The Law of Armed Conflict, Unconventional Warfare, and Cyber Attacks

Thomas P. Jordan
United States Marine Corps

Follow this and additional works at: https://digitalcommons.wcl.american.edu/nslb

Part of the Internet Law Commons, Military, War, and Peace Commons, National Security Law Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://digitalcommons.wcl.american.edu/nslb/vol6/iss2/3

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University National Security Law Brief by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.
In the early hours of February 24th, 1991, after weeks of air strikes, the ground offensive against Iraq began, resulting in Iraq's forces being routed from Kuwait in four days.  

Not quite twenty-five years later, such a set-piece conflict would seem to come from another time, when armies engaged each other directly and the enemy was easily identifiable. Now, instead, the United States is engaged with allies in military operations against the self-declared Islamic State in the Middle East, a separatist conflict supported by Russian arms and troops in eastern Ukraine, and other unconventional conflicts around the globe. These conflicts, prosecuted by states and non-state actors alike, are taking place in the grey zones between international and non-international armed conflict, raising complex questions about how the law of war should apply. In addition, the advent of new technologies and a vastly increased interconnectedness allows actors to execute non-physical actions, working within and against cyber networks. The law of war and standard military doctrine have developed over time to have primary effect on the actions of States rather than on sub-national
groups. But unconventional conflicts involving such groups are not new: the International Court of Justice (ICJ) handed down its seminal decision on unconventional conflict, *Military and Paramilitary Activities in and Against Nicaragua*, almost thirty years ago. The rise of cyber attacks is an expansion of the realm of unconventional warfare.

As the prevailing nature of conflict has changed, doctrine and law have also changed: In 2009, the International Committee of the Red Cross (ICRC) issued interpretive guidance on civilians who engage in combat on a recurring basis, expanding States’ lawful ability to use force against them. United States military doctrine refers now to “military operations other than war” and the “spectrum of operations” to discuss such conflicts. And unconventional conflicts will continue, because no dictator or politician will easily forget how quickly Iraq’s army was expelled from Kuwait. As early as 1999, military thinkers had realized that the overwhelming conventional superiority of the West, and of the United States in particular, would require a different approach to conflict. What would have happened, for example, if Russia had invaded the Crimean Peninsula in the same way that Iraq had invaded Kuwait? Because unconventional warfare will continue, the international law of armed conflict (LOAC) must be prepared to adapt to address the issues that are unique to such conflicts, including cyber attacks. In Section I, this paper will review the basic governing documents of the LOAC, the United Nations Charter and the Geneva Conventions, highlighting the areas where they do not adequately address unconventional conflicts. Section II will address the individual problems posed generally by unconventional warfare tactics, and their impact on international law, more directly. Section III will analyze the ICJ’s decision in the *Nicaragua* case in light of the problems of unconventional war. Section IV applies these shortcomings to cyber attacks.

---


10 See THE ECONOMIST, supra note 7 (“If Chinese spies . . . were seen planting explosives in the electric grid, uproar or worse would ensue. Yet state-supported Chinese hackers have, officials say, been getting away with the digital equivalent for years.”).

11 See NIELS MELZER, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 27 (2009) (“In non-international armed conflict, organized armed groups constitute the armed forces of a non-State party to the conflict and consist only of individuals whose continuous function it is to take a direct part in hostilities (continuous combat function).”).

12 See generally Jennifer Morrison Taw, RAND, Planning for Military Operations Other Than War: Lessons from US Army Efforts, 57 (1999), and Paul Scharre, Spectrum of What?, 2012 MILITARY REV. 73 (noting that conventional maneuver warfare, while labeled as a major combat operation, is now only a relatively small part of operations).

13 See generally infra note 14 and accompanying text.


I. The International Law of Armed Conflict and Its Application to Unconventional Warfare

The story of the founding of the United Nations is well known: in the waning days of World War II, the governments of the world met to form an international system that would “save succeeding generations from the scourge of war.” The United Nations Charter enshrined both the illegality of aggression in Article 2(4) and the principle of self-defense in Article 51, outlining a regime in which force could only legally be used in response to force. This forms the basis of the current legal landscape, one in which the Geneva Conventions further define and limit conflicts. In fact, “[t]he Geneva Conventions use the term armed conflict specifically to avoid the technical, legal, and political pitfalls of the term war, a direct response to the common practice of states arguing that LOAC did not apply in the absence of a declared war.” In a world where conflicts do not fit neatly into the categories of ‘international’ and ‘non-international’ outlined in the Conventions, and perhaps do not involve physical attack, even the avoidance of the term ‘war’ does not eliminate legal issues.

A. The United Nations Charter

“All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations.” So reads Article 2(4) of the United Nations Charter, which in effect outlaws the use of force “to effect changes, and ... to avoid changes in the patterns of power and other value allocation among the various nation-states.” In concert with this prohibition against the threat or use of force for political ends in Article 2(4), the Charter’s Article 51 reads:

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in ... self-defence shall ... not in any way affect the authority and responsibility of the Security Council under the present Charter

---

16 U.N. Charter pmbl, para. 1.
17 Blank, supra note 6 at 952.
18 See ICRC, How is the Term “Armed Conflict” Defined in International Humanitarian Law? (2008), https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf (stating that an international armed conflict “occurs when one or more States have recourse to armed force against another State, regardless of the reasons or the intensity of this confrontation,” and that an armed conflict not of an international character shall “include armed conflicts in which one or more non-governmental armed groups are involved. Depending on the situation, hostilities may occur between governmental armed forces and non-governmental armed groups or between such groups only.” It is into these two categories that the gamut of unconventional conflicts must be shoehorned).
19 U.N. Charter art. 2, para. 4.
to take at any time such action as it deems necessary in order to maintain or restore international peace and security.\textsuperscript{21}

These two articles together form the basis of the modern LOAC regime. Still, the ability of States and non-state actors to skirt the lines laid out by these two articles can strip them of their apparent strength. There is uncertainty surrounding what constitutes an armed attack, and when force may be used short of threatening the political independence of a State. In its ruling in \textit{Military and Paramilitary Activities in and Against Nicaragua}, the ICJ stated that irregular troops could still be considered to have launched an armed attack if the attack “would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.”\textsuperscript{22}

While helpfully including irregular or unconventional uses of force within the scope of Article 2(4), the court’s statement does not clarify the differences between a “mere frontier incident” and an actual attack. Arguments that Article 2(4) bans the use of any force outside of self-defense by rendering it inconsistent to the purposes of the Charter or defining it as a violation of a member’s territorial integrity\textsuperscript{23} do little to address the ambiguities highlighted in the ICJ’s ruling. According to the ICJ, frontier incidents, whether prosecuted by conventional or unconventional means, do not rise to the level of an armed attack; neither does “the provision of weapons or logistical or other support.”\textsuperscript{24} The ICJ ruled further, in the \textit{Case Concerning Oil Platforms}, that “a series of . . . missile attacks against United States flag and other non-belligerent vessels”\textsuperscript{25} did not “constitute an armed attack on the United States.”\textsuperscript{26} Perhaps the only working definition of armed attack would parallel Justice Stewart’s famous statement in his concurrence in \textit{Jacobellis v. Ohio},\textsuperscript{27} “we will know it when we see it.”

Article 51 preserves the inherent right of self-defense in the face of an attack. Setting aside the issues discussed above with determining what, exactly, constitutes an armed attack is, questions still remain concerning how imminent an attack must be and what constitutes an appropriate response. The paradigmatic language of self-defense comes from the \textit{Caroline} affair and United States Secretary of State Daniel Webster’s letter stating that the circumstances giving rise to the use of force must be overwhelming and leave no choice of means or time for deliberation.\textsuperscript{28} The ICJ understanding on state actions is shaped by the \textit{Oil Platforms} judgment that the United States’ attacks upon Iranian oil platforms were not self-defense,\textsuperscript{29} as well as an advisory opinion that Israel’s

\textsuperscript{21} U.N. Charter art. 51.
\textsuperscript{22} Nicar. v. United States, 1986 I.C.J. 14 at ¶ 195.
\textsuperscript{23} See, e.g., \textsc{Oscar Schachter}, \textit{International Law in Theory and Practice} 112–13 (1991) (recognizing that such an overly broad reading, however, could easily extend to sanctions enforced through embargoes and interdictions, humanitarian interventions, and security operations in areas where government rule has completely failed).
\textsuperscript{24} Nicar. v. United States, 1986 I.C.J. 14 at ¶ 195.
\textsuperscript{25} Oil Platforms (Iran v. United States), 2003 I.C.J. 161 ¶ 48 (Nov. 6).
\textsuperscript{26} Id. at ¶ 64.
\textsuperscript{27} Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).
\textsuperscript{28} See British-American Diplomacy: The Caroline Case, Avalon Project, http://avalon.law.yale.edu/19th_century/br-1842d.asp.
\textsuperscript{29} Iran v. United States, 2003 I.C.J. 161 at ¶ 76 (“The Court finds itself unable to hold that the attacks made on the platforms could have been justified as acts of self-defence.”).
construction of a wall in occupied territory is contrary to international law. These rulings highlight that modern deliberations over the legitimate use of force in self-defense focus on Webster's criteria that the threat be instant and overwhelming, which the ICJ termed in the Oil Platforms case the "criteria of necessity and proportionality.")

Considering the Charter's Article 2(4) and 51 regime, armed groups (whether state or non-state) may engage in unconventional armed attacks, including cyber attacks, specifically to take advantage of the grey areas within international law, thereby limiting the means for response from the international community. Iraqi armored units crossing the border into Kuwait in 1990 resulted in swift action from the Security Council. In comparison, Iran's involvement in ongoing conflicts throughout the Middle East draws a subdued reaction from the international community. Cyber attacks against Iran's nuclear program and massive acts of electronic espionage similarly fails to inspire a vehement reaction. Even Russia, which possesses a veto on Security Council action that may be taken against it, has chosen to engage in unconventional operations in Ukraine, softening the resolve of other nations to impose harsh sanctions and undermining the political will of other States to join Ukraine in collective defense.

The Charter's regime against the use of force is well suited to preventing and responding to conventional military attacks, but does not provide easy answers for unconventional warfare.

B. The Geneva Conventions

The main treaties governing the conduct of armed conflict are the Geneva Conventions and their Additional Protocols, which are primarily concerned with the treatment of combatants. The four Conventions feature articles common to each; these common articles define two types of conflict: international conflict, defined in common Article 2 as conflict between two or more States,

---

30 See Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 2004 I.C.J. 136, ¶ 142 (Jul. 9) ("Israel cannot rely on a right of self-defence or on a state of necessity in order to preclude the wrongfulness of the construction of the wall.").
34 See THE ECONOMIST, supra note 7 ("Stuxnet [was] a piece of malicious software that America and Israel used to destroy Iran's nuclear centrifuges.").
35 See THE ECONOMIST, supra note 7 ("[H]ackers had stolen records of around 22m federal government employees from the sleepy and ill-run Office of Personnel Management.").
36 See, e.g., NATO Express Concern After Report Of New Russian Military Base Near Ukraine, Radio Free Europe/ Radio Liberty (Oct. 9, 2015), http://www.rferl.org/content/russia-military-base-near-ukraine/27236785.html ("Russia denies directly sending soldiers to fight in eastern Ukraine . . . But with little fear of more serious Western reprisals . . . Russian President Vladimir Putin is being more brazen now.").
37 See SOLIS, supra note 8, at 186 ("Individual status [of a combatant] determines the rights and protections afforded to a fighter.").
38 See, e.g., Geneva Convention Relative to the Protection of Civilian Persons in Time of War art. 2, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 ("[T]he present Convention shall apply in all cases of declared war or of any other armed
and non-international conflict, defined in Common Article 3 by the negative to Common Article 2, that is, as an "armed conflict not of an international character." The first Convention, dealing with wounded and sick members of the armed forces in international conflicts, defines belligerents in varying terms, from regular members of the armed forces through those who "spontaneously take up arms to resist the invading forces . . . provided they carry arms openly and respect the laws and customs of war." These categories of belligerents are entitled to prisoner of war (POW) status under the third Convention. These belligerents are also defined in the 1977 Additional Protocol I as combatants, and shall be held if captured as POWs.

And what of the status of the combatants, regular or irregular, in non-international conflicts? As Gary Solis points out in considering the rules governing of such unconventional conflicts, the traditional view is that, just as there are no POWs in non-international armed conflicts, there are no "combatants," lawful or otherwise, in common Article 3 conflicts. There may be combat in the literal sense, but in terms of LOAC there are fighters, rebels, insurgents, or guerillas who engage in armed conflict, and there are government forces . . . . There are no combatants as that term is used in customary law of war, however. Upon capture such fighters are simply prisoners of the detaining government; they are criminals to be prosecuted for their unlawful acts, either by a military court or under the domestic law of the capturing state.

In unconventional warfare, then, with its hybrid nature, many belligerents are not legally considered protected combatants. At the same time, such belligerents cannot "enjoy general protection against dangers arising from military operations," as stated in the 1977 Additional Protocol, because such protection extends only "unless and for such time as [the civilians] take a direct part in hostilities." The Conventions and Additional Protocols were laid out to define who could lawfully participate in armed conflicts, and what kinds of protections and treatments those participants should have when placed hors de combat, either through injury or capture. They were also intended to define a basic set of protections for the civilian populaces directly affected by armed conflict, to

---

39 Id. art. 3.
43 Solis, supra note 8, at 191.
44 See Additional Protocol I, supra note 42, at art. 51.
45 Id.
46 See supra notes 38-42 and accompanying text.
lessen their hardships. But in the realm of unconventional warfare, where armed groups deliberately avoid placing themselves neatly into combatant or non-combatant groups, where fighters may not be regular members of a State’s armed forces or disguised, where attacks may take place in the electronic realm, and where any States involved are themselves seeking to avoid direct identification of their roles in the conflict, the categories and protections established by the Conventions and the Additional Protocols limit the ability of belligerent States and the international community to fit squarely within the laws of armed conflict. Just as utilizing unconventional warfare allows States and armed groups to escape certain responsibilities imposed by the international community, avoiding the employment of conventional armed forces allows groups to skirt the customs of the laws of war, or use them to their own advantage.

II. PROBLEMS WITH UNCONVENTIONAL WARFARE IN INTERNATIONAL LAW

Because it takes many different forms and has multiple, shifting details, unconventional warfare goes by many different names. The difficulties associated with a functional definition of these conflicts reflect the issues that international law confronts when trying to deal with them – if the international community cannot agree on a definition of “terrorism,” for example, how can it create an effective legal regime to deter terrorism? Additionally, groups may attempt to sway opinion by carefully choosing the terms describing a conflict to justify it to the international community and lessen the undesirable repercussions of their actions. Russia attempted to justify its invasion and annexation of the Crimean Peninsula in 2014 by comparing it to Kosovo’s declaration of independence from Serbia. The various shades of grey involved in unconventional conflict give

---

47 See Geneva Convention Relative to the Protection of Civilian Persons in Time of War, supra note 38.
48 See, e.g., William Taylor et al., Don’t Forget Crimea, N.Y. TIMES (Jun. 8, 2014), http://www.nytimes.com/2014/06/09/opinion/dont-forget-crimea.html?_r=0 (“After former President Victor Yanukovych fled Ukraine . . . Russia moved with stunning swiftness in Crimea. “Little green men” — the Ukrainians’ term for soldiers without identifying insignia, later confirmed by President Vladimir Putin to have been Russian military personnel — quickly occupied strategic points on the peninsula. Days after a hastily organized and flawed referendum produced dubious results, Russia formally annexed Crimea.”).
49 See, e.g., Application of the Convention on the Prevention and Punishment of the Crime of Genocide, 2007 I.C.J. 43 (Feb. 26), ¶ 413 (“It has not been established that those massacres were committed on the instructions of or under the direction of organs of the respondent State, nor that the Respondent exercised effective control over the operations in the course of which those massacres . . . were perpetrated.”).
52 See, e.g., Dusan Stojanovic, Putin Compares Kosovo’s 2008 Independence to Russia’s Annexation of Crimea; Others Disagree, Fox (Mar. 19, 2014), http://www.foxnews.com/world/2014/03/19/putin-compares-kosovo-2008-independence-to-russia-annexation-crimea-others/ (quoting Russian President Vladimir Putin as saying, “In a situation absolutely the same as the one in Crimea, they recognized Kosovo’s secession from Serbia as legitimate while arguing that no permission from a country’s central authority for a unilateral declaration of independence is necessary”).
rise to many issues. Three of these issues have been in existence for some time, and they apply to cyber attacks as well: cross-border conflicts, aggressor identification, and the revolving door problem.

A. Cross-Border Conflict

A primary strength of unconventional armed groups is their ability to seek a safe haven across an international border, because "[t]wenty-first-century armed conflicts often have no battlefield in the traditional sense." By practicing unconventional warfare, a state-supported or non-state armed group can keep its troops safe from harm across a border, allowing them to recuperate, train, and plan future offenses. The operations of the United States during the Vietnam War present a textbook example of a nation utilizing conventional warfare methods struggling and failing against an enemy utilizing unconventional warfare, particularly against the North Vietnamese use of the borders with Laos and Cambodia, as Louis Henkin explains:

The United States saw the war [thus:] North Vietnam launched an armed attack against the territorial integrity and political independence of an independent country, the Republic of South Vietnam . . . in clear violation of Article 2(4) of the Charter. In the face of this armed attack . . . the United States could come to [South Vietnam's] aid in collective self-defense . . . The United States and the Republic of South Vietnam had every right to carry the war to the territory of the aggressor [and] of any other countries that involved themselves in the aggression, or permitted the aggressor to use their territory . . . i.e., Laos and Cambodia.

North Vietnam, however, was able to portray the conflict as a civil war, and the United States faced significant criticism for attempting to attack belligerents who were located across international borders from the scene of the conflict – South Vietnam. In the long shadow of the Vietnam conflict, States were loath to engage openly in operations across international borders from

---

53 Sous, supra note 8, at 10.
56 Id. at 308 (“In such a war, United States intervention, even bombing North Vietnam, was – again – perhaps a violation of traditional international norms against intervention . . . Bombing Laos or Cambodia would be more difficult to justify . . . toleration of mutual interventions in civil war does not contemplate attacks by one intervenor against another.”); see also Henry Grabar, What the U.S. Bombing of Cambodia Tells Us About Obama’s Drone Campaign, THE ATLANTIC (Feb. 14, 2013), http://www.theatlantic.com/international/archive/2013/02/what-the-us-bombing-of-cambodia-tells-us-about-obamas-drone-campaign/273142 (“Like the current conflict, the military action in neutral Cambodia was so secretive that information about the first four years of bombing, from 1965 to 1969, was not made public until 2000. And like the current conflict, the operation in Cambodia stood on questionable legal ground.”).
the location of a conflict; a situation perhaps reinforced by the experience of the United States over the last fifteen years: “The American debacle in Iraq seemingly vindicates the restrictive use-of-force doctrine [that] called for the last-resort application of overwhelming force on behalf of vital interests and clearly defined and achievable political-military objectives.”57 Objectives can only be clearly defined and achievable if the battlefield is limited in geographic scope. It is possible, however, that technological advances will alter this hesitancy, as nations are able to strike their enemies from across the globe utilizing relatively limited resources and at little to no risk of combat losses.58 The ability to inflict damage on an adversary without leaving the office, let alone dispatching troops, can only increase the frequency of attacks. The global connectivity created by the World Wide Web means that almost all cyber attacks will be cross-border in nature.59

Of course, such conflicts involving the United States which “fail to fit nicely within the[ two dominant categories] have always been present; notably, the Boxer Rebellion in China; the 1916 United States punitive raid against Pancho Villa in Mexico; and the United States intervention in the Russian Civil War.60 International law has yet to account for the increased geographic scope of armed conflict, so that LOAC and human rights law can be facilitated. Typically, the enemy “deliberately avoids consolidating its center of gravity in such hot zones [of conflict], but instead operates out of whatever safe haven offers the best opportunity for protection from the reach of state military capabilities.”61 Unconventional armed conflict has shifted away from the relatively simple situation of an armed group seeking safe haven across a border from the conflict zone, and has become a much more complex trans-national situation in which groups seek to plan and launch physical and cyber attacks from relatively safe locations.62 The nature of cyber attacks exploits the problems posed by safe havens and cross-border conflicts; aggressors will continue to favor them as long as they remain low-risk. Proliferation of multi-national cyber attacks as part of unconventional warfare can only be addressed by an international legal regime governing trans-national conflict.

B. Aggressor Identification

A key point within LOAC’s regime to limit armed conflict is the punishment of aggression. In the aftermath of World War II, the International Military Tribunal at Nuremberg defined crimes against peace as the “planning, preparation, initiation or waging of a war of aggression,”63 setting the

59 See, e.g. Andy Greenberg, FBI Director: Sony’s ‘Sloppy’ North Korean Hackers Revealed Their IP Addresses, WIRED (Jan. 7 2015), http://www.wired.com/2015/01/fbi-director-says-north-korean-hackers-sometimes-failed-use-proxies-sony-hack/ (describing hackers’ use of proxy servers to relay their computer connections to other locations so that their identity is masked, a practice which necessarily implicates multiple countries in any cyber attack).
60 Geoffrey S. Corn, Geography of Armed Conflict: Why It Is a Mistake To Fish For the Red Herring, 89 INT’L L. STUD. 77, 78 (2013).
61 Corn, supra note 60, at 91.
62 See Corn, supra note 60, at 91 (recognizing the “under-inclusiveness” of the armed conflict framework).
63 1 Trial Maj. War Crim. 11, (art. 6(b)) (Int’l Mil. Trib. 1947).
stage for placing aggressive action by States in the realm of war crimes. Article 2(4) of the Charter forbids "the threat or use of force," and the United Nations General Assembly attempted to define aggression by adopting Resolution 3314. In the strictest terms, then, the international legal regime has defined aggression and made it illegal.

Yet, armed groups use the shadows of unconventional warfare to disguise their acts of aggression, avoiding the direct action response to a conventional invasion such as Iraq's action against Kuwait. Discussing the current international legal system's problems in coming to grips with the issue of aggressive unconventional warfare, John Norton Moore points out:

[the central symptom of this problem in the international legal system, as it is presently applied, is the system's all too frequent failure to systematically and strongly condemn the aggressive use of force, particularly in the low-intensity conflict spectrum, while simultaneously and perversely condemning and constraining the use of defensive force in response to such aggression.

One of the keys to unconventional warfare is that it allows belligerents to disguise themselves and thus disguise their aggression. By swimming in the sea of the people, in Mao's phrasing, belligerents can increase their survivability against conventional forces, prolong the conflict and sap political will, create plausible deniability for outside agents and sponsors, and increase their use of surprise and deception. They may also, as Moore points out, limit the international legal system's sanctions against them, and perhaps see sanctions passed against their opponents' attempts at defending themselves. Moore states that, for the legal system to provide effective deterrence,

[aggression, whether overt or covert, must be clearly condemned. Defense, whether overt or covert, must be clearly supported and assisted. And it must be understood that it is the difference between the systemic treatment of aggression and defense that will largely determine whether the legal system will play a significant role in war avoidance.

---

64 U.N. Charter art. 2, para. 4.
66 See supra notes 1-6 and accompanying text.
68 Gus Martin, Understanding Terrorism 259 (2012) (referencing Mao's On Guerrilla Warfare, noting that today, "terrorists can become fish swimming in the sea of the global community") (internal quotation marks omitted).
69 See Nicar. v. United States, 1986 I.C.J. 14 (explaining the concept of when the United States attempts to attack the irregular, Nicaraguan-assisted Sandinistas in El Salvador by means of supplying aid to Nicaragua's insurgency, the Contras, results in condemnation by the international community); see John Norton Moore, The Secret War in Central America and the Future of World Order, 80 AM. J. INT'L L. 43, 126 ("The result is a politically invisible attack that avoids the normal political and legal condemnation of aggressive attack and instead diverts that moral energy to condemning the defensive response. In a real sense, the international immune system against aggressive attack becomes misdirected instead to defensive response.") (internal quotation marks omitted); see also Henkin, supra note 51, at 306-08, (discussing the war in Vietnam, which, as a result of North Vietnam's successful use of unconventional warfare, was seen not as the United States rendering assistance to South Vietnam's defensive war, but as U.S. involvement in a Vietnamese civil war).
70 Moore, supra note 67, at 31; see also S.C. Res. 660, supra note 32 (providing a clear example of international law muddying the waters between aggressor and victim by calling upon both "Iraq and Kuwait to begin immediately intensive negotiations for the resolution of their differences").
As previously discussed, cyber attackers exploit the current regime by remaining across borders or in other safe zones, away from the location of their target. This cross-border problem is exacerbated by the identification problem, because the identity of a cyber attacker is exceedingly difficult to pin down and can often not be revealed if it is known without possibly compromising intelligence sources. Cyber attacks are a paradigmatic example of aggressors disguising themselves to avoid retaliation. One can only imagine the difficulty of attempting to conceal a conventional force's movement across an international border, although it is not impossible to do. Extending the legal controls effective against conventional warfare to unconventional warfare and cyber attacks will lessen groups’ reliance on the protections provided by unconventional means. The international legal regime must strengthen existing prohibitions on the use of force and on aggression by making explicit that unconventional means of waging such war will be dealt with in the same manner as their conventional equivalents.

C. The Revolving Door Problem

Unconventional warfare often involves civilian belligerents engaging in hostilities and then retreating from the zone of conflict across international borders. But even when they are in the zone of conflict, belligerents often blend in with the local populace to prevent accurate identification. They eschew identifying uniforms or insignia – in fact, as the ICRC noted in its 2008 opinion paper, persons engaged in combat can be the armed forces of an armed group that is not a State but is a party to the conflict. But what of civilians who engage in combat, and then hide their weapons and go home? And what of individuals who may or may not be members of a State’s armed forces, but are involved in cyber attacks and thus unidentifiable? Section 51 of the 1977 Additional Protocol I states that civilians “shall enjoy the protections afforded by this Section, unless and for such time as they take a direct part in hostilities.” This creates what is known as the revolving door problem: a belligerent can take up arms and engage in hostilities, and then disengage and lay down their arms at the end of the day, regaining the protections afforded to civilians under the Geneva Conventions and the Additional Protocols. Because the Conventions were aimed at restricting and controlling the actions of conventional forces, they are ill adapted to the realities of unconventional conflict.

While the revolving door problem itself is of limited application for cyber attacks, the international legal community’s response to this shortcoming should be used as an example of

---

71 See supra note 62 and accompanying text.
72 See Greenberg, supra note 59.
74 See ICRC, supra note 18, at 3 (identifying and describing what constitutes “parties to a conflict”).
75 See Additional Protocol I, supra note 42, art. 51.
76 See David Kretzmer, Targeted Killing of Suspected Terrorists, 16 EUR. J. INT’L L. 171, 193 (2005) (“If we accept this narrow interpretation, terrorists enjoy the best of both worlds — they can remain civilians . . . and only endanger their protection as civilians while actually in the process of carrying out a terrorist act. Is this theory, which has been termed the revolving door theory, tenable?”).
effective action against a spreading threat. In May of 2009, the ICRC issued *Interpretive Guidance on the Notion of Direct Participation in Hostilities.* The guidance determines that individuals engaged in hostilities on a regular and recurring basis are *de facto* armed forces and thus lose their civilian protections for the time that they are serving, rather than only for the period they are actively engaged in hostilities. The main passage discussing this solution to the revolving door problem, from chapter II, section 3, “Organized Armed Groups,” bears quoting at some length:

[T]he decisive criterion for individual membership in an organized armed group is whether a person assumes a continuous function for the group involving his or her direct participation in hostilities (hereafter: “continuous combat function”). Continuous combat function does not imply *de jure* entitlement to combatant privilege. Rather, it distinguishes members of the organized fighting forces of a non-state party from civilians who directly participate in hostilities on a merely spontaneous, sporadic, or unorganized basis, or who assume exclusively political, administrative or other non-combat functions.

Continuous combat function requires lasting integration into an organized armed group . . . . Thus, individuals whose continuous function involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities are assuming a continuous combat function . . . .

Individuals who continuously accompany or support an organized armed group, but whose function does not involve direct participation in hostilities, are not members of that group . . . . Instead, they remain civilians . . . . Although such persons may accompany organized . . . and provide substantial support to a party to the conflict, they do not assume continuous combat function and, for the purposes of the principle of distinction, cannot be regarded as members of an organized armed group. As civilians, they benefit from protection against direct attack unless and for such time as they directly participate in hostilities . . . .

In practice, the principle of distinction must be applied based on information which is practically available and can reasonably be regarded as reliable in the prevailing circumstances. A continuous combat function may be openly expressed through the carrying of uniforms, distinctive signs, or certain weapons. Yet it may also be identified on the basis of conclusive behaviour, for example where a person has repeatedly directly participated in hostilities in support of an organized armed group . . . . Whatever criteria are applied in implementing the principle of distinction in a particular context, they must allow to reliably distinguish members of the armed forces of a non-State party to the conflict from civilians who do not directly participate in hostilities, or who do so on a merely spontaneous, sporadic or unorganized basis.79

77 See Melzer, supra note 11, at 27.
78 Id. at 33–36.
79 Id. at 33–35 (citations omitted).
Under this regime, a “fighter who plants improvised antipersonnel mines remains a lawful target when he puts down his tools and walks home for lunch . . . . A senior terrorist insurgent may be targeted when he is asleep. An insurgent commander remains a lawful target . . . whatever he may be doing.”80 This is a major change in LOAC, acknowledging the prevalence of belligerents engaging in unconventional warfare while attempting to avoid the risks inherent in organizing as an armed force.81 Of the problems reviewed so far, this is one of the few where the international legal community has taken action to directly address the issues that arise in unconventional warfare situations and mitigate them. The ICRC passage on the continuous combat function concludes: “determination [of a combatant’s status] remains subject to all feasible precautions and to the presumption of protection in case of doubt.”82 While conventional armed forces of law-abiding nations must ensure that they are engaged in lawful targeting and err on the side of caution, the ICRC’s guidance does permit them to engage unconventional belligerents on a more equal footing. In regards to those participating in cyber attacks, the guidance presents a stepping-stone to determine their status as combatants. The international legal community must take more steps similar to this to address the problems of unconventional warfare, and specifically cyber warfare.

III. The Nicaragua Case

As seen above, the ICJ has issued several rulings that bear upon unconventional warfare. In 1986 the court released its decision in Military and Paramilitary Activities in and Against Nicaragua.83 The case was brought by Nicaragua, who charged the United States “with illegal intervention and paramilitary activities against the territorial integrity and sovereign independence of their state.”84 As Moore put it, the Nicaragua case was a result of the fact that “since mid-1980 Cuba and Nicaragua have been waging a secret war against neighboring Central American states.”85 Nicaragua (with support from Cuba and the Soviet Union) was engaged in many aspects of unconventional warfare. The United States’ response was to give “support to the contras, a term employed to describe those fighting against the present Nicaraguan Government.”86 The United States, then, responded to Nicaragua’s unconventional warfare campaign by supporting groups waging their

---

80 Sous, supra note 8, at 206.
82 MELZER, supra note 11, at 35 (citation omitted).
85 Moore, supra note 70, at 60 (“Cuban and Nicaraguan involvement in this serious attack includes: participation in organizing the effective insurgency; the provision of arms; the laundering of Soviet-bloc for Western arms; transshipment of arms . . . assistance in military planning; financing; ammunition and explosives supply; logistics assistance; the provision of secure command and control facilities; the training of insurgents; communications assistance; intelligence and code assistance; political, propaganda, and international support; and the use of Nicaraguan territory as sanctuary for attack.”).
own unconventional fight.\textsuperscript{87} Although the United States argued that the ICJ lacked jurisdiction, the ICJ disagreed and the case went forward, even though the United States had withdrawn before hearings on the merits began.\textsuperscript{88} Holding that the United States had violated international law and that Nicaragua’s actions did not amount to an armed attack against El Salvador, the ICJ addressed two of the major issues of unconventional war discussed above: cross-border conflict and aggressor identification.\textsuperscript{89} Examining the ICJ’s handling of these issues in this case sheds light on the problems the international legal community faces addressing these problems; the next section will demonstrate the relationship between unconventional warfare and cyber attacks. The discussion in the ICJ’s decision underscores the same general problems that will face a legal regime attempting to address cyber attacks. The United States, in particular, could face difficulties similar to those it encountered here in both international courts and the court of public opinion if it attempts to fight cyber warfare by unconventional means of its own.

\textbf{A. Cross-Border Conflict}

All groups involved in the Nicaragua conflict used cross-border sanctuaries to protect their troops: the United States kept personnel involved in training and advising the contra\textsuperscript{90} “on the other side of the frontier, or in international waters.”\textsuperscript{90} The ICJ noted that contra groups operated in Nicaragua along the borders with Honduras and Costa Rica.\textsuperscript{91} For its part, Nicaragua was responsible for “certain transborder military incursions into the territory of Honduras and Costa Rica . . . .”\textsuperscript{92} The court also found “that support for the armed opposition in El Salvador from Nicaraguan territory was a fact up to the early months of 1981.”\textsuperscript{93} However, the ICJ did not have enough evidence to conclude that the government of Nicaragua was involved or responsible for providing support to the insurgents in El Salvador.\textsuperscript{94}

Not only did the use of cross-border safe havens prolong the conflict, the trans-national nature of the conflict severely hampered the ICJ’s ability to ascertain how much support each side

\textsuperscript{87} The ICJ further notes in Military and Paramilitary Activities in and Against Nicaragua, 1986 I.C.J. 14 ¶ 20, that the groups supported by the United States operated along its borders with Honduras and Costa Rica, and engaged – according to the Nicaraguan Government – in acts such as murder, torture, rape, and kidnapping.

\textsuperscript{88} See Sean D. Murphy, \textit{The United States and the International Court of Justice: Coping with Antimonies, The Sword and the Scales: The United States and International Courts and Tribunals} 46, 46 (Cesare Romano ed., 2009).

\textsuperscript{89} See generally \textit{Nicar. v. United States}, 1986 I.C.J. 14 at ¶¶ 120–64.

\textsuperscript{90} \textit{Nicar. v. United States}, 1986 I.C.J. 14 at ¶ 102.

\textsuperscript{91} Id. at ¶ 164.

\textsuperscript{92} Id. at ¶ 164.

\textsuperscript{93} Id. at ¶ 152 (emphasis added).

\textsuperscript{94} Id. at ¶¶ 150–60, especially the ICJ’s conclusion in ¶ 160: “On the basis of the foregoing, the Court is satisfied that, between July 1979, the date of the fall of the Somoza régime in Nicaragua, and the early months of 1981, an intermittent flow of arms was routed via the territory of Nicaragua to the armed opposition in El Salvador. On the other hand, the evidence is insufficient to satisfy the Court that, since the early months of 1981, assistance has continued to reach the Salvadorian armed opposition from the territory of Nicaragua on any significant scale, or that the Government of Nicaragua was responsible for any flow of arms at either period.”
was giving to those groups. 95 This was no minor issue in the ICJ's decision making process: as it pointed out, the United States would have to have needed "effective control of the military or paramilitary operations [of the contras] in the course of which the alleged violations were committed" to be held legally responsible - but evidence of such direct control was not forthcoming. 96 Moreover, the ICJ noted that "if Nicaragua has been giving support to the armed opposition in El Salvador, and if this constitutes an armed attack on El Salvador and the other appropriate conditions are met, collective self-defence could be legally invoked by the United States." 97 Again, evidence of such support could not be clearly established. 98 In the end, because the governments involved kept the insurgent groups at arm's length and provided their support across international borders, the ICJ was unable to reach any definitive decision regarding their responsibility for the conflicts in El Salvador and Nicaragua. 99 This same problem will be faced by legal systems which seek to penalize violations of the law of armed conflict by use of cyber attacks, with an even higher bar to proper assessment of support from state actors.

B. Aggressor Identification

Identifying state responsibility was difficult for the ICJ because of the unconventional nature of the conflict. Indeed, the ICJ noted at the outset of its listing of the facts in the case that, the secrecy in which some of the conduct attributed to one or other of the Parties has been carried on . . . makes it more difficult for the Court not only to decide on the imputability of the facts, but also to establish what are the facts. Sometimes there is no question . . . that an act was done, but there are conflicting reports, or a lack of evidence, as to who did it. The problem is then not . . . imputing the act to a particular State for the purpose of establishing responsibility, but . . . tracing material proof of the identity of the perpetrator. 100

This statement encapsulates the problem of aggressor identification: by disguising their involvement in the conflict, the participants could deflect any responsibility for individual acts, even if their general participation was established. Although the United States accused Nicaragua of providing cross-border sanctuary, communications and logistics support, supplies, and weapons, the ICJ was unable to connect the actions of the insurgents in El Salvador with any direct support of the Nicaraguan government. 101 Despite the massive impact of the conflict in El Salvador, which "resulted

95 Id. at ¶¶ 19–20 (analyzing the degree of support the United States provided to the contras during the revolution).
96 Id. at ¶ 115.
97 Id. at ¶ 127.
98 Id. at ¶ 249 ("The acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State . . . .") (emphasis added).
99 Although it did determine in Military and Paramilitary Activities in and Against Nicaragua, 1986 I.C.J. 14, ¶ 231, that Nicaragua was responsible for "border incursions" into Honduras and Costa Rica, the ICJ stated that it could not determine if these amounted to armed attacks.
100 Id. at ¶ 57.
101 Id. at ¶ 135 ("In short, the Court notes that the evidence of a witness called by Nicaragua in order to negate the allegation of the United States that the Government of Nicaragua had been engaged in the supply of arms to the armed opposition in El Salvador only partly contradicted that allegation.").
in thousands of war casualties and over a billion dollars in direct war damage," it was possible to interpret the insurgency as almost entirely self-contained. Nicaragua escaped responsibility not because it was completely unclear if it was involved, but because it was just unclear enough for the international community to largely ignore its involvement — a result similar to current unconventional operations.

In fact, the ICJ was only able to assign responsibility to the United States for its support of the contras because the United States government had, in a way, admitted to it: The United States justified some of its actions, such as reconnaissance overflights, to the Security Council as collective self-defense. However, the ICJ refused to use the self-defense justification to concretely assign responsibility to the United States.

Instead, it was the rather-public debate between President Reagan’s administration and Congress over funding for covert operations in Central America that provided evidence for the ICJ to use in determining the United States’ responsibility for the contras. In the end, because of its justification to the Security Council and the public nature of its governmental debates, the United States was found to have violated the principle of non-intervention in another State’s affairs and the prohibition against the threat or use of force. However, other States and non-state groups do not have the handicap of public debate. Instead, they are able to mask their involvement, even if only enough to avoid all-out condemnation by the international community. States could interpret the ICJ’s ruling that the United States committed such a violation, but that Nicaragua did not as presenting a simple lesson: do not get caught. Avoiding such a position is much easier for actors who are engaging in cyber operations.

C. Armed Attacks

The ICJ’s ruling also discussed the question of what constitutes an armed attack. As seen above, the ICJ’s decision held that an armed attack could be committed by unconventional troops. However, the ICJ also found that “[t]here is no rule in customary international law permitting another State to exercise the right of collective self-defence on the basis of its own assessment of the situation.” That is, a State could not declare an attack on another State and commit aggression under the guise of collective self-defense; instead, “it is to be expected that the State for whose benefit

---

102 Moore, supra note 67, at 60.
103 See Nicar. v. United States, 1986 I.C.J. 14 at ¶¶ 88, 91. In paragraph 91, the ICJ found that the United States had violated Nicaraguan airspace primarily based upon the debate in the Security Council.
104 Id. at ¶ 74.
105 Id. at ¶¶ 96–98.
106 Id. ¶ 238–42.
109 Id.
this right is used will have declared itself to be the victim of an armed attack."\textsuperscript{110} This is the logic behind the ICJ's statement "that the requirement of a request [for assistance] by the State which is the victim of the alleged attack is additional to the requirement that such a State should have declared itself to have been attacked."\textsuperscript{111}

Rather than implying that States must engage in a drawn-out declaration and notification process, this reasoning by the ICJ is commensurate with accepted norms regarding self-defense: its investigation looked into the timing of possible statements by El Salvador, Honduras, and Costa Rica that an armed attack occurred and their requests for assistance, and compared them with the timing of the United States' actions in the region.\textsuperscript{112} The ICJ's reasoning regarding declarations is in keeping with the requirements of the United Nations Charter: "Article 51 of the United Nations Charter requires that measures taken by States in exercise of this right of self-defence must be immediately reported to the Security Council."\textsuperscript{113} As the Charter's reporting requirement is not construed to restrict a State's ability to react rapidly, neither should the ICJ's attempt to find a request for assistance be so construed; instead, the ICJ was attempting to deal with one of the main problems of unconventional warfare: how to determine if an armed attack was occurring, and if so, when did it begin and who initiated it?\textsuperscript{114} While the ICJ's reasoning would be highly applicable in a conventional setting, by veiling themselves through the use of unconventional warfare, the parties involved in Central America were able to prevent the international legal system from correctly identifying the aggressors and taking action to sanction them. The ICJ struggled and failed to link formal declarations of attacks and requests for assistance with the actions of the belligerent parties.\textsuperscript{115}

This inscrutability extended to the ICJ's attempts to determine if any armed attacks had occurred at all. The ICJ failed to find that "the provision of arms to the opposition in another State constitutes an armed attack on that State. Even at a time when the arms flow was at its peak, and again assuming the participation of the Nicaraguan Government, that would not constitute such armed attack."\textsuperscript{116} ICJ Judge Sir Robert Jennings sharply disagreed with this decision in his dissent:

\begin{quote}
It may readily be agreed that the mere provision of arms cannot be said to amount to an armed attack. But the provision of arms may, nevertheless, be a very important element in what might be thought to amount to armed attack . . . . Accordingly, it seems to me
\end{quote}

\textsuperscript{110} Id.
\textsuperscript{111} Id. at \S 199.
\textsuperscript{112} The ICJ discusses this issue at length in paragraphs 190–240, and especially paragraph 233, where "it appears to the Court that while El Salvador did in fact officially declare itself the victim of an armed attack, and did ask for the United States to exercise its right of collective self-defence, this occurred only on a date much later than the commencement of the United States activities which were allegedly justified by this request." Id. at \S\S 190–240.
\textsuperscript{113} Id. at \S 200 (internal quotation marks omitted).
\textsuperscript{114} As the ICJ notes in paragraph 235, the United States had not "addressed to the Security Council, in connection with the matters the subject of the present case. The report which is required by Article 51 of the United Nations Charter . . . . This fact is all the more noteworthy because, in the Security Council, the United States has itself taken the view that failure to observe the requirement to make a report contradicted a State's claim to be acting on the basis of collective self-defence." Id. at \S 235.
\textsuperscript{115} Id. at \S\S 83, 131, 164.
\textsuperscript{116} Id. at \S 230.
that to say that the provision of arms, coupled with logistical or other support is not
ammed attack is going much too far . . . . It becomes difficult to understand what it is,
short of direct attack by a State's own forces, that may not be done apparently without
a lawful response in the form of collective self-defence; nor indeed may be responded
to at all by the use of force or the threat of force.117

The ICJ's attempts in the Nicaragua case to rule on state responsibility in an unconventional
transnational conflict highlight the weakness of the current legal regime to respond to
unconventional warfare. When confronted with belligerents whose actions, sources of support, and
even methods were all subject to question, the ICJ was incapable of drawing any strong conclusions
regarding the responsible parties and appropriate sanctions.118 The debate over what constitutes a
cyber attack is ongoing,119 with a primary focus on when a cyber attack amounts to an act of war — a
debate that parallels the ICJ's struggle to determine if an armed attack, within the meaning of the
Charter, had taken place.

III. APPLYING THE LESSONS TO CYBER WARFARE

The new capabilities provided by electronic interconnections have changed the face of
unconventional warfare. What before could only be accomplished through armed troops, a complex
espionage program, or a determined propaganda effort — undermining the legitimacy of a nation's
government and committing acts of espionage and sabotage — can now conceivably be realized by
means of a relatively small, well-trained group of hackers.120 Only a few decades ago, the theft of
millions of personnel files from the United States Office of Personnel Management would have
required a complete penetration of the agency, consuming massive resources and requiring decades of
work.121 Today, we should expect such attacks, if not their successes, to be routine.

117 Id. at ¶ 543 (separate opinion of Judge Jennings).
www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/0226232-1eb8-11e2-9746-
908f727990d8_story.html; see also Damian Paletta, When Does a Hack Become an Act of War?, WALL STREET J. (Jun. 13,
120 War in the Fifth Domain, THE ECONOMIST (Jul. 1, 2010), http://www.economist.com/node/16478792; Michael
Riley & Jordan Robertson, Cyberspace Becomes Second Front in Russia's Clash with NATO, BLOOMBERG BUSINESS (Oct. 14,
nato (detailing how criminal gangs or “hacktivists” seeking to obtain data are often the main offenders of cyberattacks);
see also Michael Riley & Jordan Robertson, Cyberspace Becomes Second Front in Russia's Clash with NATO, BLOOMBERG
russia-s-clash-with-nato (mentioning how cyberattacks against the Polish stock market were carried out by a small group
of hackers).
121 Kim Zetter & Andy Greenberg, Why The OPM Breach Is Such A Security And Privacy Debacle, WIRED (June 11,
2015), http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/ (explaining that this breach was discovered
during a sales demonstration, and only took investigators four months to uncover it, compared to decades).
A. Cross-Border Conflict and Aggressor Identification

With the advent of globalized network connections, the problems of cross-border safe havens and unknown aggressors are intertwined and magnified. As was discussed above in Section II A, unconventional armed forces often seek to use safe havens in other countries to bolster their strength and security.\textsuperscript{122} One of the major problems the ICJ faced in dealing with the Nicaragua case was that the forces involved were operating across an international border and could not be easily identified as agents of the Nicaraguan government.\textsuperscript{123} Global cyber networks allow actors to commit acts of war without ever being present at the site of the attack. Moreover, attackers can disguise their location via proxy networks\textsuperscript{124} and the state or non-state actors coordinating the attack can claim plausible deniability even when confronted with evidence indicating their guilt.\textsuperscript{125}

Just as in the Nicaragua case, it is very difficult to determine if the attackers themselves are operating at the behest of or under the protection of the government in whose territory they are based, even if the location can be identified.\textsuperscript{126} The ICJ did not have enough evidence before it to determine if the government of Nicaragua was responsible for the actions of the insurgents\textsuperscript{127} – in a cyber attack, a court would also face the same difficulties assigning responsibility to a state, especially because an attack need not originate in the state sponsoring it, or even in only one state. Even in a country with a more authoritarian regime, such as Russia, it is certainly possible that a determined group of hackers could carry out an attack without the knowledge, to say nothing of the consent, of the government.\textsuperscript{128} Finally, even if the location of the attack were determined, identifying the attackers themselves is all but impossible. An attack could be traced to a certain computer, but that does not provide evidence regarding who was at the keyboard.\textsuperscript{129} Bringing the attackers to justice would be an even more difficult proposition if the government protected them. Unless LOAC is adjusted to take account of this new reality, we should expect states to more frequently engage in cyber attacks because of the relative immunity they provide. As the world’s interconnectivity grows

\begin{thebibliography}{9}
\item \textsuperscript{122} See Nicaragua v. United States, 1986 I.C.J. 14 at § 93 (establishing that although the existence of these groups were admitted, there was a lack of evidence to be conclusive).
\item \textsuperscript{123} See, e.g., Larry Greenemeier, Seeking Address: Why Cyber Attacks Are so Difficult to Trace Back to Hackers, \textit{Scientific American} (Jun. 11, 2011), http://www.scientificamerican.com/article/tracking-cyber-hackers/ (detailing how hackers can avoid detection in a variety of ways, including through malware or by taking control of personal computers).
\item \textsuperscript{124} See, e.g., Daily Chart: Hack-attack, \textit{The Economist} (Feb. 20, 2013), http://www.economist.com/blogs/graphicdetail/2013/02/daily-chart-12 (“Despite the detailed evidence presented by the firm in its report [that a group based in Shanghai engages in cyber attacks], the Chinese government denies wrongdoing.”); Michael Riley & Jordan Robertson, Cyberspace Becomes Second Front in Russia’s Clash with NATO, \textit{Bloomberg Business} (Oct. 14, 2015, 5:00am), http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia’s-clash-with-nato (stating that although many believe recent cyber attacks originated from Russia, Kremlin spokesmen reject these assertions as unsubstantiated and absurd).
\item \textsuperscript{125} See Nicaragua v. United States, 1986 I.C.J. 14 at § 93.
\item \textsuperscript{126} See id. at § 144 (finding that the court had to consider whether there was evidence that the Nicaraguan government was responsible, and was unable to do so).
\item \textsuperscript{127} Greenemeier, supra note 124 (explaining that attackers use proxies to carry out their attacks, which limits the amount of foreign aid governments can give to assist local law enforcement).
\item \textsuperscript{128} See Greenemeier, supra note 124.
\end{thebibliography}
and spreads beyond shopping and banking, our increased vulnerability to the effects of an attack will only increase the likelihood that actors will choose to utilize cyber as their preferred means of aggression. The ability to act across borders and disguise identities only lend more weight to the case for using cyber attacks as the primary means of waging unconventional war. The laws of war must take this into account, perhaps by mandating that governments, from whose territories attacks are launched, participate in identifying attackers and bringing them to justice, or face the presumption that the state itself is coordinating the attacks.

C. Armed Attacks

An even thornier problem than identifying an attacker in cyberspace is determining whether a cyber attack constitutes an armed attack for the purposes of LOAC. The ICJ struggled with the question of how much intervention would amount to an act of war, discussing the issue of ‘cross-border incursions’ and identifying the existence of, but not the exact point, of a threshold that must be crossed before an attack became an act of war. Just as cyber attacks magnify the existing problems of unconventional warfare, they also seemingly magnify the problem of identifying when the threshold between skirmish and war is crossed. However, it is possible that this problem is not as vexing as it appears. If LOAC can adapt to take into account the increasing prevalence of unconventional warfare, the issue of identifying when a cyber attack is an act of war could also be resolved. To do so, there must be a meaningful way to distinguish between unconventional and conventional warfare. Unconventional and conventional warfare are two means by which war may be waged – each with distinct advantages and disadvantages. Just as with other new types of weapons, cyber attacks are not, in and of themselves, a new means or a new end. Instead, cyber attacks are one way of waging war – a way which lends itself readily to unconventional operations.

130 See, e.g., Kim Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, WIRED.COM (Nov. 3, 2014), http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (finding that the number and type of items which are becoming connected to global networks continues to increase. The cyber attack on Iran’s enrichment centrifuges, is only one example of the increasing vulnerability of our systems to such acts. Other infrastructure is also at risk); see also Tom Brewster, There are Real and Present Dangers Around the Internet of Things, THE GUARDIAN (Mar. 20, 2014), http://www.theguardian.com/technology/2014/mar/20/internet-of-things-security-dangers (listing automobiles, houses, and industrial controls as other types of infrastructure at risk); Michael Riley & Jordan Robertson, Cyberspace Becomes Second Front in Russia’s Clash with NATO, BLOOMBERG BUSINESS (Oct. 14, 2015), http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato (detailing reports of Russian attacks on European infrastructure, including blast furnaces and stock exchanges).


133 See, e.g., John Richardson, Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, 29 J. MARSHALL J. COMPUTER & INFO. L. 1, 8 (2011).

134 See supra Section III. As an example, the United States found that its choice to wage unconventional warfare against Nicaragua did not turn out very well, at least not in the ICJ.

international community, and especially the legal community, should not focus on the ways or means when attempting to determine if an attack constitutes an act of aggressive war. Rather, the focus should be on the ends – just as acts of terrorism can be distinguished by the goals of the actor, a determination whether the threshold of war has been crossed should be made by examining the ends sought from the attack.

For example, a cyber attack stealing thousands of sensitive documents is an act of espionage, and not an act of war in and of itself. If such an act of espionage were carried out without the use of computers, it would not likely be seen as crossing the threshold to war unless it was part of a larger attack. An attack that disables, even temporarily, a State’s ability to utilize its nuclear arsenal would be an act of war, because its goal is to disable a central weapons system used in the defense of the nation. If such an attack were carried out by more traditional means, it would very likely be seen as an act of war. If the law of war is going to adjust to the new weapons and tactics that are being used, it must produce clear guidance on determining what constitutes an act of war, and how states may respond. Focusing on the ends sought by aggressors rather than on the ways and means they use is one way LOAC can move forward in this regard.

IV. CONCLUSION

The international legal system has great difficulty dealing effectively with unconventional conflicts by applying law meant for conventional state actors. Despite attempts to adjust the governing conventions, like the ICRC’s attempt with its Interpretive Guidance on the Notion of Direct Participation in Hostilities, the majority of LOAC is still geared toward regulating state-conducted conventional warfare. However, as conventional war takes second place to unconventional warfare, and non-state armed groups become increasingly more sophisticated and deadly, LOAC must adapt. The norms and standards governing state responsibility, cross-border conflict, and civilians engaged in hostilities must be adjusted to take account of the growing prevalence of unconventional warfare if the international legal community is to be effective. These problems are only magnified by the increasing likelihood of cyber attacks becoming the modi operandi of choice among both state and non-state actors. The ruling of the ICJ in the Nicaragua case highlights the difficulties in applying the current legal regime in the face of unidentifiable aggressors and ambiguous attacks.

138 For example, if hundreds of agents had infiltrated the country’s nuclear arsenal and simultaneously deactivated it.
139 See David Cole, Out of the Shadows: Preventive Detention, Suspected terrorists, and War, 97 CAL. L. REV. 693, 716 (2009) (noting that conventional warfare is no longer the norm, as the United States has not declared war since 1945); see also Herszenhorn, supra note 73 (stating that even Russia’s war in Eastern Ukraine is being fought in a highly unconventional manner, albeit with conventional arms).
— features that cyber warfare exemplifies. As Judge Jennings stated in his dissent to the *Nicaragua* decision, under the current legal regime, States are hard pressed to effectively and legally undertake collective defense in the face of unconventional threats. Judge Jennings concluded that "[t]his looks to me neither realistic nor just in the world where power struggles are in every continent carried on by destabilization, interference in civil strife, comfort, aid and encouragement to rebels, and the like."140 The international legal community must bring the current prohibitions against aggression clearly to bear on States and non-state actors using unconventional warfare, and especially cyber warfare, to shield themselves from the legal repercussions of waging war.

---