SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013 ARTICLE 2, PAGE 51

Neutrality in the Digital Battle Space: Applications of the Principle of Neutrality in Information Warfare

By Allison Gaul*

Table of Contents

Introduction	53
United States Defense Industry Infiltration	53
Stuxnet & the Iranian Nuclear Program	54
Estonia	56
The Georgian Conflict	58
1. Laws of Armed Conflict	62
2. The Principle of Neutrality	63
A. The Hague Convention	64
B. Privileges Afforded to neutrals	66
C. Duties and Obligations	66
i. Duty to Remain Impartial	67
ii. Duty to Intervene	68
iii. Duty to Repel Belligerent Forces	72
D. Right of Necessity	73
E. Conclusion	74
3. What is Information Warfare?	74
A. Armed Conflict, Espionage, or Criminal Activity?	76
i. Armed conflict	77
ii. Espionage and Military Intelligence Operations	79
iii. Criminal Activity	80
iv. Is Information Warfare Armed Conflict?	82
B. Types of Information Warfare	82
i. Exploitation	83
ii. Destruction	86
iii. Disruption	89
C. Conclusion	92
4. Analysis	93
A. How the Use of Information Warfare Affects the Privileges and Immunities of a Neutral State	93
B. What's a Neutral to do?	96
C. Applying The Hague Convention to Information Warfare Scenarios	106
5. Conclusion	110

* J.D. from Temple University Beasley School of Law. Patent Attorney with a background in Applied Mathematics & IT security. Special thanks to David Post for the many helpful reviews.

ABSTRACT

As technology develops, the spectrum of potential uses for information warfare will broaden. Creation of new applications for weaponized bits and bytes will inevitably result in the generation of new legal questions. The information warfare scenarios discussed in this article are a sample of the possible uses for digital attacks. It does not address every potential legal factor but instead examines the basis for applying the Law of Armed Conflict to information warfare that involves neutral states. Specifically, the article examines whether the Hague Convention of 1907 and subsequent Hague Rules Regarding Aerial Warfare, as pillars of the LoAC, can be reasonably applied to information warfare involving neutral states.

Introduction

The first decade of the 22nd century has seen the emergence of information warfare as a means of armed conflict that offers non-lethal, rapid strike capabilities. Many nations have military cyber divisions that employ information operations to supplement and support physical military operations. Non-state actors also utilize information warfare because of its low cost and low risk of loss to human life. There is currently no definitive legal framework in place to structure the meets and bounds of information warfare engagements. Complex legal questions arise and disappear within the blink of an eye as digital attacks travel through cyber space. Though this new mode of combat brings with it many nuanced tactical and legal considerations, it does not necessitate entirely new rules of engagement. Existing international laws, customs and norms addressing traditional modes of armed conflict are sufficient to guide information warfare practice. The international community has not formally embraced the application of existing law to information warfare, and until it does so, the digital battle space will remain a hi-tech free-for-all.

Over the last decade, the digital battle-space has become increasingly crowded as world superpowers; criminal organizations and terrorist groups develop offensive cyber capabilities. Networks are probed, data is stolen, military and civilian operations are compromised. The nature and extent of these actions varies as greatly as the groups perpetrating them. Some incidents are relatively benign episodes of experimentation, while others border on acts of war.

United States Defense Industry Infiltration

On July 14, 2011 the United States Department of Defense (DoD) publicly confirmed a

substantial breach of its digital security systems.[1] The DoD acknowledged that a digital assault in March of 2011 resulted in the theft of over 24,000 files from an unidentified defense contractor.[2] The content of the stolen files was not specifically revealed during the DoD's incident disclosure; but they did address defense intelligence thefts over the past few years, stating, "some of the stolen data is mundane, like the specifications for small parts of tanks, airplanes, and submarines. But a great deal of it concerns our most sensitive systems, including aircraft avionics, surveillance technologies, satellite communications systems, and network security protocols[.]"[3] "Foreign intruders" were blamed for the attack, but fingers were not pointed at a particular nation or group.[4] The intrusion represents the largest publicly acknowledged cyber attack on U.S. defense intelligence to date.[5]

Stuxnet & the Iranian Nuclear Program

In July 2010 a covert and complex cyber attack struck Iran's nuclear enrichment program.[6] The attack, referred to as "Stuxnet," was a worm that monitored and subverted the operations of Iran's nuclear development facilities. Stuxnet was the first publicly known attack to

---

[1] *See* William J. Lynn, U.S. Deputy Secretary of Defense, *Remarks on the Department of Defense Cyber Strategy,* U.S. DEPT. OF DEFENSE (Jul. 14, 2011), http://www.defense.gov/speeches/speech.aspx?speechid=1593) [hereinafter Lynn's Remarks].

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] William Broad J., John Markoff, David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay,* NEW YORK TIMES (Jan. 15 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all [hereinafter Broad].

not only spy on industrial facilities, but to also subvert control of their operations.[7]

The worm effected industrial machinery control computers used in Iranian uranium enrichment facilities.[8] These computers utilized Siemens software control packages to instruct centrifuge machinery to "'turn on and off motors, monitor temperature, [and] turn coolers on[.]'"[9] Once the worm infected an enrichment facility computer, Stuxnet would monitor and record files of normal plant activity.[10] These recordings were displayed to plant operators to create the illusion that machinery was operating normally.[11] At the same time, Stuxnet subverted instructions causing centrifuges to spin out of control.[12] The worm was programmed to propagate slowly, making it hard to diagnose infection because only a few computers were infected at any given time.[13] The difficulty of detection allowed Stuxnet to continue causing centrifuge malfunctions without the notice of plant operators.

Its likely target being Iranian nuclear facilities, the Stuxnet worm compromised five Iranian industrial processing organizations, including the Natanz nuclear research facility.[14] Iran

---

[7] Jonathan Fildes, *Stuxnet Virus Targets and Spread Revealed,* BBC NEWS (Feb. 17 2011), http://www.bbc.co.uk/news/technology-12465688 [hereinafter Fildes].

[8] *Id.*

[9] *See Stuxnet Worm Hits Iran Nuclear Plant Staff Computers,* BBC NEWS (Sep. 26, 2010), http://www.bbc.co.uk/news/world-middle-east-11414483 [hereinafter *Stuxnet Worm Hits Iran*]; *see also,* Fildes, *supra* note 7.

[10] *See* Broad, *supra* note 6.

[11] *Id.*

[12] *See* Broad, *supra* note 6.

[13] *See,* Fildes, *supra* note 7.

[14] *Id.*

initially denied that the attack had any impact, but later acknowledged that its uranium enrichment programs were disrupted.[15] There was much speculation that the attack was a joint effort between the United States and Israel.[16] Though these speculations were not publicly confirmed, Iran reacted with verbal hostility towards the suspected culprits.[17]

Estonia

In late April of 2007, Estonia was hit by the first of several waves of cyber attacks targeting Estonian infrastructure.[18] The attacks began on April 26th during a period of political upheaval prompted by the removal of a bronze soldier statue commemorating Russian military victory, from the center of the Estonian capital of Tallinn.[19] Cyber assaults on Estonian media, banking, and government services continued until shortly after May 9th, the Russian holiday celebrating victory over Nazi Germany.[20] After the digital dust settled, the list of affected targets

---

[15] John Markoff, *A Silent Attack, but not a Subtle One,* NEW YORK TIMES NEWS, (Sep. 26 2010), https://www.nytimes.com/2010/09/27/technology/27virus.html.

[16] Broad, *supra* note 6.

[17] Director of Information Technology Council at the Iranian Ministry of Industries and Mines, Mahmud Liaii, said: "An electronic war has been launched against Iran." Peter Beaumont, *Iran 'Detains Western Spies' After Cyber Attack on Nuclear Plant,* The Guardian, (October 2, 2010) *http://www.theguardian.com/*

world/2010/oct/02/iran-western-spies-cyber-attack .

[18] *See* Ian Tavnor, *Russia Accused of Unleashed Cyberwar to Disable Estonia,* The Guardian, (May 17, 2007) http://www.guardian.co.uk/world/2007/may/17/ topstories3.russia [hereinafter Tavnor]; *see also,* Mark Landler, John Markoff, *Digital Fears Emerge After Data Siege in Estonia,* N.Y. TIMES (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted= all [hereinafter Landler].

[19] *See supra* note 18.

[20] *See id.*

included the websites, network resources, and e-mail servers of the Estonian Parliament, the Reform Party, the Prime Minister, a number of newspapers, and the largest bank in Estonia.[21]

The attackers utilized a large network of hijacked computers, called a botnet, to assault Estonian websites and networks with a large-scale, distributed denial-of-service attack.[22] This type of attack transmits a large volume of data at a victim computer system to overwhelm its resources and degrade its ability to operate normally.[23] This is analogous to opening a dam to destroy a town downriver by flood. If enough water is released, then the town may be unable to muster the resources to defend against the aquatic assault. By instructing the botnet to send large volumes of data at Estonian networks, the attackers were able to rally enough bandwidth resources to overcome the network resources of the defending country.[24] The technique was ultimately successful and forced several sectors of Estonian government and economy offline.[25]

Media perception focused on the Russian Government as the likely culprit.[26] Kremlin

---

[21] Landler, *supra* note 18.

[22] *E.g.* , *War in the Fifth Domain. Are the Mouse and Keyboard the New Weapons of Conflict?*, THE ECONOMIST (Jul. 1 2010), http://www.economist.com/node/16478792l [hereinafter War in the Fifth Domain]; Tavnor, *supra* note 18; John Schwartz, *When Computers Attack* N.Y. TIMES (Jun. 24, 2007), http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html?pagewanted=all; Landler, *supra* note 18.

[23] Taynor, *supra*, note18.

[24] *See* Tavnor, *supra* note 18.

[25] *War in the Fifth Domain*, *supra* note 22.

[26] *See*, *e.g.*, Traynor, *supra* note 18; *War in the Fifth Domain*, *supra* note 22; Landler, *supra* note 18; *Cyberwarefare: Newly Nasty*, THE ECONOMIST (May 24, 2007), http://www.economist.com/node/9228757 [hereinafter *Newly Nasty*]; Steven Lee Myers, *'E-stonia' Accuses Russia of Computer Attacks*, N.Y. TIMES (May 18, 2007), *available at* http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html.

spokesman Dmitry Peskov ardently denied such allegations as being 'completely untrue."[27] Though the IP addresses of some attackers pointed to Russian involvement, NATO investigators did not report a conclusive link between the attacks and the Russian government.[28] A number of groups and individuals claimed responsibility including "hacktivists" (aggressive cyber activists), individual students of Russian background, the Kremlin backed youth group NAASHI (young democratic anti-fascist party), and even a Russian political party representative who jokingly claimed that his assistant had carried out the assault.[29] Some experts dismissed these claims due to the scale and complexity of the attacks, positing that it was highly improbable that such actions could be carried out without assistance from the Russian government.[30] Without publicly resolving these issues, NATO offered assistance to Estonia and in 2009 established a cyber warfare center in Tallinn to provide a base for response to future attacks in Europe.[31]

The Georgian Conflict

A year after cyber attacks assailed Estonian infrastructure, the country of Georgia became the target of a similar digital assault. In July 2008, a targeted DDOS attack was executed against the website of the Georgian president Mikhail Saakashvili.[32] The attack commenced a month

[27] *Estonia fines man for 'cyber war'*, BBC NEWS (Jan. 2852008), *available at* http://news.bbc.co.uk/2/hi/technology/7208511.stm [hereinafter Estonia Fines].

[28] *See id.; see also* Taynor, *supra* note 18.

[29] *See* Taynor, *supra* note 18; *see also, Estonia has no Evidence of Kremlin Involvement in CyberAttacks*, RIA NOVOSTi, (Sep. 6, 2007), *available at* http://en.rian.ru/world/20070906/76959190.html.

[30] Landler, *supra* note 18; Estonia Fines, *supra* note 27.

[31] *See* Newly Tasty, *supra* note 26.

[32] *See* Siobhan Gorman, *Hackers Stole IDs for Attacks*, WALL ST. JOURNAL (Aug. 17, 2009), *available at* http://online.wsj.com/article/SB125046431841935299.html; *see also* John Markoff,

prior to the Russian invasion of Georgia's Abkhazia and South Ossetia regions.[33] As the five-day Russia-Georgia conflict unfolded, a larger wave of cyber attacks hit Georgia.[34] Government and media websites were shut down, telephone and emergency services were crippled, and the web-based services of the largest bank in Georgia were disabled.[35] The resulting loss of communication capabilities impeded Georgia's ability to inform the outside world about the mounting casualties of the Russian conflict.[36]

Blame for the attacks was once again placed on the Russian government, but the obfuscated trail left by the attackers resulted in a lack of definite culpability. The bulk of the data traffic, much of which bore the pro-Russian message "win+love+in+Russa" was controlled and routed through a set of servers in the United States.[37] Combined with the timing of the cyber attacks, which closely coincided with Russian military movements into and around Georgia, these facts lead some analysts to suspect that the Kremlin was responsible.[38] Yevgeniy Khorishko, a spokesman for the Russian embassy in Washington, D.C. denied any involvement

---

Before the Gunfire, Cyberattacks, N.Y. TIMES (Aug. 12, 2008), *available at* http://www.nytimes.com/2008/08/13/technology/13cyber.html; *War in the Fifth Domain*, *supra* note 22.

http://online.wsj.com/article/SB125046431841935299.htmlhttp://www.nytimes.com/2008/08/13/technology/13cyber.html

[33] *See supra*, note 32.

[34] *See* Gorman, *supra* note 32.

[35] *Id.*

[36] *See id.*; *see also Marching off to Cyberwar*, THE ECONOMIST (Dec. 4, 2008), *available at* http:www.economist.com/node/12673385; *War in the Fifth Domain*, *supra* note 22.

[37] Tavnor, *supra* note 18.

[38] Markoff, *supra* note 32.

by the Russian government, stating, "Russian officials and the Russian military had nothing to do with the cyber attacks on the Georgian Web [.]"[39] Suspicion was later diverted from the Kremlin to the Russian Business Network (RBN), an organized crime ring known for taking part in cyber crime.[40] The RBN owned ten of the websites used to perform the attacks on Georgia, which were purchased using credit cards and identities stolen from Americans.[41] Though, American resources were used in the attack against Georgia, American servers were used to save the Georgian government's data.[42] A private company in the United States offered to host the Georgian government websites and provide data backup during the conflict.[43] Thus, Georgia was assailed by non-state actors from Russia and protected by non-state actors from the United States.

These scenarios provide chilling examples of how computers may be used to cause instability in various sectors of a country's infrastructure. One can easily imagine far more disastrous effects waiting on the horizon if appropriate deterrent measures are not developed. What legal framework should be applied in guiding the development of such measures?

Amidst the flurry of publications on information warfare printed in law reviews across

---

[39] *Id.*; see War in the Fifth Domain, supra note 22.

[40] *See* Gorman, *supra* note 32*; see also* War in the Fifth Domain, *supra* note 22; Markoff, *supra* note 32.

[41] *See* Gorman, *supra* note 32.

[42] Brandon Griggs, *U.S. at Risk of Cyberattacks, Experts Say*, CNN, Aug. 18, 2008, http://articles.cnn.com/2008-08-18/tech/cyber.warfare_1_hackers-internet-assault-web-sites?_s=PM:TECH; Peter Svensson, *Russian Hackers Continue Attacks on Georgian Sites*, AP NEWS, Aug. 12, 2008, http://www.usatoday .com/tech/products/2008-08-12-2416394828_x.htm.

[43] Svensson, *supra* note 42.

the United States, the topics of "general culpability" and "redefining warfare" are abundant; however, there is scant material addressing some of the less obvious problems presented by cyber conflicts. Should responsibility and liability change depending on whether the perpetrator is an individual, a company or a government entity? Is it legally and morally permissible to assign at least a portion of the blame for an information warfare attack to nations who were unaware of their participation? What if assigning such blame results in the nation's forced entry into an international armed conflict? These questions present legal issues for which there is little guiding precedent and a woefully incomplete framework for application. We are thus required to pursue applications of aging legal frameworks to modern dilemmas. To this end, I will examine a narrow set of legal issues posed by the onset of information warfare, and attempt to determine if the present legal framework can be equitably applied to the situations arising within that narrow set of questions.

In this paper I will examine the impact of information warfare operations on neutral states; those that have adopted a position of non-involvement with respect to international armed conflicts. While the law concerning the behavioral interaction between neutral and warring states is well established in physical settings, the application of this law to the digital battlefield is a complicated issue. What rights and duties does a neutral state have under current international neutrality law when information warfare is the modality of aggression? The following sections of this paper examine and analyze this difficult question. Section I discusses the fundamentals of the Law of Armed Conflict. Section II examines the framework of the principle of neutrality and addresses pertinent aspects of the Law of Armed Conflict. Specifically, it focuses on the Hague Conventions on neutrality as the basis for current neutrality law and the rights and duties of a neutral state. Section III assesses the definition of information warfare as it applies to the

determination of what actions may or may not be encompassed by international neutrality law. Lastly, Section IV analyzes the question of whether current international neutrality law can be reasonably applied to impose rights and duties on a neutral state in an information warfare setting.

1. The Law of Armed Conflict

The Law of Armed Conflict (LoAC) is a set of international rules and regulations that provide authorization for the military personnel of parties to an international armed conflict to engage in attacks on lawful military targets.[44] These rules and customs suggest specific behaviors that if adhered to, will limit the destructive toll exacted by international conflicts.[45] They apply equivalently to all parties to an international conflict. The LoAC comprises a multitude of treaties, conventions and international customs, but the primary sources are the Hague Convention of 1899, Hague Convention of 1907, Hague Rules of Aerial Warfare, the Geneva Conventions, and the Geneva Convention Protocols.[46] There are seven general principles established by the LoAC: 1) distinction (the differentiation of combatants from non-combatants); 2) military necessity (all enemy military personnel are automatically presumed to be hostile); 3) proportionality (military advantage to be gained by an attack must be greater than the resulting

---

[44] *See* DEP'T OF DEF. OFFICE OF GEN. COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (1999), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADB257057[hereinafter Assessment of International Legal Issues].

[45] *See id*.; *see also* David L. Wilson, *An Army View of Neutrality in Space: Legal Options for Space Negation*, 50 A.F. L. REV. 175, 192-193 (2001).

[46] These sources are particularly significant due to the number of signatories and breadth of issues addressed therein. Subsequent treaties have expanded on the concepts set forth in the Hague and Geneva Conventions, but are largely specific to particular conflicts and/or signatories, making those treaties less relevant to the international community as a whole. *See generally* Assessment of International Legal Issues, *supra* note 44.

collateral damage); 4) superfluous injury (specific weapons that cause superfluous injury are disallowed); 5) indiscriminate injury (weapons causing indiscriminate damage, such as biological weapons, are disallowed); 6) perfidy (certain persons and property are immune from attack and are designated by visually recognizable symbols); and 7) neutrality (nations wishing to remain uninvolved in a conflict may declare themselves neutral).[47] In this paper I focus on the principle of neutrality and examine how this element of the LoAC can be applied to information warfare.[48]

2. The Principle of Neutrality

The principle of neutrality is established through a set of rules and customs that provide guidelines for interaction between parties to an international armed conflict. The 1899 Hague Convention, 1907 Hague Convention and 1923 Hague Rules regarding Aerial Warfare (hereinafter jointly referred to as "the Hague Conventions") established a framework for acceptable means of interaction between neutrals and belligerents. Subsequent agreements and treaties, such as the United Nations Charter, further addressed the proscribed interactions of neutrals and belligerents; however, these sources are not within the scope of this paper.[49] As the

[47] *See* INTERNATIONAL COMMITTEE OF THE RED CROSS [ICRC], *Basic Rules of the Geneva Convention and their Additional Protocols,* Doc. Ref. 0365(1988) *available at*: http://www.icrc.org/eng/resources/documents/publication/p0365.html; *see also,* Assessment of International Legal Issues, *supra* note 44.

[48] More information on the application of other principles of the LoAC to information warfare is available through several excellent articles in the 64th Edition of the Air Force Law Review ("Cyber Edition"). *E.g., see generally* Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121 (2009) [hereinafter Schaap]; Lieutenant Joshua E. Kastenberg, *Non-intervention and Neutrality in Cyber Space: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43 (2009).

[49] While the Hague Convention and Laws of Armed Conflict are the primary sources of neutrality law, the United Nations also levies obligations on neutral states. Pursuant to the United Nations Charter, Article 51, member states may not commence the "use of force"

primary source for the principle of neutrality, the Hague Conventions are critical to understanding a neutral's obligations and immunities with respect to an international conflict. In this section, I discuss the background of the Hague Conventions, describe the privileges afforded to neutral states, and then categorize several articles of the Conventions that are potentially applicable to information warfare scenarios. These articles belong either to a duty to remain impartial, a duty to intervene, or a duty to repel. Lastly, I address a belligerent's right of necessity with respect to the duties and obligations associated with neutrality law.

A. The Hague Convention

The 1899 and 1907 Hague Conventions and subsequent Rules of Aerial Warfare established a behavioral mechanism for a state to maintain its rights as a neutral in exchange for

---

without authorization from the U.N. Security Council. U.N. CHARTER art. 39. Unauthorized use of force is only allowed when a member nation is attacked and lacks adequate time to consult the Security Council before defensive measures are taken. U.N. CHARTER art. 51. This provision is consistent with the right of necessity provided by the LoAC. The difference between the right of necessity and Article 51 of the U.N. Charter is the U.N. Security Council's ability to call upon member nations to assist in keeping the peace by peaceful means or by use of force. U.N. CHARTER arts. 41-2. Member nations are required to provide armed forces, facilities and rights of passage that the Security Council deems necessary for the maintenance of international peace. U.N. CHARTER art. 43. Thus, a neutral state belonging to the United Nations might be called upon to furnish troops or allow the troops of other nations to pass through its territory in order to bring resolution to an international armed conflict. Resources such as telecommunications facilities or satellite access can also be commandeered for U.N. peacekeeping missions. *See generally* Richard A. Morgan, *Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and Peaceful Purposes*, 60 J. AIR L. & COMM. 237, 239 (1994). Though these acts by a neutral would otherwise violate their duties under the LoAC, neutrals do not violate the principle of neutrality when they uphold their U.N. member obligations. *Id.* This is because Article 49 of the U.N. charter requires member states to cooperate with Security Council decisions, effectively absolving the neutral of fault for providing aid to peacekeeping forces. U.N. CHARTER art. 49; *see* Assessment of International Legal Issues, *supra* note 44. As a practical matter, belligerents opposing U.N. troops will likely see all neutrals participating in the mission as aligned with opposing belligerents, even if no such legal conclusion exists. Should the neutral choose not to obey the U.N. Security Council request, the neutral will suffer reproach and international relations deterioration. Neutrals would be wise to observe their duties and obligations under the LoAC and assist the U.N. as necessary, without fear of destroying their neutrality.

meeting certain obligations. The Hague Conventions were among the first international treaties to formally state the laws of war. The first convention, adopted at an international peace conference in 1899, focused primarily on structure of international arbitration, the basic laws of armed conflicts, and prohibitions on use of certain ultra-hazardous technologies such as: chemical warfare, hollow point bullets, and explosives dropped from air balloons.[50] In 1907, the peace conference met again to expand upon the principles outlined in the first Hague Convention and address emerging trends in the technology of war. Areas of major focus included large-scale naval warfare and the obligations on land and sea of neutral powers.[51] Changing trends in the modality of warfare were addressed once again at a 1923 peace conference where the Hague Rules of Aerial Warfare were drafted, further extending the rights and duties of a neutral power to cover aerial combat.[52] These rules were never officially codified as part of the Hague Convention; however, most of the international community has adopted them as custom.[53]

---

[50] *See* Convention Respecting the Pacific Settlement of International Disputes, July 29, 1899, 32 Stat. 1799; Convention with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803; Convention Respecting the Adaptation to Maritime Warfare of Principles of Geneva Convention of 1864, July 29, 1899, 32 Stat. 1827; Convention Respecting the Prohibiting Launching of Projectiles and Explosives from Balloons, July 29, 1899, 32 Stat. 1839.

[51] *See* Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V), Oct. 18, 1907, 36 Stat. 2310[hereinafter Hague Convention V]; Convention Rights and Duties of Neutral Powers in Naval War(Hague XIII), Oct. 18, 1907, 6 Stat. 2415[hereinafter Hague Convention XIII].

[52] Hague Rules of Aerial Warfare, art. 40-2, Feb. 19, 1923, 32 AM. J. INT'L L. Supp. 12 (1938) (not in force) [hereinafter Hague Air Rules].

[53] George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1135 (2000) [hereinafter Walker].

B. Privileges Afforded to Neutrals

When a state formally declines to align with any party to an international conflict, the state becomes a "neutral" and gains privileges as outlined in the Hague Convention. Signatories to the Hague Conventions agree to abide by rules governing treatment of neutral states, and afford all due privileges to those states. The primary benefit of neutrality is inviolability of territory. Once a declaration of neutrality is made, it is a violation of the Hague Convention for belligerent agents to trespass on the neutral's territory.[54] This prohibition effectively removes the territory of the neutral state from the list of potential battlefields, thereby reducing the likelihood of damage to the territory during the conflict. Neutral states are allowed to maintain trade relations and formal communications with all belligerents. For non-neutral states, these acts could draw a state into the conflict and align the state with a belligerent power in the eyes of the international community.[55] Thus, neutral states are at least partially insulated from the economic distress and opportunity costs of breakdowns in communication resulting from participation in international armed conflicts.

C. Duties and Obligations

In exchange for the aforementioned privileges, a neutral state has a duty to perform or refrain from performing certain actions.[56] A neutral's failure to meet its duties and obligations can put its neutral status at risk. The Hague Conventions set forth scenarios in which a neutral

---

[54] Hague Convention V, *supra* note 51 at art. 1-5.

[55] *See* Hague Convention V, *supra* note 51 at art. 7-8; *see also* STEPHEN C. NEFF, THE RIGHTS AND DUTIES OF NEUTRALS, 1 (2000).

[56] *See generally* Hague Convention V, *supra* note 51; Hague Convention XIII, *supra* note 51; Hague Air Rules, *supra* note 52.

may act, not act, or act in response to the actions of a belligerent. A neutral is obligated to respond in the proscribed manner, though the manner of fulfilling the duty in question is generally left to the discretion of the neutral state. The type of duty imposed on the neutral state varies according to the modality of the conflict. For instance, a neutral must not allow a belligerent to move troops, munitions, or aircrafts over the neutral's land; however, a belligerent warship that is merely passing through a neutral's waters will not trigger any responsibility on the part of the neutral power.[57] Many of these duties and obligations may be classified as: a duty of impartiality, a duty to intervene, or a duty to repel**.**

i. *Duty to Remain Impartial*

Neutral nations must interact impartially with the belligerent states on all sides of an international conflict.[58] If a neutral provides the use of its services and resources to any belligerent state, then the neutral must make the same services or resources available to all belligerent states. A neutral power that allows belligerent owned vessels, whether military or civilian, to make use of the neutral's ports may not give preference to either belligerent.[59]

Generally, private companies within a neutral state are not subject to the same resource allocation restrictions as the state's government. A neutral state that maintains relations with warring nations may not show preference to one belligerent over another with regard to available resources.[60] Conversely, material resources sold by a private company can be sold to any party.[61]

---

[57] Hague Convention V, *supra* note 51 at art. 1; Hague Convention XIII, *supra* note 51 at art. 30; Hague Air Rules, *supra* note 52 at art. 35.

[58] *See* Major David L. Wilson, *An Army View of Neutrality in Space: Legal Options for Space Negation,* 50 A.F. L. REV. 175, 192 (2001).

[59] Hague Convention XIII, *supra* note 51 at art. 9.

[60] *See* Hague Convention XIII, *supra* note 51 at art. 19, 21; *see also,* Hague Convention V, *supra* note 51 at art. 4,7-8.

Thus, private companies may continue to sell and export goods to any and all belligerents.[62] This includes munitions, supplies of war and even aircraft.[63]

An exception to the freedom of a neutral state's private companies to contract with belligerent states focuses on access to communications services. Communications resources must also be offered or denied equally to all belligerents. Neutral states must insure that private companies providing telegraphy services do not offer services or resources to one party that are not available to all.[64] Belligerent forces and companies may not erect telegraphy towers on neutral territory unless the resulting telegraphy services are publicly available.[65] The precise meaning of "telegraphy services" is not legally well defined.[66] For the purposes of this paper, telegraphy is defined as "the practice of using or constructing communications systems for the transmission or reproduction of information."[67]

---

[61] Hague Convention V, *supra* note 51 at art. 9.

[62] *Id.* at art. 7.

[63] Hague Air Rules, *supra* note 52 at art. 45.

[64] Hague Convention V, *supra* note 51 at art. 8-9.

[65] *Id.* at Art, 3.

[66] Though not technically "telegraphy," erecting of website hosting facilities on neutral territory during the Georgian conflict was seen as a violation of the principle of neutrality. l Lieutenant Joshua E. Kastenberg, *Non-intervention and Neutrality in Cyber Space: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43 (2009). *See* Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV 1427, 1428 (2008) (citing Newly Nasty, THE ECONOMIST, May 26, 2007, at 63).

[67] A Google search of the terms "definition telegraphy" yields the definition: The "science or practice of using or constructing communications systems for the transmission or reproduction of information." http://www.google.com.

The term "telegraphy" may encompass more than the telephone line based communications available at the time the Hague Convention was drafted. The United States Department of Defense has stated that the plain language of articles eight and nine of the Hague Convention justifies an extension of these constraints to satellite communications as well as ground based communication relays.[68] It is not yet settled whether the language of the articles can be interpreted to extend to systems that generate communications such as global positioning systems, weather analysis satellites, or signal intelligence systems.[69] The emergence of the Internet as a viaduct for weapons of digital warfare further complicates the question because the Internet possesses both communication relay and data generation properties. Though the Hague Convention details specific instances in which a country may not show preference to any side of a conflict, the modern trend points to the conclusion that the duty of impartiality may extend to situations beyond the instances described in the Hague articles.[70]

ii. *Duty to Intervene*

Neutral states must act to prevent belligerent forces found within neutral territory from leaving in a battle-ready condition.[71] Neutrals are thus obliged to prevent belligerent action from originating within neutral territory. The means a neutral can employ to prevent belligerents from quitting neutral territory varies according to the potential harm presented. Once the belligerents are in custody, the method and duration of detention is determined by the neutral state. The potential for internment of troops and supplies diminishes the appeal to belligerents of

[68] Assessment of International Legal Issues, *supra* note 44.

[69] *Id.*

[70] Hague Convention V, *supra* note 51 at art. 8-9.

[71] Hague Convention V, *supra* note 51 at art. 11-15.

trespassing on neutral territory by reducing the likelihood of gaining an exploitable strategic advantage.

The Hague Conventions provide neutral states a good deal of latitude in determining the extent of intervention appropriate in a given scenario, but intervention measures are mandatory.[72] In the simplest case, belligerent forces, vessels, and craft are rescued by agents of a neutral state and brought within the jurisdiction of that neutral power. Rescue scenarios present only marginal belligerent malfeasance and thus the belligerent vessel or craft, and its crew must be interned in a manner determined by the neutral, but the neutral need not take further action.[73]

On the other hand, trespassing belligerents who refuse to comply with the neutral state's orders to leave may be deprived of their means of escape. A belligerent warship or aircraft that enters the territory of the neutral state will be asked to leave. If the belligerents refuse to quit the territory the neutrals must act decisively.[74] Presumably due to the belligerents' greater level of culpability for their predicament; the neutral state may utilize what measures it deems necessary to prevent warships from being sea-worthy, or the means at its disposal to ground aircraft refusing to leave neutral territory.[75] Both events require internment of the craft's crew.[76] Any

[72] *e.g.*, Hague Convention XIII, *supra* note 51 at art. 24; Hague Air Rules, *supra* note 52 at art. 46.

[73] Hague Convention XIII, *supra* note 51 at Art. 3; Hague Air Rules, *supra* note 521 at art. 43.

[74] Hague Convention XIII, *supra* note 51 at arts. 21 & 24; Hague Air Rules, *supra* note 52 at art. 42.

[75] *Id.*

[76] *Id.*

belligerent ground forces found trespassing in a neutral's territory must be interned as far from the theater of war as possible.[77]

The most interesting case arises when the neutral state knows an aircraft within its jurisdiction is outfitted for the purposes of offensive operations or intelligence gathering, and reasonably believes such operations are targeted at opposing belligerents. Under these circumstances a neutral power is instructed to use the means at its disposal to prevent the aircraft from leaving the neutral's territory.[78] It must also take action to prevent the crew from doing any work on the aircraft, or from departing the neutral territory.[79] Additionally, a neutral must use means at its disposal to prevent aircraft in the neutral's airspace or waterways from collecting surveillance of enemy forces.[80] These articles do not stipulate that the means of prevention are limited to internment.[81] Consequently, a neutral state may act forcefully to prevent the departure of the aircraft and its crew, without jeopardizing the state's neutral status.

The duty to intervene creates an active intermediary role for neutral states and imposes a policy of "non-origination". Belligerent vessels, aircraft and forces must be interned if there is any suspicion that they have been or intend to be involved in hostile actions.[82] If there is reason to believe that belligerents in neutral territory intend to engage in hostilities with opposing

---

[77] Hague Convention V, *supra* note 51 at art. 11.

[78] Hague Air Rules, *supra* note 52 at art. 46.

[79] *Id.*

[80] Hague Air Rules, *supra* note 52 at art. 47.

[81] *Id.*

[82] Hague Convention XIII, *supra* note 51, at Art. 3, 24; Hague Air Rules, *supra* note 52 at art. 42- 43.

belligerents, then the neutral state must take whatever action it can to prevent those hostilities.[83] An active role in preventing hostile operations from originating in its territory reinforces the neutral's refusal to be politically aligned with any belligerent. Thus a neutral state may not simply turn a blind eye to the actions of belligerent states, but must actively prevent potential acts of war from originating within the neutral state's jurisdiction.

iii. *Duty to Repel Belligerent Forces*

Neutral states have an affirmative duty to repel belligerent incursions into neutral territory.[84] Denying the use of transportation infrastructure as a conduit for warfare is essential to maintaining neutral status. By attempting to prohibit belligerent forces from moving through neutral territory, a neutral state effectively asserts that its modes of transportation are not a means for facilitating hostile activities against opposing belligerents. The extent of the action necessary to satisfy this duty depends on whether the mode of incursion is by land, sea, or air. While the level of deterrent measures required by a neutral state varies according to the situation, every neutral state has a duty to try to stop belligerents from violating the neutral's territory.

Conflicts on land present the simplest scenario for repelling invading forces. Internationally accepted borders of each state are well documented, making it simple for belligerents and neutrals to determine whether or not a movement constitutes trespass. Additionally, most countries have the resources to launch minimal deterrent measures against invaders. Due to the relative ease of putting up token resistance, the Hague Conventions' prohibition against belligerent incursions into neutral territory does not impose a complex burden

[83] Hague Air Rules, *supra* note 52 at art. 46.

[84] Hague Convention V, *supra* note 51 at art 1-3.

on most neutral states.

The situation becomes less clear when combatant incursions take place at sea or in the air. Water and air are fluid media without definite delineated boundaries, making it difficult for neutral states and belligerents alike to distinguish the territory to avoid. Not all countries have the technological capability of detecting trespass over such nondescript boundaries. Even those nations that can adequately monitor their air and sea borders do not necessarily have a standing navy or air force capable of intervening in belligerent actions. These resource discrepancies amongst nations create a dilemma with respect to enforcement: how can the international community reasonably expect a poor or small country with minimal maritime resources to repel an invasion it couldn't even detect? The drafters of the Hague articles were presumably sympathetic to these concerns and decided that the duty to repel aircraft and vessels should be proportional to the resources of the neutral state.[85] Neutral states must utilize the "means at their disposal" to conduct surveillance and prevent belligerent states from entering neutral airspace or utilizing neutral waters for hostile activities.[86]

D. The Right of Necessity

[85] "A neutral Power is bound to exercise such surveillance as the means at its disposal allowing it to prevent any violation of the provisions of the above Articles occurring in its ports or roadsteads or in its waters." Hague Convention XIII, *supra* note 51 at art. 25."A neutral Government is bound to use the means at its disposal to prevent belligerent military aircraft from entering its jurisdiction and to compel them to land or to alight on water if they have penetrated therein." Hague Air Rules, *supra* note 52 at art. 42.

[86] *See* Hague Convention XIII, *supra* note 51 at Art. 25; *see also* Hague Air Rules, supra note 51 at Art. 42. *But see* Hague Convention XIII, *supra* note 51 at Art 10 stating that mere passage of a warship through neutral waters does not violate the neutral state's territory; consequently no action is required by the neutral state as long as the belligerent warship is just passing through. This discrepancy is likely due to the fact that alternative routes through airspace and on land are generally available to belligerent forces, while there may only be one passable water route for belligerents to travel on.

If a neutral state is unable or unwilling to repel or detain belligerent forces within its territory, opposing belligerent states have the right to intervene. Under a theory of "right of necessity," a belligerent state may take action in self-defense against an opposing belligerent state that has violated neutral territory.[87] This right is particularly pertinent to naval and air incursions in which a neutral nation with fewer resources may have met its duty by attempting to repel or detain the belligerent craft, but may have been unable to effectuate such measures successfully. In these circumstances, opposing belligerents may utilize the neutral's territory to defend their own interests.

E. Conclusion

The Hague Convention requires signatory neutral nations to intervene and prevent belligerents from operating within the neutral's territory, treat all belligerents impartially and equally, and repel belligerent forces trespassing on neutral territory. In a practical sense, this means neutrals must act to prevent a belligerent from utilizing the neutral's resources to commence hostilities against an opposing belligerent. Resources such as land, sea, air, telegraphy, and commercial goods are addressed in the Hague Convention, but data networks were not available when the Convention was drafted. In the following sections, this paper will explore the extension of the Hague Convention to include modern data communications networks and the tools of information warfare

3. What is Information Warfare?

The scope and nature of information warfare are amorphous and difficult to constrain to a single definition. There is no generally accepted definition concerning the coverage of the term

[87] *See* Walker, *supra* note 43.

"Information Warfare." Indeed there does not seem to even be an agreement as to what term should be used. The terms "cyber warfare," "information warfare," "cyber assault," "C4I," and "I-War" are used interchangeably.[88] U.S. attempts to describe information warfare focus on the intended result of the action. The U.S. Air Force uses the term network warfare operations" defined to mean "integrated planning and employment of military capabilities to achieve desired effects across the interconnected analog and digital portion of the battle space."[89] Another definition comes from a 2006 CRS report to Congress, which referred to cyber warfare as "operations to disrupt or destroy information resident in computers and computer networks.[90]

The DoD adopted a broader approach to defining information warfare. The DoD describes "information operations" as "he integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.."[91] This definition is overly broad because it encompasses standard operating procedures, electronic security, military intelligence acquisition, and other non-adversarial actions taken using military information systems. Definitional clarity is provided by the Department of Defense's recent separation of offensive cyber operations or "cyber attacks" into

---

[88] *See* Dr. Ivan K. Goldberg, *Glossary of Information Warfare Terms*, http://www.psycom.net/iwar.2.html (April 24, 2012).

[89] U.S. Dept. of Air Force Policy Dir.10-7, Information Operations, 19 (Sep. 6 2006) *available at* http://www.fas.org/irp/doddir/usaf/afpd10-7.pdf.

[90] CLAY WILSON, CONG. RES. SERVICE REP. FOR CONGRESS NO. RL31787, INFORMATION OPERATIONS AND CYBERWAR CAPABILITIES AND RELATED POLICY ISSUES 5 (Sep. 14, 2006), *available at* http://www.fas.org/irp/crs/RL31787.pdf.

[91] Joint Electronic Library, JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Though 15 October 2013) http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

the categories of exploitation, disruption, and destruction.[92] For the purposes of providing a simple, working definition, this paper will adopt the Department of Defense's definition of information operations as limited by the categorization of cyber attack.[93] The terms information warfare and cyber warfare will be used interchangeably. In this section, I will discuss armed conflict as contrasted with espionage and cyber crime, the types of information attacks, and which of these attacks fall within the scope of armed conflict.

A. Armed Conflict, Espionage or Criminal Activity?

It is sometimes difficult to determine if a cyber attack constitutes armed conflict, covert intelligence gathering, or merely cybercrime, because many of the same techniques and weapons are used to perpetrate each type of action. The LoAC applies to armed conflicts, briefly addresses

---

[92] *See* John D. Banusiewicz, *Lynn Outlines New Cybersecurity Effort,* U.S. Department of Defense (Jun. 16, 2011), http://www.defense.gov/news/newsarticle.aspx?id=64349.

[93] Independent authors have posited definitions that segregate offensive acts from rudimentary operations. The term "offensive ruinous information warfare" was used by Dorothy Denning to describe "organized deliberate military effort to totally destroy the military information capabilities, industrial and manufacturing information infrastructure, and information technology-based civilian and government economic activities of a target nation, region, or population. *See* Davis Brown, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179 (2006) [hereinafter Brown]] (*Quoting* Michael Erbschloe, INFORMATION WARFARE: HOW TO SURVIVE CYBER ATTACKS 125 (2001). Ivan Goldberg proposed the nuanced definition of "information warfare" as "the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries. Dr. Ivan K. Goldberg, *Glossary of Information Warfare Terms,* http://www.psycom.net/iwar.2.html. Eric Jensen described "computer network attacks," as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." *See* Brown (*Quoting* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* 38 STAN. J. INT'L. L. 208 (2002)). An important distinction is made in these definitions, which describes destructive acts rather than merely passive intrusion. Any operative definition of cyber warfare allows this distinction to necessarily be drawn.

espionage and does not apply to crime that does not rise to the level of war crime.[94] Therefore, the type of action commenced determines how the LoAC applies to parties involved in an information attack. Proper application of the LoAC to the digital battle space requires that participants are able to recognize the type of action in question. The following sections address what armed conflict, espionage, and crime look like in an information warfare setting.

i. *Armed Conflict*

The scope of armed conflict is reasonably extended to non-physical warfare through a results-based approach. The use of digital weapons to achieve military objectives does not comport with our traditional notions of "arms" as physical objects such as spears, guns, crossbows and tanks, making it difficult to conceptualize cyber attacks as armed conflict. This is not the first time that legal scholars and military lawyers have confronted the problem of the militarized use of non-physical weapons.[95] The advent of biological, chemical and electromagnetic pulse technologies also presented the question of whether or not a non-physical attack constitutes armed conflict. Enemy military personnel are presumed to be combatants, so attacks of any nature on military targets are, by default, conducted in the course of armed conflict.[96] But, a commonly held view is that armed conflict does not necessitate physical force. Non-physical attacks are conducted in the course of armed conflict if the resulting damage could

---

[94] *See* Brown, *supra* note 93, at 187-189.

[95] *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, OPINION PAPER: HOW IS THE TERM "ARMED CONFLICT" DEFINED IN INTERNATIONAL HUMANITARIAN LAW?, International Committee of the Red Cross (Mar. 2008), available at: http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf.

[96] *See* Hague Convention IV Respecting the Laws and Customs of War on Land, and its annex: Regulation Concerning the Laws and Customs of War on Land, arts. 1-3, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631 [hereinafter Hague Convention IV].

have been produced with guns and bombs.[97] This is a results-based classification of offensive actions, and is thus consistent with the DoD approach to defining information warfare attacks.[98]

Another classification proposes an extension of the results based approach and particularly focuses on the effects a non-physical attack has on the civilian population or otherwise protected persons or property.[99] The expanded approach broadens the scope of armed conflict to include actions that have effects on civilian populations as well as military personnel, such as destruction of emergency services dispatch computers, reprogramming of traffic patterns and forced stock market crashes.[100] Though some scholars protest the expansion of the definition of armed conflict into this area, arguing that adoption of such liberal interpretations presents a slippery slope, the LoAC seems intrinsically protective of civilian populations, making an civilian-effects based approach consistent with the goals of the LoAC.[101] The United States DoD recognizes this expanded approach and states that the deliberate acts of a belligerent, which "cause injury, death, damage, and destruction to the military forces, citizens, and property of the

---

[97] *See* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES, 362-63 (1963).; Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* 38 STAN. J. INT'L. L. 208 (2002) [hereinafter Jensen].

[98] "DoD is particularly concerned with three areas of potential adversarial activity: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems." U.S. DEPT. OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, (Jul. 2011) available at http://www.defense.gov/news/d20110714 cyber.pdf [hereinafter DoD Cyber Strategy].

[99] *See e.g.*, Michael N. Schmitt, *Wired Warfare: Computer Network Attack and the* Jus in Bello, 76 INT'L L. STUD. 187, 196-197 (2002) [hereinafter Schmitt].

[100] *Id.*

[101] *See* Daniel B. Silver, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter,* 76 INT'L. L. STUD. 73 (2002).

other belligerent . . . are likely to be judged by applying traditional law of war principles."[102] For the purposes of this paper, I adopt the extended definition of armed conflict used by the U.S. Department of Defense.

ii. *Espionage and Military Intelligence Operations*

International law and the LoAC do not prohibit intelligence gathering and espionage activities.[103] Intelligence gathering operations by means such as open disclosure, accessing public networks, signal processing, and satellite monitoring is internationally accepted as a necessary part of military operations.[104] Espionage, on the other hand, is the "covert collection of information about other nations," and is not limited to the use of internationally accepted methods of information acquisition.[105] Both approaches are encompassed in the Hague Convention, which states that "ruses of war and the employment of measures necessary for obtaining information about the enemy and the country" are acceptable during armed conflict.[106] International law and the LoAC have not yet addressed the legality of espionage operations during peacetime.

The difference between intelligence gathering and espionage hinges on the status of the actor. A spy is one who, "acting clandestinely or on false pretenses . . . obtains or endeavors to obtain information in the zone of operations of a belligerent, with the intention of

---

[102] *See* Assessment of International Legal Issues, *supra* note 44, at 6.

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] Hague Convention IV, *supra* note 96, at art. 24

communicating it to the hostile party."[107] But uniformed military personnel engaging in intelligence gathering in enemy territory do not commit espionage because they do not act clandestinely.[108] Many nations have domestic laws that permit the punishment and/or execution of captured spies. Conversely, the Hague Convention prohibits the execution of military personnel captured while gathering intelligence.[109] It is therefore imperative that there is a clear definitional difference between persons committing digital espionage versus military intelligence gathering.

Rules regarding the perpetration of espionage have limited application to information warfare scenarios. This is largely due to the requirements that the perpetrator acts clandestinely and within enemy territory. Primary advantages of information attacks are the range at which they can be commenced and the anonymity they provide. It would be rare for an attacker to be physically located within enemy territory and acting under subterfuge. Aside from the limited situation where an enemy operative, disguised as a worker, steals files off a computer in enemy territory, it is unlikely that digital intelligence gathering will commence behind enemy lines. Furthermore, information acquisition performed by uniformed military personnel cannot be construed as espionage; thus, an operation performed by such personnel that does not "influence, disrupt, corrupt, or usurp" a nation's decision-making is not accurately described as either espionage or an information attack. Operations of this nature are best construed as military intelligence gathering.

---

[107] Hague Convention IV, *supra* note 96, at art. 29.

[108] *See* Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, art. 52, para. 2, 1125 U.N.T.S. 3.

[109] *See* Hague Convention IV, *supra* note 100, at arts. 30-31.

iii. *Criminal Activity*

Information attacks perpetrated by civilian actors are cyber crimes and do not fall within the purview of the LoAC. The national laws of each country address the scope of cyber crime and the punishments associated therewith. International efforts between the United States and Europe suggested norms and regulations for normalizing how cyber crime is addressed in individual countries but these suggestions have not been formally adopted in many nations.[110] The types of actions that constitute cyber crime vary greatly across the international community. In the United States, citizens are entitled to unfettered access to Internet websites but engaging in unauthorized access to networks is a crime.[111] By contrast, Chinese citizens must access the Internet through elaborate content filtering systems and accessing unapproved websites is a crime.[112] The commission of a cyber attack by an individual or group of individuals in one nation against a target in an enemy country will likely be construed as cyber crime. It is conceivable that such attacks could rise to the level of war crimes by causing widespread damage or death. In

[110] "In the case of criminals and other non-state actors who would threaten our national and economic security, domestic deterrence requires all states have processes that permit them to investigate, apprehend, and prosecute those who intrude or disrupt networks at home or abroad Internationally, law enforcement organizations must work in concert with one another whenever possible to freeze perishable data vital to ongoing investigations, to work with legislatures and justice ministries to harmonize their approaches, and to promote due process and the rule of law[.]" BARACK OBAMA, PRES. OF THE U.S., INTERNATIONAL POLICY FOR CYBERSPACE: PROSPERITY, SECURITY AND OPENNESS IN A NETWORKED WORLD, 13 (May 2011) available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter White House Cyberspace Policy]; *see also* Council of Europe, Convention on Cybercrime, arts. 2-6, Nov. 23, 2001, E.T.S. No. 18.

[111] Computer Fraud and Abuse Act, 18 USC § 1030 (a)(2)-(3) (1996) (last amended 2004).

[112] S*ee* Congressional - Executive Commission of China, I*nternational Agreements and Domestic Legislation Affecting Freedom of Expression*, Congressional - Executive Commission of China Virtual Academy (Apr. 5, 2006); *contra* Jack L. Qiu, *Virtual Censorship in China: Keeping the Gate Between the Cyberspaces*. INT'L. J. COMM. L. & POL., 4.(Winter 1999).

such cases the LoAC would apply and the civilian actor tried by military tribunal instead of by domestic courts.

iv. Is Information Warfare Armed Conflict?

Whether information warfare constitutes armed conflict is a threshold question for determining the applicability of the LoAC to various information attack scenarios. Only attacks committed in the course of armed conflict are subject to the rules, regulations and norms embodied in the LoAC.[113] As discussed above, attacks that "cause injury, death, damage, and destruction to the military forces, citizens, and property of a belligerent" are committed in the course of armed conflict.[114] Some information attacks are easily described as armed conflict, while others are better classified as espionage, intelligence gathering, or cyber crime.

B. Types of Information Warfare

Traditional attacks based on physical force are often described according to their origin and/or associated weaponry (i.e. a U.S. Air strike on Afghanistan), because these factors are descriptive and easily determinable. This approach is problematic in information warfare because conventional weapons such as guns and bombs are replaced with computers and data streams, and the attackers are often unknown.[115] Due to the complexity of modern cyber attacks, it is easiest to characterize types of cyber attacks according to the result of the attack. This section discusses the results-oriented approach employed by the U.S. DoD for categorizing types of information warfare attacks, breaking them down into attacks that are primarily exploitative,

[113] *See generally* Walker, *supra* note 53.

[114] *See* Assessment of International Legal Issues, *supra* note 44, at 6.

[115] *See* Jensen, *supra* note 97, at 222.

destructive or disruptive.[116]

i. *Exploitation*

At present, the largest threat to American cyber security comes from exploitation attacks resulting in the theft of information and intellectual property from government and commercial networks.[117] The list of private sector victims of exploitation attacks includes Lockheed Martin, Google, Citibank, the International Monetary Fund, NASDAQ, and members of the oil and gas industries.[118] The government sector has suffered an alarming number of intrusions to agencies such as the Department of Defense, NASA, the Department of Energy, and Army Aviation and Missile command.[119]

---

[116] DoD Cyber Strategy, *supra* note 98.

[117] Lynn's Remarks, *supra* note 1.

[118] John D. Banusiewicz, *Lynn Outlines New Cyber Security Effort*, U.S. Dep't of Def. (June 16, 2011), http://www.defense.gov/news/newsarticle.aspx?id=6434964349 [hereinafter Banusiewicz].

[119] The "Moonlight Maze" attack involved Russian hackers who probed networks at NASA, the Department of Energy, the Department of Defense and others starting in 1998. Intelligence stolen may have included Navy passcodes and missile guidance data. Though the attack seemed to stem from the Russian Academy of Sciences, the Department of Defense suspected a state sponsored effort to obtain classified U.S. defense technology secrets. *See* Gregory Vistica, *We're in the middle of a Cyber War!*, NEWSWEEK, (Sept. 19,1999)*; see also* Schaap, *supra* note 48, at 134; *see also* Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L. L. 825, 840 (2001). In the "Titan Rain" incident Chinese hackers broke into U.S. defense systems starting in 2003. The hackers are thought to have stolen U.S. military secrets from the Redstone Arsenal, home to the Army Aviation and Missile Command, including aviation specifications and flight-planning software. The methodologies used by the attackers lead experts to suspect that the attacks had military origins. *See* Schaap, *supra* note 48, at 134; *see also* Tom Espiner, *Security experts Lift Lid on Chinese hack attacks*, ZDNET.COM (Nov. 23, 2005), http://news.zdnet.com/2100-1009_22-145763.html.

Exploitation attacks primarily utilize flaws in software design or implementation to gain access to restricted data. When software is written, the code defines specific steps that a computer must execute to obtain a desired result. If these steps are not well defined or specific enough, attackers may be able to skip the step and obtain unauthorized access. In a simple example, a piece of software may be designed to restrict access to tank blueprints to only those users having IP addresses between 12.34.567.005 and 12.34.567.009. If the software programmer code included a step to check that the last three digits of the IP address are greater than five, but forgot to include a step that checks if the last three digits are less than nine, then anyone with the IP address 12.34.567.005 to 12.34.567.999 can access the restricted tank blueprints.

In complicated real world settings, vulnerabilities in government and commercial networks are difficult for attackers to casually manipulate. Attackers must utilize additional tools referred to as "exploits." These are chunks of software code, data, or data sequences that cause unintended results to occur when the legitimate software is executed. Other methods of obtaining access to restricted data such as "IP spoofing" involve exploiting the ignorance of a legitimate user by tricking them into divulging information.[120] Once an attacker can control legitimate software or access information, he or she can obtain files such as engineering schematics, passcodes, research data, and the like.

The "theft of intellectual property threatens national competitiveness and the innovation

[120] IP Spoofing involves an attacker who masquerades as a trusted host computer to hide his identity. The method can be used to hijack networks, web browsers, and web pages themselves, thereby providing the attacker with access to potentially restricted content. "When IP spoofing is used to hijack a browser, a visitor who types in the uniform resource locator (URL) of a legitimate site is taken to a fraudulent web page created by the hijacker. If the user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. *See* Schaap, *supra* note 48, at 134.

that drives it."[121] The estimated economic loss due to exploitation attacks is over a trillion dollars in the United States alone.[122] This number does not contemplate the threat to national security posed by loss of intelligence, weapons schematics and defense strategy. There is no way of knowing how information gleaned through an exploitative attack will be disseminated and utilized. Hostile nations may use such information to gain competitive edge in defense industry markets or financial sectors. Weapons technology information may be used to develop counter-measures, thereby reducing the effectiveness of the victim nation's offensive military technology. Unlike conventional weapon attacks, the deleterious effects of exploitative information warfare may be long lasting, unpredictable, and widespread, making these attacks exceptionally dangerous to a nation's military operations.

Though dangerous to national security and economic prosperity, exploitative attacks will not generally fall within the scope of armed conflict. The exploitation of computer software and hardware vulnerabilities to gain access to restricted information and computer systems is not likely to cause injury, death, or damage akin to attacks using bombs and guns. It is feasible that an armed combatant could enter a military complex and demand tank blueprints or military intelligence at gunpoint, but such an operation would not be covert and thus the intelligence obtained necessarily limited. It is a stretch of the imagination to assume that exploitation attacks are an equivalent substitute for guns and bombs in information gathering operations. Any attempt at classifying exploitative attacks as armed conflict would thus depend on the attack causing damage to the military or civilian population, protected persons or property. Theft of military secrets could have direct repercussions on military and civilian populations alike, but exigency is

[121] White House Cyberspace Policy, *supra* note 111, at 4.

[122] Lynn's Remarks, *supra* note 1.

a problem. Even though the loss of military weapons schematics could potentially cause economic losses to civilian contractors and allow enemy militaries to gain competitive advantage, these effects are not immediately and directly deleterious to the civilian population. Thus, there is a causality problem that arises from the indirect nature of the damage of an exploitation attack. Whether an effect is adequately immediate and direct may depend on the lapse of time between the attack and the resulting harm and whether the attack directly affects the protected target(s). It is highly unlikely that the bulk of exploitation attacks will rise above the level of intelligence gathering or espionage, so the LoAC will apply minimally.[123]

ii. *Destruction*

The most fear-inspiring cyber assault scenarios arise from attacks that result in serious physical damage, known as destructive attacks.[124] These attacks use digital tools to cause physical destruction of control system equipment, network infrastructure, and in extreme cases the destruction may target geographical locations and the local human population. It is this type of strategy that Stuxnet attackers utilized when they corrupted the orders given to control system software, making the uranium centrifuges spin out of control.[125] Depending on the function of the target computer the damage caused could range from the simple cost of replacement to widespread casualties.

To cause physical damage to property with digital weapons, attackers must either alter the operation or cause the self-destruction of a computer. A particularly effective destructive attack might use exploitative methods to gain restricted access to the operations control system of a

[123] *See* Hague Convention IV, *supra* note 100, at arts. 30-31.

[124] Banusiewicz, *supra* note 119.

[125] Fildes, *supra* note 7.

computer responsible for the cooling system at a nuclear power plant. A communications link between the control system computer and the outside world could be opened to allow remote users to access the machine. A remote attacker could then disable the cooling system, resulting in a nuclear meltdown that devastates the surrounding environment.[126] The Department of Energy attempted to simulate the effects of this type of attack by executing a control hacking incident on a nuclear power plant.[127] The ease with which the hackers were able to throw the generator's control system out of control alarmed intelligence and defense agencies across the United States.[128]

Alternatively, attackers can destroy a control system computer rather than manipulate its standard function. This can be accomplished through a variety of methods, one of which is referred to as a "permanent denial of service" (PDoS) attack.[129] Such attacks target the computer's hardware in an attempt to overload that hardware until it shuts down. Unlike methods that force manual reboot of a computer, PDoS attacks result in destruction of the host computer that requires replacement of the equipment.[130] The end result of an attack on computer hardware may be the same as one that subverts system software to cause destruction, but the victim's ability to recover may differ according to the methods used. If only the system software has been

---

[126] *See generally* Jensen, *supra* note 97, at 222; *see also* Brown, *supra* note 93, at 186.

[127] *See* Jeanne Meserve, *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*, CNN (Sept. 26, 2007), http://www.cnn.com/2007/US/09/26/pow er.at.risk/index.html [hereinafter Meserve].

[128] *Id.*

[129] *See* Schaap, *supra* note 48, at 134.

[130] *Id.*

tampered with, personnel may be able to restart the affected computer or shut down a specific function. In the case of a permanent hardware disablement that destroys the host computer, the victims may be left with little or no recourse for stopping the resulting damage.

The potential for abuse of destructive information attacks is increasing. Though destructive attacks have been simulated, the U.S. Department of Defense asserts that, to date, no destructive cyber attacks have been used by military powers.[131] The current balance of cyber power lies primarily within the militaries of nation states and "the most malicious actors have not yet obtained the most harmful capabilities[.]"[132] This balance of power is unlikely to last forever due to the shrinking cost of computer systems and the increasing influence of the Internet in countries that harbor terrorist groups. As cyber weapons continue to develop in strength and ease of use, the danger to populations around the world will continue to escalate.

Destructive attacks are best classified as part of armed conflict. By definition, destructive attacks cause destruction of computer systems, infrastructure and even physical property. A properly executed destructive attack could destroy or permanently disable military systems, power plants and dam lock controls. The targeted application of small bombs or men with assault rifles could also take out these targets. A computer system destroyed by a deliberately instigated electrical short is just as useless as guns or bombs used to physically destroy the system. Destructive attacks are armed conflict because they cause injury, death, or damage to military forces, citizens, or property of a belligerent and thus fall within the purview of the LoAC.[133]

---

[131] Lynn's Remarks, *supra* note 1.

[132] *Id.*

[133] *See* Assessment of International Legal Issues, *supra* note 44, at 6.

iii. *Disruption*

Disruptive attacks deny or degrade the functioning of government or commercial networks.[134] Potential targets may include essential infrastructure such as, public utilities, financial services, defense operations, and communications networks. The disruption of any of these services can trigger a detrimental domino effect to military and civilian communities alike. It was this type of attack that hackers used to disrupt infrastructure accessibility in the Estonia and Georgia incidents.

The most common method used to execute a disruptive attack is the aptly named "denial of service" attack.[135] The term "denial of service" (DoS) refers to a family of offensive methodologies that attempt to overwhelm a target computer system to prevent it from operating normally. An attacker utilizing the DoS method sends a flood of fake communications requests, in the form of digital packets, to a server on a target network. The target system uses its resources to process the data as though it were received during the normal course of operations. Eventually, the server becomes overloaded with the effort to receive and respond to the phony messages, no longer being able to handle legitimate requests from others. If too much traffic is directed at the server, it may crash and remain inoperable until manually restarted.

The effectiveness of the method is increased with the use of botnets, or collections of

---

[134] Banusiewicz, *supra* note 119.

[135] *See* Mindi McDowell, *Understanding Denial-of-Service Attacks*, US-CERT (November 04, 2009), http://www.us-cert.gov/ncas/tips/st04-015. http://www.us-cert.gov/cas/tips/ST04-015.html

numerous computers to execute multiple DoS attacks on the same server.[136] Computers in a botnet are compromised through exploitative methods to allow a remote operator to control some of the computer's resources**.** Using a botnet, an attacker can flood a target system with many times the amount of data communications requests that could be sent with just a single computer. This type of concentrated effort is known as a "distributed denial of service attack" (DDos) and is used against large targets with robust networks such as those employed by commercial Internet websites, government agencies, and emergency services.

A preemptive disruptive attack against an enemy's critical service infrastructure could drastically reduce their ability to effectively respond to subsequent physical attacks. If the dispatch routing servers for 911 emergency calls were shut down in a disruptive attack, local civilian and military personnel would be unable to receive and respond to calls for help. Attackers could execute disruptive attacks against traffic signal control systems responsible for signal timing, equipment diagnostics, and traffic system performance. Without an operable signal control, system traffic lights would perform erratically causing serious problems in metropolitan areas. Air traffic control systems could be disrupted, preventing aircrafts from landing for dangerously lengthy periods. Many of these services can be remotely managed, making them vulnerable to offensive attempts to subvert control systems.[137]

Disruptive attacks can also target the flow of information rather than services. Attackers

[136] A remote attacker can control compromised computers from a distance. To compromise the computers, viruses may be used to open up connection points (backdoors) on a user's computer that would otherwise be closed. An attacker may then connect to the compromised computer through the open connection and launch DoS attacks at the target server. Many viruses are self-replicating and can spread to other computers, further increasing an attacker's arsenal. *See Id.*; *see also* Schaap, *supra* note 48, at 134.

[137] *Se* Meserve, *supra* note 128.

can shutdown media and government websites or hijack those websites for the purposes of disseminating the attackers' own information.[138] Television and radio signals can also be hijacked and supplanted with a phony signal. By taking over the news media and Internet press, an enemy military can make false statements about the status of fighting, the whereabouts of government officials, culpability for attacks, and whatever propaganda the attackers choose to spread.[139] Such information disruption can result in reduced awareness of the civilian population and increased disorganization during a physical assault. The LoAC prohibits the hijacking of telecommunications signals, but the prohibition is unlikely to stop terrorist groups from utilizing the tactic. [140]

Strategic use and timing of a disruptive attack can mitigate the loss of human life or increase the destructive toll. A disruptive attack's range of effects may vary from public confusion and disorientation, to numerous casualties due to loss of power, water, and access to first responders. Preemptive cyber strikes could reduce casualties by impairing a defender's ability to exert resistance to physical attacks, making it easy for invaders to seize control. On the other hand, these reduced response capabilities could open the door for malicious attackers to commit acts of mass slaughter. Whether or not disruptive cyber attacks are more humane than physical actions lies in the hands of an attacker.

Disruptive attacks are difficult to characterize because their results vary, but they will

---

[138] *See e.g.*, Rob Taylor, Reuters, *Hackers Take Over Taliban Website*, London Free Press (Apr. 27, 2012), http://www.lfpress.com/news/world/2012/ 04/27/ 19686051.html.

[139] *Id.*

[140] Passing yourself off as a government entity and alluding to armistices or ceasefires that have not actually occurred have been determined by US DoD to be a war crime. *See* Assessment of International Legal Issues, *supra* note 44.

generally be classified as armed conflict. A disruptive attack that degrades or disrupts services of critical infrastructure like air traffic control systems, utilities accessibility or first responder dispatches could have disastrous effects on both military and civilian populations. In one situation, first responders could be technologically cut off and unable to address distress calls. Alternatively, the attack might only stymie the flow of service just enough to cause a distraction that facilitates an easy ground invasion. In such a situation, Emergency calls may experience excessive disconnections or improper addresses transmitted to first responder vehicles. In the first scenario, it is fairly easy to imagine that injury, death or damage could result from the disruption. The second scenario, however, is not easily analogized to conventional arms. It seems farfetched that armed military personnel would invade a first responder dispatch without killing anyone and instruct the operators to arbitrarily send callers away. Guns and bombs are not reasonable means of obtaining these objectives; therefore, injury or death are not inevitable results. Thus, disruptive attacks at this end of the spectrum must be considered in view of the resulting damage to military or civilian populations, protected persons or property.[141] More often than not, attacks perpetrated by a state actor that degrade or disrupt services in another state will cause damage to protected persons or property. These attacks are therefore conducted in the course of armed conflict and the LoAC applies to their commission.

C. Conclusion

As I have discussed above, information warfare is an effective and rapidly evolving means of commencing armed conflict. Whether or not an action is committed in the course of armed conflict is dependent on the status of the actor, the place of the action, and the nature of the action. Information attacks conducted in the course of armed conflict should be subject to

[141] *Id.*

the LoAC in the same manner as other forms of armed conflict. In the subsequent section I will analyze the application of the LoAC to issues arising from information warfare scenarios that involve neutral nations.

4. Analysis

The Hague Conventions are applicable to digital armed conflict in much the same way as they apply to physical conflicts. Some of the rules and regulations set forth in the Hague Conventions are easily extended to the digital battlefield, while others require adjustment and adaptation. Neutral states must act as designated by the duties and obligations assigned to them by the LoAC, even when the modality of war is the digital battle space. All belligerents must respect the inviolability of the land, property and citizens of a neutral state, regardless of whether the weapons used are physical or digital. In this section, I will discuss and analyze the duties and obligations of neutral states in information warfare and apply them to the information attacks discussed at the beginning of this paper.

A. How Information Warfare Affects the Privileges and Immunities of a Neutral State

Digital communications by a belligerent that utilize a neutral state's Internet infrastructure will potentially violate the principle of neutrality. Users of the Internet cannot control the paths that their information takes before reaching the intended destination.[142] Data sent from a single source may be broken up into smaller groups and sent along different paths

[142] The Defense Advanced Research Projects Agency ("DARPA") is developing Internet modifications in the form of "active networks." Active networks can permit users more choice in the routing of their data by supplying their own instructions and requirements for path selection. *See Active Networks*, LINKTIONARY.COM (2001), http://www.linktionary.com/a/active_network.html.

before being reassembled at the end of the journey.[143] The data transmissions of a belligerent state could travel through many states, including the Internet infrastructure of a neutral state, thereby trespassing on the neutral's territory.

Unaggressive transmissions such as correspondence of information and intelligence transmitted from a belligerent state will not violate the principle of neutrality. This is because the Hague Convention provides that neutrals may allow use of their telegraphy systems by all belligerents.[144] The analogy between transmitting telegraphs over wire is easily extended to sending emails over fiber-optic cable. Indeed, the United States DoD has already adopted the extension of the telegraphy provision to modern communications systems.[145] Thus, a belligerent's Internet transmission of an informative nature will not violate the principles of neutrality if it crosses the boundaries of a neutral's territory.

Conversely, information attacks that utilize the Internet infrastructure of a neutral state violate the principle of neutrality. The primary privilege of neutrality is inviolability of territory.[146] A strict interpretation of this rule indicates that belligerents may not move munitions or troops of any kind, across the territory of a neutral state.[147] Cyber weapons are small and digital, but they can be used to destroy infrastructure, property and even cause death.[148] If a

---

[143] *See* George K. Walker, *Information Warfare and Neutrality,* 33 VAND. J. TRANSNAT'L L. 1079, 1199 (2000).

[144] Hague Convention V, *supra* note 51, at art. 8.

[145] Assessment of International Legal Issues, *supra* note 44.

[146] Hague Convention V, *supra* note 51, at art. 2.

[147] *See* Hague Convention V, *supra* note 50, at art. 2; *see also* Brown, *supra* note 93.

[148] Weapons are "devices designed to kill, injure, or disable people, or to damage or destroy property," U.S. Dept. of Air Force Policy Dir. 51-54, *Compliance with the Law of Armed*

belligerent state launches an information attack that moves cyber weapons across a neutral's Internet infrastructure, then the belligerent violates Article Two of the 1907 Hague Convention V. The violation occurs regardless of the belligerent's inability to control the transmission pathway of the attack. As a result of the current scheme for Internet traffic routing, belligerent states may inadvertently violate the principle of neutrality when using information warfare.

Like offensive information attacks, a belligerent's espionage and military intelligence gathering operations may not utilize neutral communications infrastructure. Exploitative attacks, best characterized as military intelligence gathering, or espionage, do not generally rise to the level of armed conflict.[149] Even so, the Hague Convention does provide some guidance to signatory nations on how to treat belligerent intelligence gathering activities. The Hague Convention states that such activities are "necessary" aspects of warfare, and prohibits a neutral from allowing belligerents to make aerial or sea-based observations of enemy forces, from within the neutral's territory.[150] This suggests that neutrals should not allow belligerent forces to utilize a neutral's territory even for non-offensive purposes. The premise is easily extended to the digital battlefield. If physical weapons are disallowed, then digital weapons are disallowed. If physical surveillance is disallowed, so too is digital surveillance. Therefore, a belligerent's use of neutral Internet infrastructure to conduct intelligence gathering on enemy forces will violate the principle of neutrality.

Conflict, 6.5 (Aug. 4 2011), available at: http://www.e-publishing.af.mil/shared/media/epubs/afpd51 -4.pdf.

[149] The provisions of the Hague Convention addressing espionage are more applicable to exploitative attacks than provisions addressing armed conflict. *See* Hague Convention IV, *supra* note 100, at arts. 30-31.

[150] *See* Hague Convention IV, *supra* note 100 at art. 24; Hague Air Rules, *supra* note 51 at Art. 47.

B. **What's a Neutral to Do?**

A neutral's duty to respond to information attacks that utilize the neutral's computer systems and Internet pathways is dependent on the situation. Unlike ground invasion, digital invasion presents a number of issues that would make a bright line "duty to repel" impracticable. The breakdown in real-world practicality of applying the most applicable Hague provision should not prohibit the application of other provisions that are better suited to the digital battlefield. Analogies can be drawn between information attack scenarios and situations in the physical realm that provoke a duty to remain impartial, intervene, or repel. Utilizing these analogies to adapt the existing framework of the LoAC to information warfare provides a means for addressing the potential problem of neutrality violations. In the rapidly developing arena of information warfare, it will be far more cost effective and time efficient to adapt existing frameworks rather than developing entirely new approaches, as the slow pace of international law development is likely to render treaties on information warfare obsolete before signing is complete.

There are multiple logistical issues that make digital violations different from physical violations of a neutral's territory. The problems of notification and attribution must be addressed before a neutral state can decide on the proper response to a violation of its neutrality. As a practical matter, for a neutral state to respond according to its duty under the Hague Conventions, it must be aware that an event is occurring that necessitates action by the neutral and it must know that the perpetrator of the event is a belligerent state. If a neutral state does not have notice that an attack is occurring or know the identity of the attacker, the neutral cannot be certain that an obligation to act exists.

The complexity of data routing through the Internet and the speed at which data travels

make real-time assessment of information attacks nearly impossible. Files are split up into small data packets that can travel a multitude of different paths on their way to their intended target.[151] Data packets travel at blinding speeds through a vast web of interconnections, existing in each location for portions of a second. By the time an information attack occurs, the digital weapons have already transited intermediate territories. Consequently, countries caught in the middle of an information attack are advised of their unwitting participation well after the attack is over. A middleman country rarely receives notice that it is being victimized while an attack is occurring. To find both the responsible and unaffiliated participants of an attack, computer forensics experts carefully trace the route of the attack backwards by examining data traffic at each stopping point in succession. This process can take months depending on the complexity of the attack and the routes used. Thus, significant lapses in time can occur between the actual violation of a neutral's digital territory and the time at which the neutral becomes aware of the violation.

Likewise, it may take a substantial portion of time before the perpetrator of the attack is discovered. The process of tracing the attack backwards along its path is time consuming at best. At worst, the trail is so obscured that no discernible initiation point is found. It could take days, weeks, months or even years to discover the location of computers used to initiate an attack. The location of an attack's starting point does not necessarily mean that the attacker is from that location or that the actor is a state rather than an individual or group. Perpetrating computers located on military bases are obvious indicia of state action, but computers belonging to administrative agencies or state-run businesses will not provide a firm connection between the state and the action because a private individual could access the computers without state authorization. Neutral states caught in the middle of a cyber attack may wait lengthy periods of

[151] Walker, *supra* note 53, at 1098.

time before discovering which belligerent(s) initiated the attack. In some cases the neutral state may never know the perpetrator's identity. Without attributing the attack to a specific belligerent, the neutral may be unable to effectively execute its duty to act.

A neutral's first duty is to remain impartial to all belligerents, particularly with respect to telecommunications and e-commerce. Belligerents using a neutral state's Internet infrastructure for unaggressive telecommunications purposes do not violate the principle of neutrality. Consequently, neutrals do not have a sufficient legal reason for denying specific belligerents access to Internet infrastructure and telecommunications means. Access to the neutral's telecommunications means must be available to or denied to all belligerents.[152] If preference is given to one belligerent over another, the neutral state violates its duty to remain impartial. To avoid neglecting this duty, the neutral must take steps to ensure that Internet Service Providers (ISPs) and telecommunications companies within the state do not filter, block or degrade bandwidth availability to belligerents individually.[153] This can be accomplished by a state-issued notice or temporary regulation prohibiting discriminatory behaviors during the course of the conflict.[154] Any Internet infrastructure located within a neutral's territory but owned by a belligerent must be shut down unless the owners agree to make the service available publicly and impartially.[155] Similarly, private companies in the neutral state can export arms, munitions, and

[152] *See* Hague Convention V, *supra* note 50, at art. 3, 8.

[153] *See id.* at art. 8-9.

[154] I find it highly unlikely that the duty extends to making the neutral government "hand check" each ISP on a regular basis to ensure compliance. The resulting administrative burden would be unreasonable and I was unable to find a single example of such behavior with respect to the telegraphy lines described in the Hague Convention.

[155] Hague Convention V, *supra* note 50, at art. 3.

supplies to belligerent forces as long as the goods are equally available to all belligerents.[156] On the digital battlefield, such trade goods could comprise network defense software and code for digital weapons. The sale of these items can be physical or completed over the Internet, with the goods themselves available for download by belligerents. Restriction of a belligerent's access to the neutral state's Internet infrastructure would make online purchases of digital defensive and offensive goods difficult, resulting in the violation of the neutral's duty to remain impartial with respect to export of goods of war. The best way for a neutral state to reduce the risk of inadvertent violation of its duty to remain impartial is for the state to provide actual notice to ISPs, telecommunications companies, and private businesses dealing in software or network services, communicating that all belligerents must be treated equally and without preference for the duration of the conflict. It is unreasonable to require that a neutral perform regular monitoring of each of these sectors for impartiality, but if a belligerent asserts that other belligerents receive preferential treatment with respect to Internet infrastructure access, the neutral state must act decisively to correct the error.

The next duty, the duty to intervene in belligerent operations on neutral territory, imposes an active intermediary role on a neutral state. A neutral must intern ships, planes and ground forces found within its borders to prevent belligerent attacks from originating within the neutral's territory.[157] Digital weapons, like their physical counterparts, must not be allowed to leave the neutral's territory once the weapons are discovered. Similarly, any attacks on belligerents that originate from within a neutral's borders must be disrupted immediately.

Information attacks that involve the use of a neutral's computer systems to launch

[156] Id. at art. 7, 9.

[157] *Supra* §2.c.ii.

offensive operations against a belligerent may be construed as originating from within the neutral's territory. Because neutrals are unlikely to declare neutrality and then deliberately launch attacks against belligerents, it is likely that computer systems used in the attack are compromised to allow remote control by belligerent attackers.[158] Once an attack commences, it may be discovered by an administrator of the compromised computer system or after the attack is over, during an investigation. These are the most probable scenarios for discovering the digital arms and munitions of belligerents within a neutral's territory. As discussed above, attacks merely "passing through" the neutral's Internet infrastructure are moving too fast and erratically to permit detection. In some rare cases, digital weapons such as those triggered to execute at a particular time or in parallel with a trigger event, may be discovered before an attack occurs by a computer system administrator who observes the system's odd behavior.

Intervening in belligerent information operations entails preventing operation of computer systems that would permit attacks or surveillance to commence, continue, or reoccur. The Hague Conventions stipulate that belligerent forces found within a neutral's borders must be interned as far from the theater of war as possible, thereby preventing belligerents from utilizing neutral ground to launch attacks on opposing forces.[159] At sea, neutrals may do what they believe is necessary to prevent belligerent vessels from leaving the neutral's territory in a battle-ready state.[160] With respect to belligerent aircraft on neutral ground, the neutral must use whatever

[158] It is unlikely that states that declare their official neutrality will then, of their own free will, attack belligerent states. This would destroy their neutrality and bring the state into the armed conflict. I therefore assume for the purposes of this analysis that attacks made from within neutral territory are actually perpetrated by outside attackers utilizing remote access to the neutral's computer systems.

[159] *See* Hague Convention V, *supra* note 51, at art. 11.

[160] *See* Hague Convention XIII, *supra* note 51, at art. 24.

means are at its disposal to prevent the aircraft from leaving to execute offensive operations or to obtain surveillance of opposing belligerent forces.[161] The fluid nature of the Internet and its lack of recognizable borders make the digital battle space more like air and sea warfare than traditional land based combat. Standards for aerial and naval warfare are therefore the most appropriate for application to information warfare. Applying these standards to the digital battlefield, a neutral may take actions it deems necessary to stop a potential attack from occurring, but it must use the means at its disposal to prevent an attack that is occurring or is certain to occur without intervention.

In many situations, affected computers can be quarantined and disconnected from the Internet and other computers on its network, thereby removing the computer's ability to transmit and receive data packets. A computer system that cannot transmit data is unable to participate in information attacks. Quarantine of critical computer systems can be tricky and time consuming because system administrators must attempt to prevent the system from engaging in malicious communications while maintaining its ability to engage in vital aspects of its normal operation.

Presently occurring or immediately imminent attacks are matters of exigency that may necessitate immediate intervention. Timely quarantine of affected computer systems is not always sufficient. The fastest way for a neutral to intervene is to shut down computer systems and Internet infrastructure suspected of harboring a belligerent's digital weapons or surveillance. This approach presents serious practicality problems for the neutral because it could mean shutting down systems critical to the operation of the economy, government, and general communication. It is analogous to requiring a neutral to shut down its seaport or blow up its airport to prevent belligerent ships and aircraft from quitting the neutral's supervision. Common

[161] *See also* Hague Air Rules, *supra* note 52, at art. 47.

sense suggests that it would be easier and less costly to the neutral to simply smash a hole in the side of the warship or aircraft and intern the crew. A physical aircraft or ship belonging to a belligerent can be shot down or otherwise damaged, but damaging digital weapons may be difficult or impossible without crippling the neutral's own property. Furthermore, the shutdown of telecommunications systems or Internet infrastructure can create ripple effects that cause service interruptions for countries far removed from the armed conflict.[162]

I propose the more reasonable interpretation of the disposal test to require that a neutral use the means at its disposal to intervene in an ongoing or immediately imminent attack so long as the damage to the neutral would not outweigh the harm to the belligerent. Neutrals are thus obliged to redirect manpower and system capabilities into the effort to quarantine an attacking computer system, but will only be required to shut the system down when timely quarantine is impossible and the harm to the victim belligerent of allowing the attack to continue outweighs the harm to the neutral of shutting the computer system down. A balancing test might seem unwieldy, but situations involving damage to civilian population or loss of human life will clearly outweigh most other interests. Such situations could arise during disruptive or destructive attacks, which can result in severe consequences to the human population of a belligerent state. If a neutral state learns that vital computer systems are being used by a belligerent to obtain intelligence about an opposing belligerent, the neutral would simply need to quarantine the system to the best of its ability, regardless of whether the quarantine is 100% successful. But, if the attack causes loss of human life, the neutral certainly has to shut down the offending computer systems to avoid violating its duty to intervene. By adopting a modified interpretation of the current duty, Hague Convention signatories could provide neutral states with some

[162] *See* Lynn, *supra* note 1.

flexibility in safeguarding their own interest while still meeting their duties under the Hague Conventions.

The final duty, the duty to repel, requires the employment of primarily proactive measures to prevent digital incursions onto a neutral's territory. When belligerent troops trespass on neutral land, the neutral is obligated to repel the trespassers.[163] Belligerent incursions into a neutral's airspace or waterways must be repelled using the means at a neutral's disposal.[164] The Hague Conventions do not specify whether the duty is proactive, reactive, or both. Proactive measures include barricades, sea gates, land and sea mines, and any other measures put in place to prevent a trespass from occurring. Once a trespass occurs, reactive measures using force of arms are employed. In information warfare, proactive measures take the form of firewalls, security software, closing network ports, disabling file sharing, and implementing personnel security measures. These measures are relatively inexpensive when compared to the cost of building barricades. Government agencies and military installations can easily implement such reasonable means of protecting themselves from information attacks and repel some belligerent incursions. Well-trained attackers will thwart even the best security systems, so a neutral's duty to repel cannot be absolute; nor can it end at the installation of security software and firewalls. If a neutral becomes aware of an ongoing attack that utilizes the neutral's Internet infrastructure, it should increase security measures in an attempt to block data traffic coming from the belligerent state. Attacks that continue despite an increase in security measures will trigger the neutral's duty to intervene in the attack. Consequently, the duty to repel requires mostly proactive measures by a neutral, and in the event that such actions fail, the neutral may be forced to intervene in the

[163] *See* Hague Convention V, *supra* note 51, at arts. 1-2, 5.

[164] Hague Convention XIII, *supra* note 51, at Art. 24; Hague Air Rules, *supra* note 52, at Art. 42.

attack with more aggressive measures such as quarantining or shutting down computer systems.

These duties collectively require that neutral states take an active role in preventing their inadvertent participation in an armed conflict. States cannot absolve themselves of liability by declaring neutrality. Where information warfare is concerned, neutrals must preemptively act to protect their Internet infrastructure and telecommunications highways. Neutrals must provide notice to telecommunications companies that their services shall be equally available to all belligerents and the public. The neutral must also adopt security measures to block information attacks from accessing the neutral's communications pathways. In addition to preemptive measures, neutrals must react as expeditiously as possible to intervene in information attacks originating within the neutral's territory.

If the neutral is unable or unwilling to fulfill these duties, belligerents may act in self-defense even if that action involves violating the principle of neutrality.[165] The "right of necessity" permits belligerents to protect themselves from harm when a neutral state is incapable of stopping an opposing belligerent from violating the neutral's territory. Ongoing information attacks that utilize a neutral's Internet infrastructure, computer systems, and telecommunications resources will trigger the neutral's duty to intervene, but the neutral may be unable to effectively quarantine affected services and unwilling to shut them down. The neutral acts appropriately within its duty to intervene if it deems that the harm to the neutral of shutting the systems down outweighs the harm to the belligerent of letting the attack continue. Understandably, the target belligerent's opinion may differ from that of the neutral state. If the belligerent feels that its interest strongly outweighs the neutral's interest and the neutral has not succeeded in repelling

[165] *See* Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare,* 106 MICH. L. REV. 1427-35 (2008).

the attacks or intervention therein, then the belligerent can take steps to stop the attackers from utilizing neutral resources. Such steps may include blocking Internet traffic from the neutral territory, digital sabotage of affected neutral systems and even physical invasion of the neutral's territory to shut down or destroy the offending systems.

The defensive right of necessity should be used sparingly by belligerents and only in times of exigency. On land, the invasion of neutral territory involves the rerouting of troops and supplies to cut off opposing belligerents on neutral ground. There is an opportunity cost as well as real cost associated with moving armed forces around and engaging the enemy in combat. These costs are drastically reduced in a cyber setting because effective defensive measures may be enacted from afar. The ease of affecting defensive capabilities obscures the danger associated with forcible shut down of potentially critical computer systems without warning. Unanticipated disruption in essential network infrastructure may have disastrous effects on a neutral's economy, utilities, first responder systems, and more. These effects may extend beyond the neutral's borders into other countries, some of which may not be involved in the armed conflict in any way. While belligerents are free to take measures to protect their citizens and their interests, they should think carefully before invoking the right of necessity to shut down neutral systems because the results may be significantly deleterious to the international community.[166]

[166] The United States recently asserted its right of self-defense in cyberspace, stating, "[w]hen warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking

C. Applying The Hague Conventions to Information Warfare Scenarios

Applying a neutral's duties and obligations to real-world scenarios involves subjective decision-making. There are many shades of grey regarding a belligerent's culpability for violating the principle of neutrality that can make it difficult to rationalize harsh intervention or repellant actions in some situations. More importantly, harsh actions responses can cause a degradation of Internet accessibility of countries not involved in the conflict. Neutrals must carefully consider the potential outcomes of their actions and be prepared for the possibility of international outcry arising over the results of a decision. In this section, I examine how a neutral state should act to meet its duties and obligations if involved in the scenarios described in the introduction to this paper. For the purposes of providing uniformity and simplicity, I impose a recognized international armed conflict on each scenario wherein the target state and the proposed actor are belligerents in the armed conflict. In each case, the duties and obligations of a hypothetical neutral state are discussed.

What should a neutral do if its Internet infrastructure was used to perpetrate an exploitative attack on the U.S. Department of Defense that resulted in the theft of a substantial quantity of electronic files? Exploitative attacks are espionage or military intelligence gathering, not armed conflict. If the attacker is a belligerent clandestine agency or military, then the neutral must take action to prevent further incidents of espionage or intelligence gathering. But, if the actor is a private group or individual and the state does not exert "effective control" over the actor, then the attack is merely cyber crime and the LoAC does not dictate the neutral's behavior.[167] Attribution is necessary before determining a proper course of action. This case

broad international support whenever possible." White House Cyberspace Policy, *supra* note 111, at 14.

[167] *See* Hague Convention V, *supra* note 51, at arts. 2-3.

presents a prime example of the problems that attribution can cause. No single state has been blamed for the theft and no evidence has been published that suggests specific actors. The neutral state cannot accurately gauge the extent of its obligation without knowledge of the actor's status as a belligerent. Still, it is best to err on the side of caution and assume that the actor is a belligerent military and a duty exists. The duty requires active participation by the neutral, because the attack has already taken place and proactive measures were ineffective. Was the information attack "just passing through," invoking a duty to repel, or was it utilizing the neutral's computer resources to assist in the execution of the attack, invoking the duty to intervene? The neutral should conduct its own inquiry if possible to determine the answer to this question. If a duty to repel exists, then the neutral must increase security measures and attempt to block traffic from the offending belligerent. If a duty to intervene exists, then the offending computer must be removed from the belligerent's arsenal if reasonably possible.

Because the attack is unknown in this case, repellant measures will be ineffective, making intervention necessary. A neutral state cannot repel attacks by blocking data traffic from a specific country, if the identity of the attacker is unknown. Neutrals cannot arbitrarily block traffic from all potential attackers because doing so denies telecommunications infrastructure to individual belligerents, violating the neutral's duty to remain impartial. The ineffectiveness of repellant measures gives rise to the duty to intervene. Here, the distinction between whether an information attack is passing through or originating within neutral territory is rendered moot by the lack of proper attribution. The neutral is therefore obligated to use the means at its disposal to intervene, so long as the damage to the neutral would not outweigh the harm to the belligerent.

The neutral should balance the cost to both parties of the neutral's intervention in the attack. While the neutral is required to conduct a reasonable investigation to discover computer

systems used in the attack, it does not need to exhaustively scour the digital landscape. Any computer systems identified as facilitating the attack must be shut down or quarantined. The neutral should determine whether systems can be effectively quarantined and, if this is not possible, whether the harm of shutting the systems down outweighs the harm of allowing ongoing theft of U.S. Department of Defense files. Systems vital to the neutral's critical infrastructure should not be shut down because the harm to the neutral would likely outweigh the harm to the United States. The neutral will successfully meet its duty to intervene by performing a reasonable search for participating computer systems and quarantining or disabling those systems to the best of its ability.

What should a neutral do when a belligerent actor employs a destructive information attack to destroy an opposing belligerent's non-critical resources, as in the Stuxnet attack? The Stuxnet worm was directly installed on target computer systems by an undercover operative, making this attack an act of espionage/sabotage rather than armed conflict. Whether the worm was electronically transmitted to or manually carried by the undercover operative, a neutral's territory could be violated during transit.

Once again, attribution is problematic for the neutral. The United States and Israel are suspected culprits but the suspicion is unconfirmed. In the previous example, meeting the duty to repel was impracticable given the lack of attribution, but in this case the neutral can choose to "repel" the U.S. and Israel based on the suspicion that these belligerents are responsible for the attack. Denying Internet accessibility to the U.S. or Israel would likely create the international perception that the neutral chose to side with Iran. Although the neutral would meet its duty under the Hague Conventions, the neutral could suffer serious international relations detriment. Alternatively, the neutral can choose to skip attempts at repelling and move to intervene in the

attack. A reasonable attempt at identifying and quarantining or disabling affected computer systems in accordance with the modified disposal standard will satisfy the neutral's duty to intervene. If intervention is not successful and more worms cross the neutral's borders, the neutral will be forced to repel the U.S. and Israel or risk losing its neutral status.

Lastly, what should a neutral do when its computer systems are used to disrupt essential infrastructure services of a belligerent, as in the Georgia/Estonia conflicts? The attack was attributed to Russia but the actor might be the state or a private group. Private group actors should be dealt with according to international cyber crime treaties, while state actors are addressed in the LoAC. The neutral here is the United States, whose servers were absconded and used in the botnet that launched numerous assaults on Estonian and Georgian network infrastructure. American computers, controlled by Russian attackers, executed repeated disruptive attacks, thereby triggering the U.S.'s duty to intervene and stop attacks from originating within U.S. territory. All involved states are known in this scenario and the neutral's obligation is clear, but this situation displays the problem associated with the timing of notification. The time at which the U.S. became aware of its involvement in the attacks is unclear from public reports. If it knew that its computer systems were compromised while the attack was occurring, the U.S. would be required to quarantine or disable those systems. But, if the U.S. did not receive notice of its involvement until the attacks were over, it would only need to remove remote control capabilities from the affected computers and take proactive measures to prevent attacks from reoccurring. Taking the proscribed action in either circumstance would satisfy the obligations of the U.S., but the extent of required action varies because of the differing levels of exigency.

The U.S. private company's storage of Georgian government data backups during the

Georgian conflict does not violate the U.S.'s neutrality, so long as no digital weapons were stored. The Hague Conventions prohibits belligerents from moving weapons and munitions onto neutral territory but does not restrict the movement of general resources.[168] Belligerents are thus free to store goods on neutral land that are not weapons or munitions of war. Georgian government websites are not digital weapons or munitions. Accordingly, private companies within a neutral state may offer to buy/sell or store belligerent goods without risking the violation of the principle of neutrality.

The application of the Hague Convention's duties and obligations to real world information warfare scenarios illustrates the many nuances of this mode of combat. Neutrals face problems with notice of attacks, attribution of attacks to a particular belligerent, potential damage to the neutral's digital resources, and damage to the neutral's international relations. Often, neutrals will be forced to make decisions on how to respond to an attack within a short period and without all necessary information. The positive side to this form of warfare is the potential for decreased loss of human life; so, even if neutrals suffer a greater rate of error, they may be less likely to make errors that result in loss of human life.

5. Conclusion

The ever-increasing utilization of information warfare will continue to pose a variety of complex legal problems. As technology develops, the spectrum of potential uses for information warfare will broaden. Creation of new applications for weaponized bits and bytes will inevitably result in the generation of new legal questions. The information warfare scenarios discussed in this article are a sample of the possible uses for digital attacks. It does not address every potential

[168] A non-state actor must be "effectively control[led]" by a state actor in order for the actions to be attributed to the state. *Nicaragua v. U.S.,* 1986 I.C.J. 14, (June 27, 1986).

legal factor but instead examines the basis for applying the Law of Armed Conflict to information warfare that involves neutral states. Can the Hague Convention of 1907 and subsequent Hague Rules Regarding Aerial Warfare, as pillars of the LoAC, be reasonably applied to information warfare involving neutral states? Yes. The duties and obligations imposed on neutral states by the Hague Conventions extend to the digital battle space. Information warfare will generally be construed as a form of armed conflict because it can result in injury, death, or damage to military, civilians, and protected property. Some information attacks, such as data theft, will be best categorized as espionage or cyber crime, but most information attacks pose serious physical threats. Information warfare, therefore, will generally fall within the purview of the LoAC. Neutrals thus have a duty to remain impartial, a duty to intervene in harm originating from within their borders, and a duty to repel belligerent forces in any form. Telecommunications services must be offered impartially, compromised computers within the neutral state must not be allowed to contribute to attacks on belligerent states, and pre-emptive measures must be taken to prevent information attacks from utilizing neutral telecommunications infrastructure. If neutrals cannot or will not meet these duties, then belligerents may exercise their right of necessity and take action to shut down neutral telecommunications resources that are used against the belligerent.

Though the LoAC applies to current methods of information warfare, the international community will have to work together to stay abreast of emerging trends in the use of digital weapons. Modification to the existing law of neutrality could be used to guide the actions of neutrals during armed conflicts involving information warfare. Norms that encourage neutral states to consider the legal and social consequences prior to choosing a course of action, will be far more beneficial to the rapidly developing area of warfare than new treaties that cannot fully

contemplate the extent of information warfare's future applications. Indeed, U.S. President Barack Obama stated that existing norms of international conduct in war and peacetime still apply in cyber space, making the re-invention of existing law unnecessary.[169] Nations must collaborate to develop new technologies that improve early warning capabilities and deterrent measures on the Internet.[170] By working together to adjust existing norms and create new technologies, the international community can shape the scope of information warfare, taking advantage of its non-lethal potential to mold a more humane form of war.

[169] White House Cyberspace Policy, *supra* note 111, at 9.

[170] *Id.* at 13.