Cyber Operations
Conflict Under International Law
Catherine Lotrionte

On 6 September 2007, Israeli jets flew into Syrian airspace unobserved by Syrian military forces and bombed what Israeli government sources believed to be a nuclear facility. The failure of the Syrian air defense network was the result of an Israeli cyber attack. In the age of cyber warfare, the Israelis defeated the enemy before the battle had begun. The cyber operation facilitated the successful use of kinetic military resources.

Cyberspace, however, can also be used by states to conduct a war without ever needing to engage in kinetic military operations. In 2007, ethnic tension escalated between native Estonians and ethnic Russians in Estonia following the movement of a Soviet era war memorial. That April, Estonia was hit by a Distributed Denial of Service attack (DDOS), which overwhelmed computers and servers across the country for two weeks. By the end of the attacks, Estonia’s largest bank had lost over $1 million. The Estonian authorities ultimately blamed Russia, claiming that at least one query had been traced to an IP address in the Russian administration.

Both episodes demonstrate that cyberspace is a real battle-ground in today’s warfare operations. The first section of
this article examines the challenges in defining the term cyberwar and will propose a working definition for the legal analysis of the topic. The second section considers the relevance of the contemporary [jus ad bellum] to the problems of cyberwar, examining five questions of law:

1. Does international law apply to cyber?
2. Is cyberwar permissible?
3. When is a cyber operation a use of force?
4. When is a cyber operation an armed attack?
5. How does a victim state legally respond to a cyber attack?
6. When can a victim state legally respond to a cyber attack?
7. Where can a victim state legally respond to a cyber attack?

This analysis will focus on state practice in digital activities since 1945, analogous areas of state practice over the same period, and the writings of legal experts and publicists. Finally, the article will set forth a number of conclusions about the relevance of the Charter [jus ad bellum] and [jus in bello] to the post-Charter digital era and the onset of cyber conflict.

**Outlining Cyberwar.** As early as 2006, at least 20 nations had their own cyberattack programs. The rising prominence and risks of cyberspace have forced states to define cyber threats and develop a legal framework for cyberwar operations. There is no one universally accepted definition for “cyberwar,” but most working definitions include a few common elements of all cyber warfare acts:

1. Violence against computers, computer networks or information within computers,
2. The disruption or destruction of information or computer systems.

For the purposes of this article, cyberwar will be defined as: "the unauthorized penetration by, on behalf of, or in support of, a government into another nation’s computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls." It is currently waged by states that use cyberspace to achieve the same ends they pursue through the use of conventional military force: achieving advantages over a competing nation or preventing a competing nation from achieving advantages over them.

That said, the realm of cyber warfare is not likely to remain the exclusive province of states. By 2009, experts agreed that beyond states, "some non-state actors – such as criminal organizations, terrorist, and activists – are developing sophisticated arsenals of cyber weapons and that some have demonstrated a willingness to use them for political objectives." Non-state actors will use cyberspace with or without state support, further complicating the understanding of cyberwar. This poses unique challenges to the developing of a legal framework for cyberwar, such as determining what, if any, relationship non-state actors have with a state sponsor. The relationship between cyber actors and states can be analyzed within four categories:

1. Cyber actors without state tolerance, support, or sponsorship;
2. Cyber actors with state toleration, but without state support or sponsorship;

3. Cyber actors with state support, but without immediate state sponsorship; and

4. Cyber actors with state sponsorship.

“State toleration,” exists when a state does not sponsor or support the cyber group within its borders, but knows of their existence and fails to suppress them and their activities. A state “sponsors” cyber attacks when it "contributes active planning, direction, and control" to a cyber warrior or group.7 "State support" of a cyber warrior group includes "a state’s provision of intelligence, weapons, diplomatic assets, funds or rhetorical endorsement."8

Does International Law apply to Cyber Warfare? The laws governing the legality of the recourse to the use of force (jus ad bellum) and the laws related to the behavior of actors while engaged in conflict (jus in bello) are applicable to cyber operations. This article focuses on jus ad bellum legal issues but introduces some of the principles of jus in bello in addressing the last three questions. Jus ad bellum is a set of rules that govern the resort to armed conflict and determine whether the conflict is lawful or unlawful in its inception.9 In 1945 the UN Charter, in articles 2(4) and 51, redefined previously accepted ideas of jus ad bellum and codified the contemporary jus ad bellum in its entirety.10 If a state activity is a use of force within the meaning of Article 2(4), it is therefore unlawful. Article 2(4) prohibits the threat or use of force to violate another sovereign state.11 There are two primary exceptions within the UN Charter to this restriction, namely when it is an exercise of a state’s inherent right of self-defense in response to an armed attack as recognized under Article 51 of the Charter12 and when it is authorized by the Security Council under its coercive Chapter VII authority. There are competing views as to international law’s applicability in cyberspace. On one hand, the United States has explicitly stated that the laws of war apply to cyberspace, and that it will therefore abide by them.13 On the other hand, states such as China have asserted that "existing mechanisms", such as the international laws of war, do not apply to cyber operations. Such positions taken by states is a point of concern for the United States and other states that seek to minimize the use of force in cyber and maintain peace and security in this domain.14 This article examines some the difficulties in addressing cyber operations under these jus ad bellum principles.

Is Cyber Warfare Permissible under International Law? No existing provision of international law explicitly prohibits cyber warfare. This absence of any detailed prohibition is significant, as it is generally understood that that which international law does not prohibit it permits.15 International law, however, traditionally places limits on when a state may use force. These restrictions as applied in the domains of land, air, space, and sea would also be applicable in cyberspace. In an area where the law is not well-established, such as cyberspace, state practice will likely dominate in establishing what is
acceptable behavior. Where there is a lack of consensus on the applicability of treaty law in this area and little likelihood of a new treaty regulating the cyber domain, state practice will inform the interpretation of the relevant treaty provisions over time. As state expectations shift in the context of cyber warfare the international norms will evolve to meet those expectations.

**When Is a Cyber Operation a Use of Force?** Although the UN Charter outlaws the "use of force," no international treaty, including the UN Charter, actually defines the "threat or use of force." Therefore, the existing international law that governs the use of force must be derived from an analysis of how the Charter’s use of force paradigm has been interpreted by international courts and the Security Council and applied through state practice.

On 1 May 1960, the U.S. high-flying reconnaissance plane, the U-2, piloted by Francis G. Powers, came down within Soviet territory. The U.S. had been clandestinely collecting overflight operations within Soviet territory in order to assess its development of military weapons. Following the incident, the Soviets protested to the United States and on 18 May the Soviet Union requested that the United Nations Security Council convene to consider the U.S. U-2 flight into its territory as "aggressive action." Initially, the U.S. denied the existence of the U-2, claiming that the plane was a missing National Aeronautics and Space Administration (NASA) meteorological observations plane that accidentally crossed into Soviet territory. On 23 May the Soviet Union proposed a draft resolution to the UNSC claiming that actions by the U.S. were acts of aggression in violation of international law. The then-Soviet Foreign Minister Andrei Gromyko argued that under the circumstances where one plane can carry an atomic weapon, such an act justified military retaliation.

The UN Security Council rejected the Soviet draft resolution. While the incursion into Soviet airspace was a violation of the territorial integrity of the Soviet Union, it was not an act of aggression or unlawful use of force. As in this case of the U-2 flights, acts of espionage are generally not considered to be a use of force or act of aggression under international law. At the time of the U-2 incident, both the Soviet Union and the United States assumed that aggression meant the use of armed force in international relations with aggressive intent. They disagreed, however, as to whether the penetration of foreign territory by an unarmed reconnaissance plane operated by another state could be regarded as such a use of armed force. Based on the UNSC discussions, it was generally accepted that such an unarmed plane within another

As state expectations shift in the context of cyber warfare, the international norms will evolve to meet those expectations.
territory would not constitute an act of aggression as used in the Charter.

Over time, states, including the United States and the Soviet Union, have sought to include a broader range of acts within the meaning of a use of force including acts that would not necessarily be armed, but that had aggressive intent. During the 1960s, however, the predominant opinion confined the term to direct uses of or threats to use armed force with aggressive intent justifying defensive military action. It is notable, however, that article 2(4) does not use the word armed in reference to force. Today, there is a general understanding that uses of force do not necessarily have to be actions conducted by a state’s armed forces to constitute a use of force. Most international legal scholars today accept that in analyzing actions that may rise to the level of a use of force consideration should be given to the scale and effects of the actions rather than focusing solely on whether it involved armed action by a state’s forces.

Certainly, if the actions cause the death or injury to persons or damage to property the actions would constitute a use of force. In the cyber context, a cyber operation causing an air traffic control system to fail leading to deaths would constitute a use of force. Furthermore, if the consequences of a cyber operation were to cause significant disruption and turmoil for a state, such was the case of the cyber attacks against Estonia in 2007, even without lose of life, such an operation may constitute a use of force under a scale and effect threshold. In sum, while in the U-2 case infringement of another state’s airspace was found by the UNSC not to constitute an unlawful use of force, the infringement of a state’s computer networks may constitute an unlawful use of force or act of aggression based upon the consequences of the action. Overtime, state practice will provide more clarity on what cyber operations will be considered by states to be uses of force.

**When Is a Cyber Operation an Armed Attack?** In assessing whether a state’s action would constitute a use of force, as discussed above, the goal is to determine whether the actions violate international law (i.e., the UN Charter and customary international law). In contrast, in assessing whether an action constitutes an armed attack under international law, the goal is to determine whether the victim state may forcibly respond in self-defense without violating the article 2(4) prohibition. In *Nicaragua v. United States*, the International Court of Justice (ICJ) asserted that states do not have the right of armed response to acts that do not constitute an armed attack as envisioned by the UN Charter. According to Article 51 of the UN Charter, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security." Accordingly, a state’s right of self defense is dependent upon whether the particular use of force at issue amounts to an armed attack. In the *Nicaragua* case, the ICJ drew a clear distinction between lower-level uses of force and “the most grave forms of the use of force” that
would constitute "armed attacks."25

The UN Charter itself does not provide a definition for an "armed attack" creating some difficulty in extending the notion of armed attack to address non-kinetic cyber attack operations. Using a consequence-based approach reliant on the use of force scale and effects model from the Nicaragua case, however, provides a basis for assessing whether a particular cyber attack constitutes an armed attack. Under this approach, an armed attack does not need to be carried out by traditional military forces. Rather, its consequences would need to be equivalent to an attack by conventional military forces in order for the

armed attack against the facility would have caused great physical destruction and potentially death to those within and near the facility. Similarly, a cyber attack that caused a generator to overheat and fail to function properly, temporarily interrupting service and requiring a replacement, would not meet the threshold of an armed attack. The Stuxnet operation as well as the operation against the generator, however, would likely be categorized as uses of force. The more difficult cases to analyze are those computer operations deployed for purposes of stealing or altering data. Without any physical consequences such cyber operations will not meet the armed attack threshold. If, however, such computer intrusion operations were to result in the disruption of an air traffic control system causing it to fail and planes to crash, the computer operations would rise to the level of an armed attack.

The benefit of adopting a standard for armed attacks under international law for cyber operations would be to assist states in determining when it would be lawful to exercise self-defense using forcible measures to stop and prevent cyber attacks. Without a consensus on what constitutes an armed attack in the cyber domain, states either risk responding against harmful cyber attacks and being condemned by others for "acts of aggression" or refrain-

Without a consensus on what constitutes an armed attack in the cyber domain, states risk being condemned by others for "acts of aggression."

attack to constitute an armed attack for purposes of Article 51.26 For example, if a cyber attack operation does not have the potential to cause the analogous devastating results that a military armed force would, it would not constitute an armed attack, thereby prohibiting any forcible self-defense action. Such a cyber attack, however, may constitute a use of force.

According to this analysis based upon the Nicaragua standard, the Stuxnet cyber attack against the Iranian nuclear facility at Natanz would likely not constitute an armed attack since the result of the cyber operation was the malfunctioning of centrifuges at the facility resulting in no actual physical damage to the facility or death. A military
ing from responding, putting national security at risk.

How Can a Victim State Legally Respond to a Cyber Attack?

International law has developed a number of legal requirements for uses of force beyond the requirements in the UN Charter for self-defense. For example, all uses of force must be necessary and proportional. In the Nicaragua case the ICJ confirmed that both principles were requirements. These limitations were asserted by then-U.S. Secretary of State Daniel Webster in the Caroline Affair of 1837, which involved Great Britain sinking a ship in U.S. territory being used by Canadian rebels to carry out attacks into Canada. In his correspondence with Great Britain, Webster wrote that, to be justified, the use of force in self-defense must be necessary and proportionate under the circumstances of the particular case. Webster asked the British Government to show that the action was “nothing unreasonable or excessive; since the act justified by the necessity of self-defense, must be limited by that necessity, and kept clearly within it.”

A state’s use of cyber weapons in self-defense is not limited to a specific weapon or type of attack as long as under the necessity principle the forcible response is required in order to address the threat (no other non-forcible measures could address the threat) and under the proportionality principle such forcible actions cause no further damage than needed to address the threat under the circumstances. With respect to necessity, for example, if the use of passive measures such as firewalls could stop a cyber attack, a state must use these measures and not resort to a forcible measure of self-defense. The requirement of proportionality is determined by the size and magnitude of what is reasonably necessary to achieve the permissible objectives of any self-defense operation.

States must also follow the principle of discrimination and the principle of chivalry when responding in self-defense. Under customary international law, the principle of discrimination requires that those involved in hostilities distinguish between combatants and noncombatants, avoid targeting civilians and their property, and take all reasonable precautions against injuring civilians or damaging their property in the course of attacking military targets. The modern principle of chivalry dictates that those involved in hostilities are required to distinguish between lawful ruses and unlawful perfidy. While ruses are meant to mislead the enemy and are lawful under the laws of war, acts of perfidy are breaches of expressed or implied agreement between belligerents, such as the misuse of a flag of truce or Red Cross flag, and are prohibited under the laws of armed conflict.

These prohibitions apply just as readily to cyber operations as they do to kinetic operations. For example, if a state sent a logic bomb disguised as an email from the International Committee of the Red Cross to an enemy, this action would be considered perfidious behavior. Another example of a perfidious cyber operation would be an email sent to an adversary declaring its intention to surrender and specifying the time and place that the surrender would take place. However, at the
pre-planned time of surrender those that sent the email ambush the adversary. Just as a state would expect men and women in Red Cross uniforms to be genuine and therefore under legal protection and acts of surrender to be legitimate, so too are Red Cross-based emails and emails of surrender reasonably expected to be genuine, and thereby free of subterfuge. In contrast, permissible ruses in cyber operations could entail the use of false computer identifiers or networks such as a honeypot.

**When Can a Victim State Legally Respond in Self Defense to a Cyber Attack?**

Assuming a cyber attack constitutes an armed attack under international law, a state can legally respond in self-defense to the cyber attack while the attack is on-going in order to stop the attack and after the attack has occurred in order to prevent further attacks. Clearly, article 51 of the UN Charter recognizes the right of states to defend themselves once an armed attack has occurred or is in the process of occurring. The more controversial position is if a state responds in self-defense against an attack before the attack occurs. This principle is referred to as anticipatory self-defense and, although not explicitly mentioned in article 51, has support in the travaux of the UN Charter’s drafting committee. Anticipatory self-defense’s legal basis comes from the 19th century Caroline case. According to then-Secretary of State Webster, anticipatory self-defense is only justified when “the necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment for deliberation.” Traditionally, under anticipatory self-defense, it was understood that the threat would need to be imminent before the right of self-defense was triggered. Particularly with cyber operations where attacks can occur within milliseconds, there may not be any time to act to prevent the attack from occurring once the attack is launched. With cyber operations that threaten the security of the state, state practice may dictate that states will act in anticipation of cyber attacks, before the attacks are launched, in order to ensure the security of the state. Measures of “active defense” may develop through state practice further developing the area of international law with respect to anticipatory self-defense.

**Where Can a Victim State Legally Respond in Self Defense from a Cyber Attack?**

The UN Charter does not provide complete answers to questions such as how far the right of self-defense against cyber attacks extends, or whether this right can be exercised solely at the site of the launch of the actual or potential attack, or beyond that area. If a state allows its territory to be used by another state for launching armed attacks against a third state, the third state can legally use force in self-defense against both the former states. What if the attackers, however, are not a third state but instead simply a group of individuals residing within a neutral state? The United States is concerned about the potential for non-state actors such as terrorist groups or criminal organizations to use cyber operations to attack the United States. Traditionally, international lawyers have characterized the
right of self-defense as applicable only to armed attacks conducted by states. After the 9/11 attacks, however, the Security Council and the international community recognized the applicability of the right of self-defense against al Qaeda as a non-state actor. In the context of cyber where perfect attribution for cyber attacks to a state may be impossible and non-state actors may launch attacks against a state, states may resort to the use of force against non-state actors residing in another state’s territory.

According to both treaty and customary international law, the territory of neutral states is inviolable by the forces of those engaged in armed conflict. An attack using a neutral country’s satellites, computers, or networks could be viewed as infringing upon the neutral’s territory. The attack would therefore be considered illegal and perhaps an act of war against the neutral state. Conversely, a neutral state’s failure to resist the use of its networks for attacks against another country may actually make it a legitimate target for an attack by the country that is the ultimate target of those attacks. All states have a responsibility under customary international law not to allow their territory to be used to cause harm to another state. If a state is unwilling or unable to prevent such harmful use of its territory, a victim state may use proportionate force in order to stop the harmful attacks.

NOTES


3 Ibid.


5 Richard A. Clarke and Robert Knake, Cyber War, (Harper Collins, 2010), 228.


8 Ibid.


11 UN Charter, art. 2, para. 4, “All Members [of the United Nations] 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.” This prohibition is also accepted as customary international law.

12 UN Charter, art. 51: “[n]othing in the present Charter shall impair the inherent right of individual or collective shield-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security…”.


16 U.S. Department of State, E. Europe Region; Soviet Union, Foreign Relations of the United States:


20 The UN General Assembly as equated the use of force by a state against the territory of another state as an “act of aggression.” See Definition of Aggression, G.A. Res. 3314 (XXIX), Annex art. 3(a), U.N. Doc. A/RES/3314 (Dec. 14, 1974).


22 During the proceedings leading to the UN General Assembly’s Declaration on Friendly Relations the suggestion to limit the prohibition on the use of force to armed force was rejected. See U.N. GAOR Special Comm. on Friendly Relations, U.N. Doc. A/AC.125/SR. 114 (1970).

23 The threshold of scale and effect was originally employed by the ICJ in the Nicaragua case in the Court’s assessment of what would constitute an armed attack. The Court drew a distinction between the arming and training of the Contras by the United States which the Court ruled was a use of force versus the funding of the Contras by the U.S. which it ruled did not constitute a use of force. See Nicaragua v. U.S., 1986 I.C.J. 14 (June 27), para. 228.

24 UN Charter, art. 51.


29 Letter from Daniel Webster, U.S. Secretary of State to Lord Ashburton, British Special Minister (Aug. 6, 1842). Reprinted in John Bassett Moore, A Digest of International Law (1906) 412.


31 Moore, Crisis in the Gulf, 158, supra note 27.

32 Nuclear Weapons Advisory Opinion, para. 78 (“States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets.”).

33 IV Hague Convention, 1907, Arts. 2, 3, 24.

34 Derek W. Bowett, Self-Defense in International Law (Great Britain: Manchester University Press, 1958), 188-89.


38 Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (1907), Article 1.
