little or no difference whether either the attacking State A and/or defending State B employed or did not employ cyber weapons or techniques to assist their operations in terms of assessing the legality of the response.

The questions concerning the legality of the anticipatory response would be exactly the same with or without the use of cyber by either State. Was the evidence of an imminent attack credible? Were there available alternatives under the circumstances? Did the defender strike within the last feasible window of opportunity? Was the strike precipitate, therefore premature, because it was conducted before the evidence of attack was clear, before alternatives to the use of force were exhausted or before a determination was made that possible alternatives were not feasible under the circumstances? Was the response proportionate in relation to the reasonable evidence of the scope and nature of the threat?

The use of cyber weapons in such a scenario would have little or no influence on the answers to these questions and would, therefore, have equally little bearing on whether the response was in conformity with the law or not. In short, when cyber is employed alongside other means and methods of warfare, it will not significantly affect the outcome of an assessment of a preemptive response as a lawful or unlawful act of anticipatory self-defense.

The problem of identification of the potential attacker would not be increased if cyber weapons and techniques were employed in the attack since evidence of those preparations would be weighed together with physical indications of an impending attack. In fact, cyber activities might make identification of the attacking party easier if, for example, previous cyber espionage probes of the defending State's capabilities and deployments could be traced back to a State now demonstrating clear indications of preparation for an attack. This would be no different, in principle, from the use of electronic warfare techniques to intercept and decode messages indicating an attacking party's intentions.

2. Stand-alone Cyber Attack

In contrast to the cyber attack undertaken in conjunction with a kinetic attack, preparations for a stand-alone cyber attack would, in most cases, significantly affect the ability to act in anticipatory self-defense. To illustrate, assume actor A (a State or non-State actor) is on the point of launching the attack against State B and that State B is able to determine a digital attack on its critical infrastructure is being prepared. State B's right to launch a preemptive digital and/or kinetic defensive response in accordance with the criteria for the lawful exercise of anticipatory self-defense would depend entirely on its capacity to identify the prospective attacker and ascertain the attacking party's intentions and capabilities. In the absence of physical indicators, such as force deployments, aerial reconnaissance and intercepted communications, it would be exceedingly difficult, if not impossible, for a prospective target State to be able to identify the attacking party, ascertain the existence and nature of the threat, and gauge the necessary and proportionate response with a reasonable degree of certainty.

3. Accumulation of Events

There may be situations in which it is feasible for a State to determine the origin of an attack, perhaps because of reliable human or other intelligence, or other clear evidence, such as positive identification of the source of a prior attempt to carry out a similar, partially unsuccessful cyber attack. In that situation, the response would not be wholly anticipatory, since the attempted attack could be considered as continuing. This analysis would also apply to situations in which there had been a prior series of small-scale

digital attacks from the same source falling below the threshold of armed attacks that occur over a reasonably connected span of time—for example, a series of small-scale attacks to ascertain a defending State's vulnerabilities and capabilities. These attacks, taken together, comprise an attack of sufficient gravity to qualify as an armed attack justifying an exercise of self-defense to ward off the phased attacks and neutralize the threat of further attack.

Responding in self-defense to these small-scale digital attacks represents an application of the "accumulation of events" theory to a "*Nadelstichtaktik"* form of armed attack.[49] The defensive response in such a scenario would have both a reactive and anticipatory element, with the former predominating since it would be reacting to an ongoing attack, but it would also be forward looking by warding off further attack.

The importance of the anticipatory element would increase if the series of prior small-scale attacks clearly indicated a large-scale digital attack was imminent. In that case, a defensive response at the last window of opportunity before the attacker had completed preparations for launching the attack would qualify as an exercise of anticipatory self-defense. Whether it would qualify as a lawful exercise of anticipatory self-defense would depend on the credibility, reliability and sufficiency of the evidence and the absence of feasible alternatives, as well as the effort taken to ensure the response was proportionate to the threat.

4. Identification of the Author and the Threat

Probably the single greatest obstacle to the exercise of anticipatory self-defense in response to a stand-alone cyber armed attack is identification of the attacking party. A lawful exercise of anticipatory self-defense is an option only if reliable intelligence or other evidentiary factors enable the defending State to identify the prospective attacker and the nature and scope of the threat posed. The cyber domain is different from the physical one in a number of ways, but the one which is crucial in this respect is the relative degree of anonymity possessed by a prospective attacking party acting wholly within the cyber domain.

While the problem of identification of both the identity of the attacking party and the nature of the threat posed is real and substantial, it is not necessarily impossible to do so in at least some situations.

---

[49] *See supra* note 10 and accompanying text.

First, it may be possible to "hack-back" to obtain at least a preliminary indication where the attack originated. This will not necessarily be conclusive. Data travels over an entire network of connections and splits into data packages that traverse various geographic points and nodules. Even if the point of origin could be identified, the geographic source of a digital attack does not necessarily indicate the identity of the attacking party; it simply shows the data's originating location. If a digital attack utilized a so-called "botnet," of which there are many on the Internet, it would probably be unclear initially as to who or what was behind the attack, although this could become clearer after further investigation. However, any forcible response after the elapse of time required to establish the identity of the attacker would, in these circumstances, no longer be anticipatory. A more feasible alternative is prevention of the attack through the dismantling of botnets before they could be employed on the scale of an armed attack.[50]

That problem could be partially overcome by the fact that there are—at least at present and in the reasonably near future—relatively few States and even fewer, if any, non-State actors capable of mounting a wholly digital attack rising to the level of an armed attack, particularly one with potentially devastating consequences. This narrows the number of potential authors considerably, thereby making a positive identification of the source of the incipient attack more feasible.

Even with this narrowing, however, identifying the source of an incipient attack and determining the nature and scale of the threat pose significant, but not necessarily insurmountable, obstacles to the exercise of a lawful preemptive response when other more specific evidence of authorship is not present.

5. Preemptive Response

In sum, while anticipatory self-defense in response to an incipient armed attack that will employ both kinetic and cyber weapons and techniques is not substantially different from situations in which cyber operations are not part of the attack, there are significant obstacles to its exercise in reaction to a potential stand-alone cyber armed attack in the absence of clear intelligence or other factors enabling the defending State to identify the nature

50. For an example of the successful "take down" of a criminal botnet, see *Taking Down Botnets: Microsoft and the Rustock Botnet*, MICROSOFT ON THE ISSUES (Mar. 17, 2011, 6:36 PM), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx.

and source of the attack. In some cases, there will be sufficient information to permit an anticipatory defensive response, but in others—perhaps the majority—there will not. This is a fact with which policy makers and military commanders must learn to live. There is, after all, no such thing as perfect security in the physical world either; surprise attacks have been carried out with varying degrees of success throughout military history.

This relative degree of uncertainty and the obstacles posed to the lawful exercise of anticipatory self-defense from a stand-alone cyber armed attack are real and cannot be wished away, but these factors do not preclude such action when they can be overcome and when other alternatives are neither feasible nor adequate to address the threat.

This uncertainty and these obstacles provide no reason to panic and certainly do not justify a weakening or changing of the law with regard to the exercise of anticipatory self-defense. Anticipatory self-defense is not frequently employed in the physical domain, with only a relatively few instances of it being exercised in response to more traditional modes of attack.[51] There is no reason why this should be different in the digital context.

Improvement of measures to enhance cyber security of vital military and civilian systems and the possession of adequate means of cyber defense, including the potential to carry out credible and effective cyber intelligence, will go far towards deterring a potential attack and limiting the effects of one, should it occur. Likewise, as stated earlier, the nature and scope of the threat of cyber attack should be kept in perspective; over reliance on preemption is not necessarily a way to increase cyber security. To the contrary, if used without proper attention to the well-established legal criteria governing the exercise of anticipatory self-defense, it could well increase the degree of "cyber insecurity" and needlessly escalate situations on the basis of misperceptions and miscalculations.

---

[51] While self-defense has an intrinsically anticipatory element that includes forestalling future attack, it is comparatively rare that the anticipatory element is exercised without an accompanying reactive element responding to a previously conducted attack. For example, the U.S. airstrikes on Libya in 1986 were designed to deter future attacks, but were also in response to the bombing of a Berlin disco in which U.S. service members were killed.

IV. SUMMARY AND CONCLUSIONS

We have detailed our reasons for concluding that the present legal framework governing the exercise of the right of self-defense is both relevant and applicable to cyber armed attacks. That framework provides a right of self-defense in response to either an ongoing or imminent armed attack within the conditions laid out in the UN Charter and under customary international law. The criteria of the Charter and customary law are complementary and apply to any invocation of the right of self-defense. This legal framework has long recognized the right to exercise anticipatory self-defense in response to a manifest and unequivocal threat of attack in the proximate future, within the general parameters of necessity, proportionality and immediacy. There is no reason to conclude the Charter eliminated this long-standing preexisting right. Anticipatory self-defense continues to be in force in the contemporary legal order as an intrinsic part of the larger notion of self-defense.

Anticipatory self-defense does not, however, permit so-called "preventive self-defense," i.e., the reaction to mere potential threats of attack that may or may not crystallize at some indeterminate point in the future, or action taken in the absence of credible evidence that an attack is imminent and establishing who or what is responsible.

Anticipatory self-defense includes the possibility of responding to an imminent armed attack that is wholly or partially conducted within the digital domain, provided the attack to be conducted would be on a comparable scale and have similar effects to a traditional kinetic attack carried out by a State. This would include situations where a cyber armed attack had the intended effect of resulting in more than nominal human casualties or causing significant physical damage and destruction through the direct secondary consequences of the digital attack. Additionally, in our opinion in those cases where the attack causes no direct physical effects, but where long-term, serious damage to digital systems controlling a State's critical infrastructure or essential functions resulted or was clearly intended, such action could constitute an armed attack justifying the exercise of self-defense when the damage was not capable of being remedied within a reasonable timeframe and the stability of a State and its society were seriously threatened.

In our view, anticipatory self-defense may be carried out in response to an imminent digital armed attack irrespective of whether the attack is conducted (1) by a State; (2) by a non-State actor acting either under the con-

trol, or with the substantial involvement, of a State; or (3) by a non-State actor acting alone.

We examined the probable modes by which an incipient cyber armed attack could be conducted and concluded that there are basically two modes. First, and increasingly the most likely, is in preparation for, or adjunct to, a traditional kinetic armed attack. In this case, the scope of a possible anticipatory defensive response would not be significantly affected, since it would be assessed in tandem with other physical indications of an impending attack. Second, a stand-alone cyber armed attack could occur justifying a proportionate anticipatory exercise of self-defense.

For a number of reasons, however, the stand-alone cyber attack is less likely to occur and less likely to warrant an anticipatory defensive response. First, most stand-alone cyber attacks fall well below the threshold of armed attack, which would preclude a use of force in self-defense. Second, even in cases where the level of the attack does reach the requisite legal threshold, in many—probably most—cases there will be insufficient knowledge of the author of the attack and its probable scope and intended effects to enable a reasonably accurate assessment of which State or non-State actor is responsible and to gauge the appropriate defensive response within the parameters of necessity and proportionality. Nevertheless, there could be limited situations in which sufficient information is available to enable a lawful preemptive defensive response to a stand-alone cyber attack. Although this option will not be available in many, indeed, probably most situations, that reality should not lead to panic and overreaction, or be used as justification for "bending the rules." Cyber attack is unlikely in most cases to require the exercise of self-defense. Even when it does, anticipatory self-defense is not necessarily the only or most appropriate response. Its use will be limited to those instances when it can be carried out with the least possible danger of miscalculation and when no other alternatives are feasible.

There are means other than the exercise of anticipatory self-defense in which cyber security can and should be improved and the effects of a potential attack deterred or limited. Overreaction or overreliance on preemption would be more likely to increase, rather than decrease, the level of "cyber insecurity." It would also undermine the legal framework for the use of force at great cost to all members of the international community.