AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY

# The Legal Limits of Targeting the Cyber Capabilities of a Neutral State

by

Ja Rai A. Williams, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

**MASTER OF OPERATIONAL ARTS AND SCIENCES**

Advisor: Wing Commander Graem Corfield, RAF

Maxwell Air Force Base, Alabama

October 2015

**Disclaimer**

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

**Abstract**

Legal practitioners must rely on current international law and norms to address the legalities of injurious cyber operations conducted by one State against another State.[1] Cyber operations can be surprising and debilitating—especially if States conduct such operations against U.S. armed forces. With its focus on defensive operations, the U.S. military appears to be less prepared to act offensively. In *Cyber War*, Richard A. Clarke and Robert K. Knake wrote "there is no conventional military force in the world superior to that of the U.S., assuming that the U.S. military is not blinded or disconnected by a cyber attack."[2] However, due to the nature of these types of operations and the need for swift action, it is imperative that experts prepare for potential scenarios that are likely to occur. Therefore, this thesis is a scenario-based research paper to contribute to such an exercise. This project seeks to address how the U.S. can target the cyber capabilities of a neutral State that provides data useful to an enemy engaged in an armed conflict against the U.S. and permits the enemy's access to its cyber infrastructure—both with and without the neutral State's knowledge.

In conducting research for my thesis, this author primarily relied on the *Tallinn Manual on the International Law Applicable to Cyber Warfare* ("*Tallinn Manual*"). The *Tallinn Manual* is the result of a project that brought together distinguished international law practitioners and scholars in an effort to examine how extant legal norms applied to cyber warfare.[3] While many of the specific issues analyzed in the *Tallinn Manual* did not result in unanimity among the group of experts, it is persuasive that the work embodies efforts from a consensus of the group rather than one purported authority or expert on this subject. Thus, after reviewing the *Tallinn Manual* and other persuasive authorities, this author concluded with limitations inherent in the Law of Armed Conflict ("LOAC") when a State that is involved in an armed conflict uses the cyber

capabilities of a neutral State to gather information that is used to attack its opponent, and that attack causes injury to people and property, the aggrieved State can target the neutral State's cyber capabilities with cyber attacks. This paper also analyzes variations to the scenario this author presented. While this body of work includes this author's opinion regarding the legality of such operations, it does not address the means by which to conduct them as experts who are trained to actually employ such maneuvers can make this determination.

## Contents

## Introduction

Cyber warfare is a prevalent concept that has been the subject of much rhetoric over the past decade. As this rhetoric increases, experts are emerging and scrutinizing existing international norms to determine how to best analyze cyber operations conducted by both State and non-State actors. International law has developed over centuries to establish who can carry out acts of warfare and who must remain apart from engaging in conflict.[4] Most of the international agreements and practices of States that comprise LOAC predate the cyber era and many observers believe the need for a new legal regime designed for cyber war is urgent.[5] However, the President of the United States' *International Strategy for Cyberspace* States: "[t]he development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete."[6] It also States that "[l]ong-standing international norms guiding State behavior—in times of peace and conflict—also apply in cyberspace."[7] In addition, according to Professor Michael Schmitt, claims that cyberspace is a new domain to which international law is inapplicable (or inapplicable in part) persist but are steadily diminishing.[8]

While many cyber experts grapple with defining cyber activities that amount to warfare, this paper will address an armed conflict scenario that encompasses both kinetic and cyber operations. Cyber attacks do not typically include physical effects, but there have been a handful of notable exceptions.[9] Moreover, there is a growing body of evidence that nations and non-State actors are looking to cyber assets as a mechanism for inflicting damage against opponents.[10] Whether the law of war applies to a particular cyber activity or operation may depend on whether a State of armed conflict exists between the actors.[11] Furthermore, if death, injury, damage or destruction results from an activity, it is likely to be considered a use of force

under international law.[12] Thus, when a State that is involved in an armed conflict uses the cyber capabilities of a neutral State to gather information that is used to attack its opponent, and that attack causes injury to people and property, the aggrieved State can target the neutral State's cyber capabilities with cyber attacks with the same limitations inherent in LOAC if three conditions exist. First, the aggrieved State must comply with the LOAC principles of military necessity, the avoidance of unnecessary suffering, proportionality and distinction. Second, the neutral State must have actual or constructive knowledge of the cyber activity at issue. Third, the neutral State must be unwilling or unable to take timely action to rectify the matter.

**Scenario**

The United States ("U.S.") and State B are engaged in armed hostilities within which both countries have employed their armed forces against the other and have routinely engaged in cyber attacks in furtherance of the conflict. One such attack included the use of a modular computer malware virus to target the other State's government computer systems, accessing personnel files of military members. Another cyber attack involved the hijacking of a large number of the other State's government computers located on a military network at a higher headquarter, causing servers to overload due to a flooding of traffic and severely disrupting electronic communication.

Most recently, State B used a neutral State's ("State N") private, government monitored satellite systems to locate and disable the U.S.'s defenses at a top-secret location in an allied State bordering State B. The U.S. used this top-secret location for intelligence, surveillance and reconnaissance ("ISR") operations pertaining to the ongoing conflict with State B. The location primarily housed ISR personnel and assets.

State B relied on State N's satellite capabilities due to the U.S.'s degradation of State B's cyber systems. The U.S. does not have open access to State N's satellite capabilities. Incidentally, State B previously provided State N with component parts that State N's government contractor used to produce its satellite systems. State B first used State N's reconnaissance satellite system to locate the U.S.'s classified ISR location. Next, State B remotely disabled the defenses used by the ISR personnel. Finally, State B used State N's small satellite dish-based computer systems to run a Supervisory Control and Data Acquisition system controlling an electrical grid in the allied State resulting in a fire at the ISR location. The fire caused the deaths of over one hundred ISR personnel and destroyed a large number of ISR systems. State N has publicly declared its neutrality with regards to the conflict but its government leaders at the highest levels–both military and civilian–knew that State B was using its satellite system to gain information about the military assets of the U.S due to information they received from the governmental intelligence agency. However, State N was largely concerned with that informing the U.S. of State B's activities would invoke the ire of State B. State N has economic ties to State B, as they were neighbors, and a large diaspora of State B supporters are residents of State N. Thus, State N's leaders opted to instead monitor State B's use of its satellite system and keep the public (and both parties to the conflict) unaware of the extent of its knowledge.

State B signed and ratified the Geneva Conventions of 1949 and two of its three protocols. State N signed and ratified both the Geneva Conventions of 1949 and all three of its protocols.

**The U.S.'s Military Objective**

In order to determine if it can target State N's satellite systems with cyber attacks, the U.S. must first analyze its duty to ensure compliance with the basic LOAC principles of military necessity, the avoidance of unnecessary suffering, proportionality, and distinction. Military objectives are defined as those objects which by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military objective.[13] In addition, it is unlawful for a party to a conflict to destroy or seize the enemy's property unless the necessities of war imperatively demand such destruction or seizure.[14] In regards to targeting, attacks must be limited strictly to military objectives.[15]

In accordance with the *Tallinn Manual*, LOAC governs all cyber operations that either the U.S. or State B conducts in the context of the described hostilities.[16] The manual offers that computers, computer networks, and cyber infrastructure may be the object of attack if they are military objectives.[17] At least two aspects of State N's cyber infrastructure have become the U.S.'s military objective and lawful targets. Its satellite systems enabled State B to obtain highly sensitive information and permitted them to facilitate a cyber attack that resulted in the death of U.S. personnel and the destruction of U.S. property.

Still, the U.S.'s right to injure portions of State N's cyber infrastructure is not unlimited as the principle of unnecessary suffering dictates that the injury must not be disproportionate to the military gain.[18] While it is difficult to imagine what could constitute suffering in the virtual world, cyber activities can have a significant impact on the physical world to the degree that a cyber attack causes suffering.[19] A broad-based cyber attack on a State N's infrastructure could keep the power-grid off-line for weeks, pipelines unable to move gas and oil, trains sidelined,

airlines grounded, banks unable to dispense cash, distribution systems crippled, and hospitals working at severely limited capacity.[20] State N's civilian population could be left in cold, darkened dwellings with little access to food, money, medical care, or news about what's happening.[21] For example, if the U.S. seizes or destroys all of State N's satellite capabilities, this could result in catastrophic loss to State N if an environmental weather condition occurs, since the ability to warn its population dissipates with the destruction of the satellite capability. Although this example may be tenuous, the point is the global interdependence of the cyber infrastructure warrants the U.S.'s analysis of the effects of unnecessary human suffering by virtue of its attack of State N's cyber capabilities.

Similarly, the U.S. must consider the principle of proportionality—whether the proposed action is expected to cause collateral damage—before it targets State N's cyber infrastructure. Incidental civilian death or injury, or damage to civilian objects, may not be excessive in relation to the concrete and direct military advantage anticipated by those actions.[22] In this regard, the *Tallinn Manual* offers that a prohibited cyber attack is one that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[23] Furthermore, a cyber attack can cause collateral damage during transit and because of the cyber attack itself.[24] Thus, if the U.S. attacks State N's satellite and destroys its Global Positioning System, and this denial of navigational data will cause damage to merchant vessels and civil aircraft relying on such data, the U.S.'s military advantage must exceed these harms (and these harms can be calculated into the timing of a U.S. cyber attack).[25]

Finally, the U.S. must apply the principle of distinction to its cyber operation against State N. This principle, also referred to as discrimination, requires parties to a conflict to

distinguish between combatants and the civilian population, and between military objects and civilian property.[26] A cyber attack against civilians or civilian objects—or other protected persons and objects—is prohibited by this principle and those rules of LOAC that derive from the principle.[27] For instance, the principle of distinction would prohibit the U.S. from using self-replicating, destructive malware which is incapable of distinguishing between military and civilian targets.[28] However, dual-use systems that provide service and capabilities to the civilian population and that are also used for military purposes (e.g. State N's satellite/Global Positioning System, as Stated above) are lawful military objectives since they make an effective contribution to State B's warfighting efforts.[29]

**The Law of Neutrality: State N's Knowledge**

After confirming whether U.S. cyber attacks against State N's satellite systems are in compliance with the principles of LOAC, the U.S. must determine whether State N has actual or constructive knowledge that State B used its cyber infrastructure for military purposes against the U.S. International law generally recognizes the right of States to declare themselves 'neutral' by openly indicating they are taking no part in hostilities.[30] Although the right already existed by custom, neutrality was officially recognized in Hague Convention V, *Respecting the Rights and Duties of Neutral Powers and Persons (1907),* and Hague Convention XIII, *Concerning the Rights and Duties of Neutral Powers in Naval War*.[31]

The law of neutrality regulates the relationship between the parties to an international conflict and States that are not party to the conflict.[32] One of its key purposes is to protect parties to a conflict against action or inaction on the part of neutral States that benefits their enemies.[33] Due to global dependency on cyber infrastructure, cyber operations of the parties to a conflict can easily affect private or public neutral cyber infrastructure.[34] Cyber infrastructure located

within the territory of a neutral State is considered neutral in character provided that is it not used for the exercise of belligerent rights as outlined in the *Tallinn Manual*.[35] Thus, 'neutral cyber infrastructure' means public or private infrastructure that is located within neutral territory.[36] This includes civilian cyber infrastructure owned by a party to the conflict or that has the nationality of a neutral State (and is located outside of the enemy's territory).[37]

The armed force of a party to the conflict is prohibited from conducting cyber operations from neutral territory.[38] This encompasses remotely taking control of neutral cyber infrastructure and using it for such purposes.[39] A neutral State may not knowingly allow the exercise of belligerent rights by the parties to the conflict from cyber infrastructure located in its territory or under exclusive control.[40] 'Belligerent rights' are actions that a party to the conflict is entitled to take in connection with the conflict, to include cyber operations.[41] The phrase 'under its exclusive control' refers to non-commercial government cyber infrastructure.[42] Moreover, a neutral State may not allow a party to the conflict to use its pre-existing cyber infrastructure on neutral territory for military purposes.[43] An exception applies to public, internationally and openly accessible networks.[44] A neutral State has actual knowledge of such cyber activity if it detected a cyber operation conducted by a party to a conflict or that party informed the neutral State of its activity. [45] It has constructive knowledge if it should reasonably have known of the activity.[46]

State N generally had actual knowledge that State B was using its satellite system to gain information about the U.S. Even if State N did not have extensive knowledge regarding State B's plan to employ a virus to attack its SCADA system, it reasonably should have known that State B might attempt to attack the U.S. using its cyber infrastructure since both parties have attacked the other through the cyber realm. State N cannot benefit from its choice to act as if it is

ignorant to State B's activities. The issues, however, are how the U.S. will determine what and how much State N knew. It is reasonable to expect that State N will keep this information closely held to insulate itself from the fallout.

**The Law of Neutrality: The U.S.'s Action**

If State N has knowledge of State B's cyber activities and is unwilling or unable to take action to prevent State B's activities, the U.S. can take immediate action to eliminate further threats to its security. If a neutral State fails to terminate the exercise of belligerent rights on its territory, the aggrieved party to the conflict may take such steps, including cyber operations, as are necessary to counter that conduct.[47] This rule only applies to violations that negatively affect the aggrieved party.[48]

Moreover, the operation of this rule depends on two criteria.[49] First, the violation of the neutral State's territory must be 'serious.'[50] In this regard, State B's use of State N's satellite systems in order to ultimately attack the U.S. resulted in the loss of lives and assets; thus, the violation is serious.[51] Second, the exercise of belligerent rights on neutral territory by a party to the conflict must represent an immediate threat to the security of the aggrieved party and there must be no feasible and timely alternative to taking action on neutral territory.[52] Therefore, the rule only applies if the neutral State is either unwilling or unable to comply with its obligations to not allow a party to the conflict to use its cyber infrastructure on neutral territory for military purposes.[53] Thus, State N's failure to either inform the U.S. of this activity or request that State B cease and desist means it failed to comply with its obligations.

Measures of self-help are subject to a requirement of prior notification that allows a reasonable time for the neutral State to address the violation.[54] However, if the violation immediately threatens the security of the aggrieved party and there is an absence of any feasible

and timely alternative, that party may use such immediate force as is necessary to terminate the violation.[55] If the U.S. is unable to determine whether State N knew of State B's cyber activities, then it would usually be required to notify State N of its intent to take action if State N fails to do so. But State B's use of State N's satellite system poses an immediate threat to the U.S. as evidenced by the death and destruction that already occurred from the prior use and attack.

In addition, the U.S. does not have the time to place confidence in State N's ability to take action (or even figure out what action it should take). Thus, the U.S. should immediately disable State N's satellite capabilities for a duration that is necessary for State N to step in and address the situation. While such an act will likely have an impact on the civilian population, the U.S. advantage in doing so outweighs the impact on the population and forces State N to take responsibility. There is the risk that State N may enter the conflict in opposition of the U.S. by virtue of such action. But if the U.S. fails to take this course of action, State B will be emboldened and other States will be more likely to do exactly what State N did—nothing—in an effort to remain "neutral."



Because of the interconnected nature of cyberspace, cyber operations targeting networked information infrastructures State N may create effects in another State that is not a party to the armed conflict.[56] For this reason, the U.S. also must ensure it evaluates the effects on the sovereignty of other States before initiating a cyber attack on State N.

## Variations to the Scenario

### *Variation #1: What if State N was unaware of State B's use of its government satellite system?*

If State N did not know of State B's activities, it certainly should have known that an outsider was exploiting its satellite capabilities. As previously discussed, neutral States are obliged to take all feasible measures to terminate an abuse of the cyber infrastructure located

within their territory (or on their sovereign immune platforms) by any of the belligerents.[57] Therefore, the requirement that the U.S. notify State N of State B's violation remains the same in this scenario. For example, if State B routes cyber operations against the U.S. through a server in State N, the U.S. must demand that State B prevent this use of its cyber infrastructure.[58] If State N fails to terminate the operations in a timely manner, the U.S. may lawfully launch a cyber operation to destroy the server's functionality.[59] However, LOAC still permits the U.S. to take immediate action if it deems it necessary.

***Variation #2: What if State B used State N's publicly accessible cyber infrastructure to gain the same information with State N's knowledge?***

When belligerent parties use for military purposes a public, internationally and openly accessible network such as the Internet, the fact that part of this infrastructure is situated within the jurisdiction of a neutral State does not constitute a violation of neutrality.[60] As such, merely relaying information through a neutral communications infrastructure (provided that the facilities are made available impartially) generally would not constitute a violation of the law of neutrality. This rule was developed because the drafters viewed it impractical for neutral States to censor or screen their publicly available communications infrastructure for belligerent traffic. Moreover, many experts believe this rule to be applicable even if the information that is being routed through neutral communications infrastructure may be characterized as a cyber weapon or otherwise could cause destructive effects in a belligerent State (but no destructive effects within the neutral State).[61]

Thus, it would not be prohibited for State B to route information through the cyber infrastructure of State N that is open for the service of public messages. In addition, State N would have no obligation to forbid such traffic.

***Variation #3: What if State B used a private satellite from a commercial company operating within State N but not under State N's control?***

The private cyber infrastructure located within the territory of a neutral State is protected against any harmful interference by the belligerents. It does not matter whether the respective cyber infrastructure is owned (or exclusively used) by the government, corporations or private individuals.[62] So State B is prohibited from using the cyber infrastructure of commercial companies that operate from neutral territory to conduct cyber attacks against the U.S.[63] Thus, if such a violation does occur, the U.S. would have to engage in the same process of notifying State N of the violation and requesting State N take action to prevent the violation. Notably, if the private company's cyber infrastructure is publicly accessible and available to both the U.S. and State B, then the second variation explored above would apply.

There would still be a violation of the law of neutrality even if a commercial company operating from State N permits State B to do so. Take, for the example, Russia's alleged distributed denial of service cyber attack against Estonia in 2008. Shortly after these attacks, a U.S. company with no clear authority and no apparent U.S. government approval directly contacted the Georgian government and arranged to protect its Internet assets by moving them to U.S. territory.[64] In this instance, the actions of the Georgian government and this U.S. company could have imperiled U.S. cyber neutrality even though the company's actions had no U.S. government involvement or approval.[65]

However, the larger issue is whether the U.S. can target a commercial company's cyber infrastructure. Civilian objects shall not be made the focus of cyber attacks.[66] Decision-makers must determine on a case-by-case basis whether an object is a civilian object protected from attack or a military objective subject to an attack.[67] But when a civilian object or facility is used

for military ends, it loses its protected status and becomes a military objective.[68] To qualify as a military objective, the object in question must, through one of the four criteria, make "an effective contribution to military action."[69] Thus, if a party to the conflict uses a certain civilian computer network for military purposes, that network loses its civilian character and becomes a military objective.[70]

This is so even if the network also continues to be used for civilian purposes.[71] An entire computer network does not qualify as a military objective based on the mere fact that an individual router so qualifies.[72] However, it may be impossible to know over which part of the network military transmissions, as distinct from civilian ones, will pass.[73] In such cases, the entire network, or at least those aspects in which transmission is reasonably likely, qualifies as a military objective.[74] Civilian objects that have become military objectives by use can revert to civilian status if military use is discontinued.[75] Once that occurs, they regain their protection from the attack.[76]

Given this, it is important that the U.S. provides State N with the opportunity to take action to prevent a company operating from its territory from allowing State B to use its cyber infrastructure—whether knowingly or unknowingly. For the reason that private commercial companies have considerable control over the cyber infrastructure, this poses a unique challenge to the application of LOAC to cyber operations. Although nations still bear ultimate responsibility for the acts of their citizens or surrogates, translating this protocol to fit the modern realities of cyber conflict is a complex challenge.[77]

## Conclusion

It is well-settled that harmful State on State conduct in cyberspace is subject to international law and norms. However, applying these norms pose inexact challenges unique to

cyber operations. The U.S. military is dependent on its cyber systems without which it would function with reduced effectiveness.[78] In this regard, potential enemies cannot overlook the value of cyber operations as a means to erode the U.S.'s fighting capabilities, and hence cyber operations are a part of present and future conflicts.[79] This paper specifically addresses a scenario that included both kinetic and cyber operations whereby a cyber attack resulted in the death, damage and destruction of U.S. armed forces personnel and property. Thus, under the facts of this scenario, because State B is involved in an armed conflict with the U.S. and used State N's cyber capabilities to gather information that is used to attack the U.S., and that attack causes injury to people and property, the U.S. can target State N's cyber capabilities with cyber attacks. However, the same considerations applied to kinetic operations in accordance with LOAC also apply to cyber operations.

**Bibliography**

*Additional Protocol to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflict (Protocol I)*, adopted 8 June1977, 1125 U.N.T.S. (1979) 3-608, 16 I.L.M. (1977) 1391-441 (entry into force 7 December 1978, signed by the U.S. 12 December 1977; not submitted to the Senate).

Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 9 (May 2011).

*Charter of the United Nations with the Statute of the International Court of Justice annexed thereto*, 26 June 1945, 59 Stat. 1031, T.S. 993, 3 Bevans 1153, (as amended, 17 December 1963, 16 U.S.T. 1134; T.I.A.S. 5857; 557 U.N.T.S. 143 20 December 1965, 19 U.S.T. 5450; T.I.A.S. 6529 and 20 December 1971, 24 U.S.T. 2225; T.I.A.S. 7739) (entry into force 24 October 1945, for U.S. same date).

*Department of Defense Law of War Manual* (June 2015), www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf.

Hague Convention No. IV, *Respecting the Laws and Customs of War on Land and Annex Thereto*, 18 October 1907, T.S. 539, 36 Stat. 2227.2 A.J.I.L. (1908), Supplement 90-117 (entry into force 26 January 1910, for U.S. 27 November 1909).

Hague Regulations (1907).

Jens David Ohlin, Kevin Govern, and Claire Finkelstein (ed), *Cyberwar, Law and Ethics for Virtual Conflicts* (New York: Oxford University Press).

John Wardell III, *The Enemy as a System*, Airpower Journal (Spring 1995).

Joshua E. Kastenberg, "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law," 64 AFLR 43-64 (2009).

Kristen M Thomasen, *Air Power, Coercion, and Dual-Use Infrastructure: A Legal and Ethical Analysis*, International Affairs Review (October 24, 2008), http://www.iar-gwu.org/node/40,

Major General (retired) Charles J. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwarfare," Strategic Studies Quarterly (Spring 2011), www.au.af.mil/au/ssq/2011/spring/spring11.pdf .

Michael N. Schmitt (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

Naval Warfare Publication, *The Commander's Handbook on the Law of Naval Operations*, NWP 1-14M (July 2007).

Paul J. Springer, *Cyber Warfare*, (Santa Barbara: ABC-CLIO).
Program on Humanitarian Policy and Conflict Research at Harvard University, Manual on International Law Applicable to Air and Missile Warfare, Section X (Bern 2009).

Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins).

Wolff Heintschel von Heinegg, "Neutrality in Cyberspace" (Tallinn: NATO CCD COE Publications, 2012), https://ccdcoe.org/sites/default/files/multimedia/pdf/1_3_von_Heinegg_NeutralityInCyberspace.pdf.

**Endnotes**

[1] I wish to thank Professor Michael Schmitt for his suggestions on research topics.
[2] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins), 196.
[3] Michael N. Schmitt (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), 1-5.
[4] Paul J. Springer, *Cyber Warfare*, (Santa Barbara: ABC-CLIO), 52.
[5] Major General (retired) Charles J. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwarfare," Strategic Studies Quarterly (Spring 2011): 82, www.au.af.mil/au/ssq/2011/spring/spring11.pdf (argues that LOAC does apply).
[6] Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 9 (May 2011), 9.
[7] Ibid., 9.
[8] Jens David Ohlin, Kevin Govern, and Claire Finkelstein (ed), *Cyberwar, Law and Ethics for Virtual Conflicts* (New York: Oxford University Press), v.
[9] Springer, *Cyber Warfare*, 53.
[10] Ibid., 53.
[11] Department of the Air Force, The Judge Advocate General's School, *Air Force Operations and the Law* (3rd ed., 2014), 105, www.afjag.af.mil/library/.
[12] *Charter of the United Nations with the Statute of the International Court of Justice annexed thereto*, 26 June 1945, 59 Stat. 1031, T.S. 993, 3 Bevans 1153, (as amended, 17 December 1963, 16 U.S.T. 1134; T.I.A.S. 5857; 557 U.N.T.S. 143 20 December 1965, 19 U.S.T. 5450; T.I.A.S. 6529 and 20 December 1971, 24 U.S.T. 2225; T.I.A.S. 7739) (entry into force 24 October 1945, for U.S. same date), art. 2(4) and 51.
[13] *Additional Protocol to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflict (Protocol I)*, adopted 8 June1977, 1125 U.N.T.S. (1979) 3-608, 16 I.L.M. (1977) 1391-441 (entry into force 7 December 1978, signed by the U.S. 12 December 1977; not submitted to the Senate), art. 52(2)(Although not a party to this protocol, the U.S. considers this provision to be a reflection of customary international law. FM 27-10, Law of War Documentary Supplement (2008), pp. 396-401.); Schmitt, *Tallinn Manual*, Rule 38; *Air Force Operations and the Law*, 105.
[14] Hague Convention No. IV, *Respecting the Laws and Customs of War on Land and Annex Thereto*, 18 October 1907, T.S. 539, 36 Stat. 2227.2 A.J.I.L. (1908), Supplement 90-117 (entry into force 26 January 1910, for U.S. 27 November 1909), art. 23(g).
[15] *Additional Protocol I*, art. 52(2).
[16] Schmitt, *Tallinn Manual*, Rule 20, Rule 22.
[17] Ibid., Rule 37.
[18] *Additional Protocol I*, art. 35(1).
[19] *Air Force Operations and the Law*, 106.
[20] Clarke, *Cyber War*, 242.
[21] Ibid., 242-243.
[22] *Additional Protocol I*, art. 57(2)(a)(iii); *Air Force Operations and the Law*, 106.
[23] Schmitt, *Tallinn*, Rule 51; *Additional Protocol I*, art. 51(5)(b), 57(2)(iii).

[24] Schmitt, *Tallinn Manual*, 160.
[25] Ibid., 160.
[26] *Additional Protocol I*, art. 48; Naval Warfare Publication, *The Commander's Handbook on the Law of Naval Operations*, NWP 1-14M (July 2007), para. 5.3.2; *Air Force Operations and the Law*, 107.
[27] Schmitt, *Tallinn Manual*, 112.
[28] *Air Force Operations and the Law*, 107.
[29] Kristen M Thomasen, *Air Power, Coercion, and Dual-Use Infrastructure: A Legal and Ethical Analysis*, International Affairs Review (October 24, 2008), http://www.iar-gwu.org/node/40 ; John Wardell III, *The Enemy as a System*, Airpower Journal (Spring 1995); *Air Force Operations and the Law*, 107.
[30] *Air Force Operations and the Law*, 111.
[31] *Air Force Operations and the Law*, 111.
[32] Schmitt, *Tallinn Manual*, 248.
[33] Ibid., 248-49.
[34] Ibid., 249.
[35] Ibid., 249.
[36] Ibid., 248.
[37] Ibid.
[38] Ibid., 251.
[39] Ibid.
[40] Ibid., Rule 93.
[41] Ibid., 249.
[42] Ibid., 253.
[43] Ibid., 252.
[44] Ibid.
[45] Ibid., 253.
[46] Ibid.
[47] Ibid., Rule 94.
[48] Ibid., 254.
[49] Ibid., 255.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] *Department of Defense Law of War Manual* (June 2015), 113, www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf.
[57] Wolff Heintschel von Heinegg, "Neutrality in Cyberspace" (Tallinn: NATO CCD COE Publications, 2012), 37, https://ccdcoe.org/sites/default/files/multimedia/pdf/1_3_von_Heinegg_NeutralityInCyberspace.pdf.
[58] Schmitt, *Tallinn Manual*, 255.
[59] Ibid.

[60] Program on Humanitarian Policy and Conflict Research at Harvard University, Manual on International Law Applicable to Air and Missile Warfare, Section X (Bern 2009), Rule 167(b).
[61] *DoD Law of War Manual*, 1003.
[62] Von Heinegg, *Neutrality in Cyberspace*, 38.
[63] Schmitt, *Tallinn Manual*, 252.
[64] Joshua E. Kastenberg, "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law," 64 AFLR 43-64 (2009); 60-61
[65] Ibid., 61.
[66] Schmitt, *Tallinn Manual*, Rule 37.
[67] Ibid., 125.
[68] Hague Regulations (1907), Art 27 (noting that civilian objects enjoy protected status unless "used at the time for military purposes").
[69] Schmitt, *Tallinn Manual*, 130.
[70] Ibid., 128.
[71] Ibid.
[72] Ibid.
[73] Ibid., 135.
[74] Ibid.
[75] Ibid., 129.
[76] Ibid., 129.
[77] Kastenberg, Non-Intervention and Neutrality in Cyberspace, 47.
[78] Springer, *Cyber Warfare*, 53.
[79] Springer, *Cyber Warfare*, 53.