Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated November 29, 2024

Use of Force in Cyberspace

Introduction

There are presently no internationally accepted criteria for determining whether a nation state cyberattack is a use of force equivalent to an armed attack, which could trigger a military response. Likewise, no international, legally binding instruments have yet been drafted explicitly to regulate inter-state relations in cyberspace. Self-defense and countermeasures for armed attacks are permitted in international law when a belligerent violates international law during peacetime, or violates the law of armed conflict (LOAC) during wartime. However, the term "armed attack" has no universally accepted definition with respect to cyberattacks. In addition to what constitutes an armed attack in cyberspace, questions remain over which provisions of existing international law govern the conduct of war in cyberspace.

Relevant Treaty Provisions

North Atlantic Treaty Article 4: "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened."

North Atlantic Treaty Article 5: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."

United Nations Charter Article 51: "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."

United States Doctrine

In September 2012, the State Department took a public position on whether cyber activities could constitute a use of force under Article 2(4) of the United Nations (U.N.) Charter and customary international law. According to State's then-legal advisor, Harold Koh, "Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force." Examples included triggering a meltdown at a nuclear plant, opening a dam and causing flood damage, and causing airplanes to crash by interfering with air traffic control. By focusing on the ends achieved rather than the means with which they are carried out, this definition of cyber war arguably fits within existing international legal frameworks. If an actor employs a cyber weapon to produce kinetic effects that might replicate fire power under other circumstances, then the use of that cyber weapon rises to the level of the use of force. However, the United States recognizes that cyberattacks without kinetic effects are also an element of armed conflict under certain circumstances. Koh explained that cyberattacks on information networks in the course of an ongoing armed conflict would be governed by the same principles of proportionality that apply to other actions under the LOAC. These principles include retaliation in response to a cyberattack with a proportional use of kinetic force. In addition, "computer network activities that amount to an armed attack or imminent threat thereof" may trigger a nation's right to self-defense under Article 51 of the U.N. Charter. The 2011 *International Strategy for Cyberspace* affirmed that "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country." The 2024 *International Cyberspace & Digital Policy Strategy* states that the United States is working to advance responsible state behavior based on a U.N.-endorsed framework on "the applicability of existing international law, adherence to globally accepted and voluntary norms of state behavior in peacetime, development and implementation of confidence-building measures to reduce the risk of conflict in cyberspace." It refers to the 2023 Department of Defense (DOD) *Cyber Strategy* goal "to reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms." Chapter XVI of the DOD Law of War Manual notes that the United States strives to work with other states to clarify not whether international law applies to cyberspace, but how. Both the Departments of State and Defense contend that cyberattacks rising to the level of an armed attack may trigger mutual defense treaty obligations, though an armed attack in cyberspace remains undefined.

NATO Doctrine

In 2009, the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Center convened an international group of independent experts to draft a manual on the law governing cyber conflict. The first *Tallinn Manual*, as it is known, was published in 2013 and offers 95 "black letter rules" addressing sovereignty, state responsibility, the LOAC, humanitarian law, and the law of neutrality. The *Tallinn Manual* is an academic text and as such nonbinding. The February 2017 *Tallinn Manual 2.0* expands upon the first and offers 154 black letter rules governing cyber operations, including in peacetime. In the provisions of Article 5 of the North Atlantic Treaty, an attack on one member is considered an attack on all, affording military assistance in accordance with Article 51

of the U.N. Charter. However, NATO does not presently define cyberattacks as clear military action. The *Tallinn Manual* equates a use of force to those cyber operations whose "effects ... were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack." Article 4 of the North Atlantic Treaty applies the principles of collective consultation to any member state whose security and territorial integrity has been threatened; however, it is unclear how this article would apply to the various categories of cyberattacks, some of which may not have kinetic equivalents. Also unclear is the concept of jurisdiction and what constitutes territorial integrity for those member states who view cyberspace as a global domain or commons.

International Law

The so-called "Law of War," also known as the LOAC, embodied in the Geneva and Hague Conventions and the U.N. Charter may apply to cyberattacks, but lacks specific agreement on its applicability. Complicating factors include difficulties in attribution, the potential use of remote computers, and possible harm to third parties from cyber counterattacks, which may be difficult to contain. In addition, as with NATO doctrine, questions of territorial boundaries and what constitutes an armed attack in cyberspace remain. The law's application would appear clearest in situations where a cyberattack causes physical damage, such as disruption of an electric grid. As mentioned above, the *Tallinn Manual* addresses many of these questions. In the absence of a treaty-based definition for what constitutes an armed attack or use of force in cyberspace, *Tallinn Manual* co-author Michael Schmitt has proposed in his academic publications criteria for analysis under international law.

Schmitt Analysis

Severity: Consequences involving physical harm to individuals or property will alone amount to a use of force while those generating only minor inconvenience or irritation will not. The more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force.

Immediacy: The sooner consequences manifest, the less opportunity states have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, states harbor a greater concern about immediate consequences than those that are delayed or build slowly over time.

Directness: The greater the attenuation between the initial act and the resulting consequences, the less likely states will be to deem the actor responsible for violating the prohibition on the use of force.

Invasiveness: The more secure a targeted system, the greater the concern as to its penetration. By way of illustration, economic coercion may involve no intrusion at all (trade with the target state is simply cut off), whereas in combat the forces of one state cross into another in violation of its sovereignty. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target state's territory.

Measurability: The more quantifiable and identifiable a set of consequences, the more a state's interest will be deemed to have been affected. This is particularly challenging in a cyber event where damage, economic or otherwise, is difficult to quantify. Economic coercion or hardship does not qualify under international law as an armed attack.

Presumptive legitimacy: In international law, acts that are not forbidden are permitted; absent an explicit prohibition, an act is presumptively legitimate. For instance, it is generally accepted that international law governing the use of force does not prohibit propaganda, psychological warfare, or espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate.

Responsibility: The law of state responsibility governs when a state will be responsible for cyber operations. However, that responsibility lies along a continuum from operations conducted by a state itself to those in which it is merely involved in some fashion. The closer the nexus between a state and the operations, the more likely other states will be inclined to characterize them as uses of force, for the greater the risk posed to international stability. Attributing the level of state involvement to a cyberattack can be particularly challenging.

The basic principles encompassed in the Hague Conventions regarding the application of Armed Forces are those of military necessity, proportionality, humanity, and chivalry. A nation whose military is conducting cyber operations according to these principles may be said to be engaging in cyber war.

United Nations Norms

A 2004 U.N. General Assembly resolution called for the convening of and a report from an international group of government experts (GGE) from 15 nations, including the United States, to secure cyberspace by agreeing upon "norms, rules and principles of responsible behaviour by States." Unlike the work done at Tallinn under the auspices of NATO, this U.S.-led process included both China and Russia. The 2015 GGE report achieved consensus on 11 norms for the use of cyberspace, to include, among others, that nations (1) should not intentionally damage each other's critical infrastructure with cyberattacks, (2) should not target each other's cyber emergency responders, and (3) should assist other nations investigating cyberattacks launched from their territories. A fourth norm, stating the United States will not use cyber surveillance to steal information about foreign companies to benefit U.S. firms, was articulated by then-Secretary of State John Kerry and adopted as official U.S. government policy. While also nonbinding, U.N. Resolution 70/237 calls upon member states to be guided by the norms set forth in the 2015 GGE report. The following 2016/2017 GGE failed to achieve consensus, due in part to objections from some member countries on explicitly applying rules on the use of force under Article 51, which they argued would represent the militarization of cyberspace. The March 2021 final GGE report affirms the applicability of both international law and the U.N. Charter in its entirety. The 2021 GGE report also notes that international humanitarian law applies only in situations of armed conflict.

Catherine A. Theohary, Specialist in National Security Policy, Cyber and Information Operations

Disclaimer