NOTE

THE REUSABLE BOMB:

EXPLORING HOW THE LAW OF ARMED CONFLICT APPLIES IN CYBERSPACE

Rebecca Helene Sussman[1]

Abstract

In a world where lines of code can dismantle a nuclear power facility, the Law of Armed Conflict needs to change to reflect the devastation that one State can inflict on another through the use of cyber-weapons. The Law of Armed Conflict is too narrow to encompass current methods and means of cyberwarfare, including a weapon such as Stuxnet. Cyber-weapons are unlike conventional weaponry because a worm like Stuxnet is a reusable bomb—it destroys its target without destroying itself. This article illuminates the necessity for amendments to hold countries accountable for use of force and occupation through a State's invisible border.

[1] Rebecca H. Sussman is a 2016 graduate of Emory University School of Law, J.D. with a certificate in transactional law; 2013 magna cum laude graduate of Washington College B.A. in English Literature with honors, and is currently working as Associate Cyber Security Counsel, US Grid Company. Eternal thanks to Julie and Jerry Sussman for your unwavering support and encouragement, I strive to live everyday by your example. Countless thanks to Jacob Worenklein for allowing me to pursue my passion; working for you is a joy and an honor. Many thanks to Professors Laurie Blank, Johan Van der Vyver and Mark Goldfeder for encouraging me to be an active academic; your teachings have expanded beyond the lecture hall, and I am forever grateful to each of you. Dr. Erel Shvil, I cannot thank you enough for getting me to where I am today, I will always be thankful for your guidance. David and Stephanie, thank you for all your kindness. And finally, thank you to the BU JOSTL staff for publishing this article, I am forever grateful for your diligent work.

Introduction

The Great War saw the end of the cavalry, World War II saw the rise of nuclear power, and the Cold War showed the world that words can kill. The more information a country has, the stronger it is, which is why the Law of Armed Conflict must be adapted to encompass the nonphysical weapons of war. A word can indeed take the form of a weapon—when it is written in Python or C++. Now, a hundred thousand lines of code can shut off an entire city.[2]

States can be under siege and not realize it; in 2009 Iran was unaware for over a year that its nuclear facility was under attack throughout this period.[3] Cyber-attacks are not lethal in force, but the outcome of a cyber-attack can lead to having millions of people without power or a way to communicate with their government.[4] "Traditionally, when we think about security and protecting ourselves, we think in terms of armor and walls," said President Obama in an interview with Wired magazine.[5] Mr. Obama continued:

Increasingly, I find myself looking to medicine and thinking about viruses, antibodies. Part of the reason why cybersecurity continues to be so hard is because the threat is not a bunch of tanks rolling at you but a whole bunch of systems that may be vulnerable to a worm getting in there. . .You can't build walls

[2] Nicholas Schmidle, *Getting Bin Laden*, NEW YORKER (Aug. 8, 2011), http://www.newyorker.com/magazine/2011/08/08/getting-bin-laden [http://perma.cc/P5VJ-HKJQ]. *See also* Scott Pelley, *SEAL's First-Hand Account of Bin Laden Killing*, CBS NEWS (Sept. 24, 2012), http://www.cbsnews.com/news/seals-first-hand-account-of-bin-laden-killing [http://perma.cc/M9HA-GR93] (explaining that during Operation Geranimo, "there was a blackout in the neighborhood . . . [which] meant ideal darkness for the SEALs with their night vision goggles.").

[3] Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011, 7:00 AM), http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/ [https://perma.cc/6QUN-H5H6].

[4] LAURIE BLANK & GREGORY NOONE, INTERNATIONAL LAW AND ARMED CONFLICT: FUNDAMENTAL PRINCIPLES AND CONTEMPORARY CHALLENGES IN THE LAW OF WAR 131-132, 431 (2013); Pentagon Signs Off on Cyber Command, SEC. FOCUS (Jun. 24, 2009), http://www.securityfocus.com/brief/978; Roger W. Barnett, *A Different Kettle of Fish: Computer Network Attack*, 76 U.S. NAVAL WAR C. INT'L L. STUD. 21, 31-32 (2002); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 894 (1999); Natasha Solce, Comment, *The Battlefield of Cyberspace: The Inevitable New Military Branch – The Cyber Force*, 18 ALB. L. J. SCI. & TECH. 293, 301 (2008).

[5] Andy Greenberg, *Obama's Concerned an AI Could Hack America's Nukes*, WIRED (Oct. 12, 2016, 6:55 AM), https://www.wired.com/2016/10/obamas-concerned-ai-hack-americas-nukes [http://perma.cc/8L53-BMM2].

in order to prevent the next airborne lethal flu from landing on our shores.[6]

Instead of armor protecting a soldier from attack, computer scientists have to arm America's infrastructure to withstand a major cyber-attack. The days of tanks are over, now computer scientists are on the front lines protecting the State.

Richard Clarke, the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism at the National Security Council has warned of the severity of cyber-crimes against the United States: "Imagine a few years from now a President goes forth and orders troops to move. The lights go out, the phones don't ring, the trains don't move. That's what we mean by an electronic Pearl Harbor."[7] The United States is dependent on the power grid for everything from transportation to water purification, and even a short blackout has proven to create hysteria.[8] Department of Homeland Security officials have stated that "without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function."[9] As seen with the scramble to get New York City back on the grid in 2003, because the United States is on a large grid system when a disaster strikes it can take days to get back to normal capacity.[10]

On a hot summer's day in 2003, a single stroke of lightning left New York City in total darkness. [11] The blackout that followed left parts of Canada and

[6] *Id.*

[7] Tim Weiner, *The Man Who Protects America from Terrorism,* N.Y. Times (Feb. 1, 1999), http://www.nytimes.com/1999/02/01/world/the-man-who-protects-america-from-terrorism.html?pagewanted=all [http://perma.cc/ RE3W-BBJQ].

[8] Joel Siegel & Corky Siemaszko, *Blackout Hits New York City and the Northeast in 2003,* N.Y. Daily News (Aug. 13, 2015, 12:00 PM), http://www.nydailynews.com/news/national/blackout-hits-northeast-united-states-2003-article-1.2322074 (noting that in August of 2003, New York City endured a mass blackout that "stopped 50 million people in their tracks") [http://perma.cc/J2R5-A833].

[9] *Energy Sector,* Dep't of Homeland Security, http://www.dhs.gov/energy-sector (last visited Jan. 17, 2017) [http://perma.cc/ UK4Z-QBE9] (stating that the reliance of virtually all industries on electric power and fuels means that all sectors have some dependence on the Energy Sector).

[10] Jen Chung, *Huge 2003 NYC Blackout was 13 Years Ago*, Gothamist (Aug. 14, 2016), http://gothamist.com/2016/08/14/huge_2003_nyc_blackout_was_13_years.php#photo-1 [http://perma.cc/ ZGR5-DKSP].

[11] Siegel & Siemaszko, *supra* note 8. *See*, James Barron, *The Blackout of 2003: The Overview; Power Surge Blacks Out Northeast, Hitting Cities in 8 States and Canada; Mid-day Shutdowns Disrupt Millions***,** N.Y. Times (Aug. 15, 2003) http://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html [https://perma.cc/EM95-9JFV] (stating that "The office of the Canadian prime minister, Jean Chrétien, initially said the power problems were caused by lightning in New York State but later retracted that. Canadian officials later expressed uncertainty about the exact cause but continued to insist the problem began on the

the northeast without power for days. The fact that it was all caused by a single stroke of lightning could disrupt power for millions illuminates how interconnected and dependent the two nations are for electricity. This blackout halted elevators and stopped subway cars in their tracks.[12] The traffic lights dimmed, and the city that never sleeps was forced to rest.[13] Clean water became a luxury, and people filled their tubs with as much water as they could.[14] Phones and radios died out, leaving no way to communicate with emergency responders.[15] But what would happen if the lightning strike had been vicious code that disrupted the power plant? Power plants are set up to handle infrastructure disasters, but are they capable of thwarting a cyber-attack? When the same piece of code that attacked Iran's nuclear facility shut down the electricity to a nearby construction site, the entire nuclear enrichment program halted, and further damaged Iran's non-nuclear infrastructure.[16] As countries become more dependent on electricity and the Internet, they also become more vulnerable to cyber threats and the Law of Armed Conflict is unable to keep up.[17]

Countries have attempted to define what an act of war in cyberspace is,[18] and whether states should ban certain types of cyber-weapons,[19] typified by the

United States side of the border.").

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] Solce, *supra* note 4, at 302-303; Blank & Noone, *supra* note 4, at 350; Schmitt, *supra* note 4, at 894; Barnett, *supra* note 4, at 31-32.

[17] *See* David Weissbrodt, Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, 22 Minn. J. Int'l L. 347, 366-367 (2013). *See also* Mary Ellen O'Connell, *Cyber Security Without Cyber War,* 17 J. Conflict & Security L. 187 (2012); Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 2010 Duke L. & Tech. Rev. 003, at i-xxvii (2010).

[18] In 2009, NATO created the Tallin Manual on the International Law applicable to Cyber Warfare as a way to create the first steps to connect the Law of Armed Conflict with Cyber warfare. Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013), http://buprimo.hosted.exlibrisgroup.com/primo-exlore/fulldisplay?docid=ALMA_BOSU151718637500001161&context=L&vid=BULAW &search_scope=Books&tab=books&lang=en_US [hereinafter Tallin Manual] [http://perma.cc/T7GS-QFHE].

[19] When encryption first became a tool used by state and non-state actors to disrupt government and private practices, the international community created the Wassenaar Arrangement, which "promotes transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies." *What is the Wassenaar Arrangement?*, The Wassenaar Arrangement, http://www.wassenaar.org/the-wassenaar-arrangement/ (last visited Feb. 19, 2017) [hereinafter *Wassenaar Arrangement?*] [https://perma.cc/5UMG-PPKC].

creation of NATO's Tallinn Manual[20] and the Wassenaar Arrangement.[21] Many academic scholars have come forward, pleading for the international community to ban autonomous weapons,[22] while others recommend a "wait-and-see approach" to establishing customary law.[23] The problem is that states cannot apply the "wait-and-see approach" when it comes to National Security, and without clear guidelines for what constitutes an act of aggression via the Internet, the world will continue to fall victim to black hats[24] and state-sponsored hackers. Bill Woodcock, the research director of the Packet Clearing House said that "cyber-attacks are so inexpensive and easy to mount, with few fingerprints, they will almost certainly remain a feature of modern warfare . . . you could fund an entire cyber warfare campaign for the cost of replacing a tank tread."[25] Woodcock's statement does not come lightly. With computer code costing less to operate than replacing a tank tread,[26] it is going to be difficult for the ICC and the United Nations Security Council to approach how to deter states from cyber-attacks.[27]

The main issue is that the definition of war crimes under the Rome Statute does not encompass the nature of the cyber weapons,[28] and many nations are trying to create pacts to protect themselves.[29] Can a cyber-weapon cause unnecessary or prolonged suffering? If malware corrupts a State's nuclear center, does that constitute an armed conflict for the duration of the attack? Is controlling a State's internet and infrastructure tantamount to an occupation in the digital age? This paper will discuss these questions and more, but first the ba-

[20] Tallinn Manual, *supra* note 18.

[21] *Wassenaar Arrangement?*, *supra* note 19.

[22] Human Rights Watch, Losing Humanity: The Case Against Killer Robots 1-2 (2012), http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf [hereinafter Human Rights Watch] [http://perma.cc/ MN5H-E88V].

[23] Weissbrodt, *supra* note 17, at 387. *See also* Blank & Noone, *supra* note 4, at 436; Barnett, *supra* note 4, at 32; O'Connell, *supra* note 17, at 190-91; Ophardt, *supra* note 17, ¶62-63; Schmitt, *supra* note 4, at 931; Solce, *supra* note 4, at 296, 318.

[24] A black hat hacker is a hacker who hacks with malicious intent, the term comes from the old western fashion of the villains wearing black hats and the heroes wearing white hats. *See What's a Black Hat Hacker?*, PCTools, http://www.pctools.com/security-news/blackhat-hacker/ (last visited Mar. 31, 2017) [https://perma.cc/SG4R-ARYS].

[25] John Markoff, *Before the Funfire, Cyberattacks*, N.Y. Times (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html [https://perma.cc/WS5M-XJBK].

[26] *Id.*

[27] *Id.*

[28] Rome Statute of the International Criminal Court, art. 8, July 17, 1998, 2187 U.N.T.S. 3.

[29] *Wassenaar Arrangement?*, *supra* note 19.

sics of cyber-warfare must be addressed.

I. WHAT IS CYBER-WARFARE?

Cyber-warfare is the general term for collective instances of cyber-attacks against a State.[30] The definition of what constitutes as a cyber-attack remains up for debate among experts; some argue that this term is an amalgam of a variety of acts of cyber terrorism and cyber warfare, while others argue that a cyber-attack is in a separate category of cyber terrorism and warfare.[31] Despite this broad definition, many academics argue that the definition should be narrow in scope and must coincide with actual conventional weaponry aimed at targets with a degree of harm;[32] therefore, the issue with defining cyber warfare is that this term does not neatly fit within the traditional framework regarding the use of force according to International Humanitarian Law.[33] The International Criminal Court will need to broaden its definition of war crimes under Article 8 to include the new concepts of territoriality on the worldwide web as well as the new weapons of cyberspace and autonomous weaponry. [34]

When deciphering the lines between cyber-crimes, cyber-espionage, cyber-terrorism, cyber-attacks and cyber-warfare, it is important to have a basic understanding of the different levels, because this can escalate a simple attack into a war crime.

> Cyber crime . . . involves: the production of malware, the distribution of child pornography, hijacking for ransom, the sale of mercenary services . . . .[35] Cyber espionage is characterized [as] a motivation to discover sensitive information rather than that of causing harm,[36] [and] . . . can be conducted by an individual or a collective with the goal of pecuniary gain or stra-

[30] *How Does Cyber Warfare Work?*, FORBES TECH, (July 18, 2013, 12:45 PM), http://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/#e88b49133c34 [https://perma.cc/N84W-F63B].

[31] Ophardt, *supra* note 17, ¶ 8. *See also Marching Off to Cyberwar*, THE ECONOMIST (Dec. 4, 2008), http://www.economist.com/node/12673385 [hereinafter *Marching Off to Cyberwar*] [http://perma.cc/PU8H-9NZL]; Ethan Zuckerman, *Misunderstanding Cyberwar in Georgia*, REUTERS (Aug. 16, 2008, 1:50 PM), http://www.reuters.com/article/reutersEdge/idUSGOR66065320080816 [http://perma.cc/6S3U-4VEV].

[32] Ophardt*, supra* note 17, ¶ 8.

[33] *Id.* ¶ 1.

[34] *How Does Cyber Warfare Work?*, FORBES TECH, (July 18, 2013, 12:45 PM), http://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/#e88b49133c34 [https://perma.cc/N84W-F63B].

[35] Ophardt*, supra* note 17, ¶ 7; *see also* Solce, *supra* note 4.

[36] Ophardt*, supra* note 17, ¶ 8.

> tegic military advantage.[37] Cyber terrorism . . . is intended to influence an audience or motivate a government through threats and violence.[38]

Both cyber terrorists and hackers working on behalf of a State use malware to destroy physical targets as well as targets in cyberspace.[39] This leads to an important question, if a non-physical weapon such as code destroys a non-physical object, then can the victim respond using force?

As previously mentioned, cyber-warfare can include the following: defending information and computer networks, deterring information attacks, denying an adversary's ability to defend networks, engaging in offensive information operations against an adversary, or dominating information.[40] The issue with defining a cyber-attack separately from an act of cyber terrorism or warfare is that an armed attack can escalate from a simple virus to a massive State-crippling hack.[41] Oftentimes, it is impossible to determine the actors behind the attack, such as in the example of the first publicized cyber weapon, Stuxnet.[42] The designers of this groundbreaking software rendered it impossible to determine if the attackers were acting on behalf of a State, many States, or non-State actors.

II. CYBER WARFARE: THE NEW BATTLEGROUND

Each new war brings a new challenge to the armies: the trenches of the Somme, the hill at Agincourt, the tunnels of Cu Chi in that they all forced the troops to adapt to the land in order to fight. But what about when the battlefield is invisible? When the battleground is in a State's network, the greater the network integration of a State's infrastructure, the greater the vulnerability.[43] The Law of Armed Conflict must broaden its definition of warfare to allow for the adjustment of the new age of cyber-warfare. The Internet allows for an entirely new battlefield because the combatants do not need to physically meet in order to carry out an attack.[44]

[37] *Id.*

[38] *Id.*

[39] *Hacker*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/hacker (defining "hacker" as "a person who illegally gains access to and sometimes tampers with information in a computer system") [http://perma.cc/8M7W-RPT7].

[40] STEVEN A. HILDRETH, CONG. RESEARCH SERV., RL 30735, CYBERWARFARE 1 n.3 (2001); BLANK & NOONE, *supra* note 4, at 132.

[41] *See Marching Off to Cyberwar*, *supra* note 31.

[42] Zetter, *supra* note 3..

[43] Barnett, *supra* note 4, at 22; Ophardt, *supra* note 17, ¶ 10; Schmitt, *supra* note 4, at 893-94.

[44] This is accomplished because of the far reach of the Internet as well as the use of similar software throughout the world.

The combination of the Internet's global reach and the uniformity of the software creates the largely anonymous world-wide access, thereby allowing the triggering of botnet[45] attacks from any computer with internet connectivity.[46] For example, a non-State aggressor could control hundreds of botnets stationed around the globe, which would be ready to be implemented in a Distributed Denial of Service (DDoS) attack similar to those used against Estonia and Georgia. Alternatively, a non-State aggressor could have donated its services in the spirit of nationalistic motivations, such as seen in the cyber-attacks suffered by Georgia.[47] These types of cyber-attacks defy the simple categorization of traditional weaponry currently used in international humanitarian law. The Rome Statute needs to broaden Article 8 to be applicable to such acts of cyber war crimes and cyber weapons.[48] The first and most notable instances of cyberwarfare occurred in Georgia.

A. Georgia: the First International Armed Conflict with Cyber Attacks

Before the world media was dominated by images of Russia's invasion of Georgia, a security researcher in the United States was watching Georgia being attacked by an invisible army. This security researcher was Jose Nazario of Arbor Networks, and the cyber-attack he witnessed against Georgia's infrastructure was a DDoS.[49] This specific DDoS attack caused an overload of requests that systematically shut down Georgia's Internet servers.[50] DDoS attacks do not require tanks, bullets, or boots on the ground; all this attack requires are computers. This attack is far more devastating than a simple denial of service attack and it is extremely difficult to defend against.[51] The computers used in a DDoS attack are oftentimes controlled remotely through previous security holes, such as malware infections.[52] The importance of this specific DDoS attack against Georgia is that this is the first cyber-attack that has ever

[45] Ophardt, *supra* note 17, ¶ 21 (explaining that botnets allow a cyber attacker to implement a coordinated attack from numerous locations, including within the target network, with very limited warning for a nominal cost).

[46] *Id.*

[47] *Id.*

[48] *See id.* ¶ 68.

[49] Markoff, *supra* note 25.

[50] *Id.*

[51] Ophardt, *supra* note 17, ¶4. (noting that Denial of Service attacks require only one computer compared to a DDoS attack).

[52] Malware is commonly defined as computer code and software designed with malicious intent. *Malware*, OXFORD ENGLISH DICTIONARY, https://en.oxforddictionaries.com/definition/malware (last visited Feb. 17, 2017) [https://perma.cc/MF7T-N72H].

coincided with an armed attack, specifically gunfire during an armed conflict.[53] The ICC would be able to prosecute the aggressors behind these attacks because they took place during an armed conflict, but as with the conflict in Estonia, it is impossible to determine if code counts as a weapon and if the attack was carried out by the Aggressor State.

Georgia is another example of how one cyber-attack can threaten an entire nation, eventually weakening it and leaving it open to physical attacks such as bombings and invasion. In addition to the DDoS attacks that left Georgia's Internet infrastructure crippled, there was additional evidence that Internet traffic was being redirected through Russian telecommunications only one week prior to the cyber-attacks.[54] SecureWorks, a computer security firm, noticed that in the days before the armed conflict multiple computer researchers witnessed botnets being "staged" in preparation for the attack, and were activated before the Russian air strikes began.[55] The DDoS attack left Georgia's government unable to efficiently communicate with its citizens and neighboring states, and according to the Law of Armed Conflict, this could potentially be considered part of an occupation.[56]

Under Article 42 of the 1907 Hague Regulations, occupation occurs when the territory is "placed under the authority of the hostile army. The occupation extends only to the territory where such authority has been established and can be exercised."[57] Common Article 2 establishes that once a territory is occupied then the four Geneva Conventions apply.[58] According to the International Committee of the Red Cross, "occupation exists whenever a party to a conflict exercises some level of authority or control within foreign territory" which effectively means that once the occupier cuts off communication from the host's government, controls the Internet which in turn controls everything from hospital machinery to power plants, by controlling the Internet the occupier con-

[53] *See* Markoff, *supra* note 25.

[54] *See id.*

[55] *Id.*

[56] *Id. See* Int'l Comm. of the Red Cross, The Law of Armed Conflict: Lesson One 10-1 (2002), https://www.icrc.org/eng/assets/files/other/law1_final.pdf [https://perma.cc/X37R-474D]. The Russian Business Network ("R.B.N.") is a criminal gang based out of St. Petersburg, Russia. The R.B.N. has been linked to many online criminal activities such as malware, identity theft, child pornography, spam, and phishing scams.

[57] Hague Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, art. 42, Oct. 18, 1907, 36 Stat. 2277, T.S. 539 [hereinafter 1907 Hague Regulations].

[58] Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Member of Armed Forces at Sea art. 2, Aug. 12, 1949, 6 U.S.T. 3217, T.I.A.S. No. 3363, 75 U.N.T.S. 85 [hereinafter Geneva Convention II].

trols the territory.[59] The opposition to the ICRC's commentary follows the approach that occupation exists only once a party to a conflict is effectively able to "exercise sufficient authority over enemy territory to enable it to discharge *all* of the duties imposed by the law of occupation."[60] In other words, this provides a loophole for a State to cut off power to a city or an entire state without having the duties imposed by the Geneva Conventions when serving as the occupying force.[61] Common Article 2 of the Geneva Conventions states that "[t]he Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance."[62] In other words, when a State takes control of part of a State's territory, then they have entered into occupation which triggers the rights listed in Geneva Convention IV, and when a State disregards these rights then that State has committed a war crime.

However, there is a major problem when determining occupation by means of a cyber-attack. In order for a State to be occupied, there has to be an obvious Occupier. When the Internet for the State is being controlled by a belligerent force and all communication with local government is cut off, then it is clear there is occupation. But how can the United Nation Security Council or the International Criminal Court determine who is the occupying State when it is nearly impossible to tell who is carrying out such attacks over the Internet? Georgia blamed the Russian government, but Russia claimed the attacks were the Russian Business Network, which is to say it would be impossible to hold a

[59] *Occupation and International Humanitarian Law: Questions and Answers*, ICRC (Apr. 8, 2004), https://www.icrc.org/eng/resources/documents/misc/634kfc.htm [https://perma.cc/9RL8-BJ43].

[60] *Id.* See also, DEPARTMENT OF DEFENSE, Department of Defense Law of War Manual, 735 (2015). http://archive.defense.gov/pubs/Law-of-War-Manual-June-2015.pdf.

[61] The 1907 Hague Regulations and the Fourth Geneva Convention establish the duties of the occupying power. *See* 1907 Hague Relations, *supra* note 57, at arts. 42-56; Geneva Convention Relative to the Protection of Civilian Persons in Time of War arts. 27-34, 47-78, Aug. 12, 1949, 6 U.S.T. 3516, T.I.A.S. 3365, 75 U.N.T.S. 287 [hereinafter Geneva Convention IV]. Food and medical supplies may be requisitioned exclusively for the use of the occupation forces and administration personnel themselves (i.e., not for purposes of export outside of the occupied territory and not for the benefit of anyone beyond the occupying personnel, unless necessary for the benefit of the population under occupation itself) and only if the needs of the civilian population have been taken into account. *Id.* at art. 55. The occupying power may seize any movable property, belonging to the state, which may be used for military operations. *See* 1907 Hague Regulations, *supra* note 57, at art. 53. The occupant does not acquire ownership of immovable public property in the occupied territory, since it is only a temporary administrator. Subject to restrictions regarding their exploitation and use, it can nevertheless make use of public property, including natural resources, but it must safeguard their capital value, in accordance with the law of usufruct. *See id.* at art. 55.

[62] Geneva Convention II, *supra* note 58, at art. 2.

non-entity responsible for humanitarian aid since the occupier is unknown.[63] The International Criminal Court could not determine who to hold accountable for occupation since it would be nearly impossible to determine who the Occupying State is.

B. Estonia: The First Nonphysical Armed Conflict

When the Soviet Union and the Communist government of East Germany raised the Berlin Wall, their goal was to cut off East Berlin from outside fascist items such as food and even their own families.[64] How could Russia control a territory without raising another wall? Simply by controlling the territory's Internet.

Estonia suffered a massive series of DDoS attacks in 2007, immediately following the Estonian government's resolution to transfer a bronze statue of a World War II-era Soviet soldier from Tallinn.[65] The Estonian government was prepared for protests, and Hillar Aareliad, the director of Estonia's Computer Emergency Response Team, stated: "if there are fights on the street, there are going to be fights on the Internet."[66] Estonia is as reliant on the Internet as it is for running water, the people use the Internet for everything including communicating with their government, investing, banking, and even buying groceries.

Director Aareliad's prediction was correct, what followed the removal of the statue was a three-week long battle in cyberspace that strained the Estonian government to defend the entire State from a debilitating data flood assumed to be from Russia.[67] What makes identifying the attacker so difficult in cyberwarfare is that there are few, if any footprints, no key identifiers that can point to a particular Non-State aggressor or State, and if a piece that is traced to a State is found then it is easy to deny. Some Estonians stated that one of the Internet addresses used in the attacks belonged to an official under the admin-

[63] *Id*. *See supra* text accompanying note 56.

[64] *Berlin Wall*, HISTORY, http://www.history.com/topics/cold-war/berlin-wall (last visited Mar. 12, 2017) [https://perma.cc/TL85-76L4].

[65] *See* Mark Landler & John Markoff, *In Estonia, What May Be the First War in Cyberspace*, N.Y. TIMES (May 28, 2007), http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html [hereinafter Landler & Markoff, *Estonia I*] [https://perma.cc/EKK6-X8SA].

[66] *Id.*

[67] *See* Ian Traynor, *Russia Accused of Unleashing Cyberwarfare to Disable Estonia*, GUARDIAN (May, 16 2007), https://www.theguardian.com/world/2007/may/17/topstories3.russia [https://perma.cc/H4TP-FNTE].

istration of Russian President Vladimir Putin.[68] Gadi Evron, the Israeli expert who wrote the "postmortem" of the cyber-attack stated: "I don't think it was Russia, but who can tell? The Internet is perfect for plausible deniability."[69] The ICC can prosecute if these attacks are considered to be war crimes, which requires that there is an armed conflict. This should have been recognized as an International Armed Conflict (IAC) because an IAC exists where there is a "resort to armed force between two or more States" even if one Contracting Party is not aware or nonresponsive to the Conflict.[70] However, because it is impossible to determine who the aggressors are and if the attacks are even physical enough to be considered as a war crime in an armed conflict, it is vital that the definition of armed conflict be broadened to include nonphysical acts of war. The International Criminal Court and the UN Security Council must establish a broader definition of armed conflict, because otherwise without this there can be no punishment for a State engaging in a cyber-attack that cripples another State.

The cyber-attacks against Estonia were DDoS attacks, which clogged the State's websites with data, congesting Estonia's routers, switches, and even direct traffic on the network.[71] After the first wave of DDoS attacks, the hackers then infiltrated computers worldwide with bots, which when banded together were able to create zombies.[72] In one example, the hacker unleashed a single "huge burst of data to measure the capacity of the network"[73] as if throwing a rock into a cave to listen to how deep the cave is, and then after a few hours, "data from multiple sources flowed into the system, rapidly reaching the upper limit of the routers and switches."[74] These attacks were only the first to come, as this was just week one.

[68] *See* 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 [hereinafter Landler & Markoff, *Estonia II*] [https://perma.cc/Q9N4-J3X9].

[69] *Id.*

[70] *See, e.g.*, Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

[71] Landler & Markoff, *Estonia II*, *supra* note 68.

[72] *Id.* Zombies are essentially the common term for a computer that acts on behalf of a single controlled computer, similar to how a foot soldier doesn't act on his own but on the behalf of his commander. *Zombie*, PCMAG, http://www.pcmag.com/encyclopedia/term/55227/zombie (last visited May 14, 2017) [https://perma.cc/E2KM-RDPM].

[73] Landler & Markoff, *Estonia II*, *supra* note 68.

[74] *Id.*

The week of Victory Day[75] Internet traffic spiked to about a thousand times its average amount, which caused Hansabank, Estonia's largest bank, to shut down its online service for over an hour, resulting in about one million in losses.[76] Arbor Networks, an expert Internet Security firm in Michigan, stated:

> The 10 largest assaults blasted streams of 90 megabits of data a second at Estonia's networks, lasting up to 10 hours each. That is a data load equivalent to downloading the entire Windows XP operating system every six seconds for 10 hours.[77]

In other words, these attacks were powerful and crippling to both the private and government infrastructures in Estonia. This extreme use of botnets was the first time in history that a cyber-attack ensnared other countries in the use of its actions, such as seen by the use of botnets around the world. [78] This in turn spawned NATO to question if it needs to modify its commitment to a collective defense, and if so what would constitute an act of war and what would be reasonable as the right to defend.[79]

The attacks on Estonia were catastrophic. Estonia's defense minister, Jaak Aaviksoo, said during an interview: "It turned out to be a national security situation."[80] "It can effectively be compared to when your ports are shut to the sea."[81] The attacks were partially successful in shutting down Estonia's digital infrastructure, congesting the websites of Estonia's government officials, and blocking Estonia's largest bank as well as several of Estonia's news sites. The digital infrastructure of a State is now as vital as physical infrastructure, and if the attackers against Estonia had succeeded, the country would have been weakened to the point of its demise. The attack on Estonia illustrates for the world that there is a new vulnerability for States: the more reliant a State is on the Internet and electricity, then the more damaging a cyber-attack could be. There is no question, the most dangerous threat to a State is online.

[75] *Id.* Victory Day is the Russian holiday to mark the Soviet Union's defeat of Nazi Germany. *Russians Enjoy a Victory Parade,* HISTORY, http://www.history.com/this-day-in-history/russians-enjoy-a-victory-parade (last visited on Mar. 31, 2017) [https://perma.cc/5UJ7-PWUS].

[76] Landler & Markoff, *Estonia I*, *supra* note 65; Ophardt, *supra* note 17, ¶ 21 (Botnets—infected computers—"can be rented for close to four cents a machine, providing the equipment needed for a DDoS attack to any paying party for use against any desired target.").

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] *Id.*

C. The Reusable Bomb

Hollywood movies such as War Games[82] and Hackers[83] have dramatized the notion of a computer virus destroying democracy and the economy, but little did the filmmakers know that their daydreams of cyber warfare would turn into reality. In 2009, Iran had the shocking revelation that it was enduring an armed conflict unknowingly more than a year.[84]

Stuxnet is known as the "most complex malware ever written," and it is also infamous as the world's first cyber-weapon.[85] In June 2009, someone either working on behalf of a State or a non-State actor, had unleashed a "sophisticated" and "destructive" worm[86] that had been traveling between computers in Iran with the intent of sabotaging the country's uranium enrichment program. This was done in order to impede the country's production of nuclear weapons.[87] Stuxnet was not detected until a year after its release, and it was discovered because of a security check when a worker realized an infected computer was caught in a reboot loop, which shuts down and restarts the computer despite individuals trying to control it manually.[88] The discovery team realized that the worm infecting the computers was using a "zero-day exploit" to spread the worm.[89] The main issue here is whether or not this can be considered to be an armed attack, or if it can be considered as necessary for international humanitarian law to keep the peace.

Stuxnet was able to begin its attack when an infected USB flash drive was inserted into a computer, and as Windows Explorer completed an automatic scan of the contents of the USB stick, the exploit code awakened and clandes-

[82] *War Games. Dir. John Badham. MGM, 1982.*

[83] *Hackers*. Dir. Iain Softley. By Rafael Moreu. Perf. Jonny Lee Miller, Angelina Jolie, and Fisher Stevens. MGM/UA Home Video, 1996.

[84] Prosecutor v. Tadic, Case No. IT-94-1-AR72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) ("An armed conflict exists whenever there is a resort to armed force between States.").

[85] Zetter, *supra* note 3.

[86] *Id. See Worm*, TECHTERMS, http://www.techterms.com/definition/worm (last visited May, 14, 2017) (A "worm" is "a type of computer virus that replicates itself but does not alter any files on your machine"; it "can replicate themselves and travel between systems without any action from the user.") [https://perma.cc/Q44U-8K8E].

[87] Zetter, *supra* note 3.

[88] *Id.*

[89] *Id.* A "zero-day exploit" is the most lethal tool of hackers. Zero-day exploits take advantage of the vulnerabilities in software that are yet unknown to the software maker or the security companies. Zero-days are rare; it takes immense skill to find vulnerabilities and to exploit them. "Out of more than 12 million pieces of malware that antivirus researchers discover each year, fewer than a dozen uses a zero-day exploit." *Id.*

tinely dropped a sizeable, partially encrypted file onto the computer.[90] This worm can be seen as an attack on Iran, much like when Russia put boots on the ground in Georgia. In order to analyze the type of attack that Stuxnet caused, it is important to note that cyberspace is not classified as territory within a country. It is possible to hack into a computer network server, or to shut down electricity through malware, but the insertion of a USB flash drive cannot be considered as threatening the territory of a State. However, under the same analysis as dropping foot soldiers into a State, the bringing of an infected USB flash drive into a protected area such as a nuclear facility should logically be considered as entering a State's territory with the purpose of mass destruction and harm. This is why the ICC needs to 1) recognize this as an armed conflict and 2) expand the Rome Statute to include such actions as war crimes under Article 8.

The mysterious creator of Stuxnet had updated and refined the malware over time and released three different versions of this worm. One of the virus's driver files used a valid signed certificate stolen from a RealTek Semiconductor[91] in order to fool systems into believing that this worm was a trusted program from RealTek.[92] "Internet authorities quickly revoked the certificate. But another Stuxnet driver was found using a second certificate, this one stolen from JMicron Technology, a circuit maker in Taiwan that was — coincidentally or not – headquartered in the same business park as RealTek."[93] It is still up for question if the hackers physically broken into the companies to steal the certificates, or if they were able to hack them to steal the company's digital certificate-signing keys.[94] ESET, a security firm that found one of the certificates, stated on its blog: "We rarely see such professional operations. . . . This shows [that the attackers] have significant resources."[95]

The average zero-day sells on the black market for $100,000 USD, and Stuxnet utilized four.[96] Finding one piece of malware that uses one zero-day exploit takes tremendous skill, but using four was unheard of until Stuxnet.[97]

[90] *Id.*

[91] RealTek is a hardware maker in Taiwan. *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id. See also,* Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, Wired, (April 17, 2015) https://www.wired.com/2015/04/therealdeal-zero-day-exploits/ [https://perma.cc/5T95-575F].

[97] Zetter, *supra* note 3. *See also,* Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, Wired, (April 17, 2015) https://www.wired.com/2015/04/therealdeal-zero-day-exploits/ [https://perma.cc/5T95-575F].

The worm remained dormant within the computer until it found its targets, which were the main centrifuges that spun nuclear material at Iran's enrichment facilities.[98] Stuxnet is the first weapon made entirely out of code—this is the world's first weapon that cannot be held or dispersed by the use of man without a computer. [99] Stuxnet also managed to damage the Bushehr Nuclear Facility in Iran, which was under construction when Stuxnet was discovered.[100] Iran came forward and stated that if they started the plant, then Stuxnet could lead to the destruction of their electricity across cities.[101] In the wake of Stuxnet, Iran called for hackers to join the Iranian Revolutionary Guard, which in 2011 was considered to be the "second largest online army."[102] If the ICC does not recognize an online army as capable of threatening the territory of a State, then the ICC cannot prosecute the actions of this online army if they commit war crimes.[103]

The war crimes Stuxnet committed are not on the level of the horrors seen by the ICC, but shutting off the power to a State and occupying without overseeing the humanitarian relief of the citizens should be taken just as seriously. As previously mentioned, when a State occupies a territory, then the occupying State is responsible for all humanitarian oversight which includes everything from running water to ensuring the government can communicate with the citizens. Civilians and civilian objects are protected from being targeted as military objectives,[104] but what if the military targets a nuclear power plant that

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] Hungry Beast, *STUXNET: The Virus that Almost Started WW3*, YOUTUBE (June 8, 2011), http://www.youtube.com/watch?v=7g0pi4J8auQ [https://perma.cc/5GE3-LYTA].

[103] "[A]rmed conflict exists whenever there is a resort to armed force between States." Prosecutor v. Tadić, Case No. IT-94-1-AR72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

[104] Article 52 reads:

> 1. Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives as defined in paragraph 2.
>
> 2. Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.
>
> 3. In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling

cuts off all power to the hospitals in the city? Is making the hospital inoperable the same as bombing it?

The ICC, if able to prosecute, would need to first determine who created this weapon that caused so much destruction to Iran's infrastructure. Stuxnet is believed to be Israeli based due to references in the code to the Talmud and the day of death of an Israeli spy; however, the issue is not who created it, but who will redesign it. [105] Stuxnet is an open source weapon, which allows hackers to download the code and make it their own.[106] Stuxnet has the potential to shut down oil pipelines and to wipe out electrical grids. The use of code to create physical destruction is now possible thanks to the creators of Stuxnet. It begs the question which should be brought before the ICC and the next conference in 2017: should the creator be prosecuted for a war crime because this code much like an army carrying out attacks based on orders from its commander?

Stuxnet was designed to hit one specific target. This worm goes through a series of checks, like a fingerprint process, to probe. Stuxnet was complexly written to find a piece of equipment used only in Iran's nuclear facility despite entering so many computers and networks.[107] This worm was searching for this exact piece of equipment on a specific floor of a specific nuclear facility in Iran. In other words, this was an extremely complex code written with the intent to target only this plant. When the worm was able to speed up the centrifuges, the operations were unable to realize that there was even a problem with the centrifuges, because Stuxnet was able to mask the error.[108] The International Atomic Energy Agency stated that between 1000-2000 centrifuges were removed, and people concluded that Stuxnet succeeded.[109] The computer experts behind this attack are assumed to come from a government agency because it is politically motivated.[110] The worm did not steal identities or money, and targeted to such specificity that the creators have to have had extremely detailed insider information.[111]

The President of Iran downplayed the attack and the damage it caused and

> or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts art. 52, June 8, 1977, 1125 U.N.T.S. 27 [hereinafter Geneva Convention IV, Protocol I].

[105] Zetter, *supra* note 3.

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.*

stated that enemies of the State carried out the attack. [112] The goal of Stuxnet was accomplished, and even though Stuxnet was intended to be undetected for years and delete itself, it was able to increase the turnover of centrifuges that ultimately set back Iran for several years.[113] Former Director of the National Secuirty Agency General Michael Hayden in an interview with 60 Minutes stated: "When you use a physical weapon, it destroys itself and the target if it is done properly. A cyber weapon doesn't"[114] which makes this a weapon that can be used and reused by anyone capable of understanding the complex code. In other words, Stuxnet and other cyber weapons are similar to a bomb that explodes but is not itself damaged.

There are four phases of Stuxnet: 1) when the thumb drive is inserted, it is commanded to spread on its own 2) then when it discovers the proper computers it is able to, while 3) evading detection, 4) disrupt the centrifuges.[115] While Stuxnet used seven different mechanisms to spread, the above average worm will use up to four.[116] Stuxnet was able to attack the software in printer software and Windows Remote Procedure Call Service[117] because it was not secure.[118] It attacked the Siemans Step7 software, which is used to process industrial machines; the Programmable Log Controller (PLC)PLC actually runs the centrifuges.[119]

The computers run the database, and are able to see any errors, but the database kept its default name and password. Stuxnet used the default password to drop itself into the computer.[120] The Siemans Step7 software has database files

[112] *Id.*

[113] *Id.*

[114] *CBS News: 60 Minutes: Stuxnet: Computer worm opens new era of warfare* (CBS television broadcast Mar. 4, 2012).

[115] Zetter, *supra* note 3.

[116] *Id.*

[117] Also known as RPC, this is a service that allows two computers to talk to each other to perform a command. By replacing dedicated protocols and communication methods with a robust and standardized interface, RPC is designed to facilitate communication between client and server processes. The functions contained within RPC are accessible by any program that must communicate using a client/server methodology. *How RPC Works*, TECHNET (Mar. 28, 2003), https://technet.microsoft.com/en-us/library/cc738291(v=ws.10).aspx [https://perma.cc/ZB3P-D774].

[118] Zetter, *supra* note 3.

[119] STEP 7 basic software is the standard tool for the SIMATIC S7, SIMATIC C7, and SIMATIC WinAC automation systems. It enables the user to use the performance capability of these systems, which prides itself as being convenient and easy to use. *See SIMATIC Step 7 Professional*, SIEMENS, http://w3.siemens.com/mcms/simatic-controller-software/en/step7/step7-professional/pages/default.aspx (last visited, May 14, 2017) [https://perma.cc/76YW-33QQ].

[120] *Dissecting Stuxnet*, CISAC STANFORD, (May 8, 2012),

containing logic for the PLC, Stuxnet embedded itself into a data file, and when copied, it spreads. In addition, if just one Stuxnet threat on a network can reach the internet to install an update, then it will update itself on the network even if the network is disconnected. This was unthinkable and because of this brilliance, even the best cyber-security companies did not think to come up with the proper tools to prepare for this type of attack. Stuxnet was so ahead of its time that it is comparable to the use of machine guns during the Great War when troops were still using horses.

If there is a computer in an air gap, then there are ways to get to it, such as a USB flash drive, or a shared printer. [121] To gain control of the system, the worm had to use zero-days exploits. Stuxnet verifies that the discovered Programmable Logic Controller ("PLC") is controlling at least 155 total frequency converters, which means Stuxnet had a specific target. Stuxnet downloads a set of malicious logics to the PLC. This was groundbreaking, because a threat had never occurred on both Windows and a PLC. Whoever launched this attack built a threat on a Windows computer and an entirely different system.[122]

Essentially, someone created a weapon that can speak two different computer languages, which is like having a bullet that can seamlessly fit all guns. Stuxnet raised and lowered the rate of the speed of the centrifuges, and then would sleep for 27 days. Stuxnet's code also accounted for the fail-safe fault, which meant that if someone hit the plant's shutdown button, nothing would happen.[123] Stuxnet's authors signed the program with certificates, which means the authors stole the encryption keys from RealTek Corporation. If hackers could distribute a payload to spread quickly, and then hurt the hardware, it could have infrastructural outage, which could take months to repair what is left after the attack.

So how can a piece of computer code be analyzed under the Rome Statute to be a use of force, a weapon of attack, or an attack on an undefended place? Stuxnet can't be considered a war crime because there is no evidence of what State is responsible, and if it really was Israel, it is unsure if it will even fall under jurisdiction of the ICC. If cyberspace is considered to be an undefended location, then the act of Stuxnet spreading from computer to computer to reach

http://www.youtube.com/watch?v=DDH4m6M-ZIU [https://perma.cc/84GD-YHVE].

[121] An air-gap refers to computers or networks that are not connected directly to the internet or to any other computers that are connected to the internet. Many companies insist that a network or system is sufficiently air-gapped even if it is only separated from other computers or networks by a software firewall. Such firewalls can be breached if the code has security holes or if the firewalls are insecurely configured. Kim Zetter, *Hacker Lexicon: What is an Air Gap?*, WIRED (Dec. 08, 2014, 10:15 AM), http://www.wired.com/2014/12/hacker-lexicon-air-gap/ [https://perma.cc/6B59-EYXY].

[122] Landler & Markoff, *Estonia I*, *supra* note 65.

[123] *Id.*

its target could be considered a crime. But the right of self-defense does not exclude offensive measures, such as protecting one's servers or preventing others from creating nuclear weapons.[124] While the prevention of an arms race is not an intuitively defensive action, NATO reasoned that in order to prevent a massive, catastrophic incident, it is necessary to better construe what can and what cannot be measured as a defensive tactic in cyberspace, which is what led to the creation of the Tallinn Manual.[125] The conclusion when analyzing if Stuxnet is a war crime by the ICC depends entirely on whether a piece of code, which is not physical and cannot be destroyed upon usage, is even a weapon in the defined terms of the Rome Statute.[126] In order to protect future States from being attacked, like Georgia and Iran, there needs to be broader definitions of what is and what is not an act of war in cyberspace.

The most dangerous aspect of Stuxnet is not that it dismantled a nuclear reactor for years while going undetected, but that it does not destroy itself like other weapons. When the atomic bomb landed, it created an explosion. This bomb was the first in its kind, and the physics behind it could only be obtained by the ones who created it. Cyber weapons are much different because once they carry out their mission, they are still alive in the sense that they are not obliterated upon impact. The millions of lines of code within Stuxnet is alive and floating around in cyberspace, which makes this the first reusable bomb. Governments will now have to cope with creating a weapon that upon use can be reused by anyone on the Internet. Just like with the scale of methods and means of warfare in the Law of Armed Conflict, using a cyber weapon and having it incapable of completely deleting itself upon use will have to be weighed.

D. Japan v. China: The David and Goliath of the Pacific

While much of the world's cyber-attacks are centered in Eastern Europe and the Middle East, Japan has endured the most number of cyber-attacks in a single year. [127] The National Institute of Information Communications Technology (NICT) conducted a study on the frequency of cyber-attacks, and found that Japan experienced more than 25 billion cyber-attacks in 2014, with 40 percent of them traced back to China, followed by South Korea, Russia, and the United

[124] *See* North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

[125] *Tallinn Manual Process*, NATO COOPERATIVE CYBERDEFENSE CTR. OF EXCELLENCE https://ccdcoe.org/tallinn-manual.html (last visited Mar. 12, 2017) [https://perma.cc/FS9U-K6DX].

[126] Rome Statute of the International Criminal Court (Rome, 17 July 1998) UN Doc. A/CONF.183/9 of 17 July 1998, *entered into force* 1 July 2002.

[127] Franz-Stefan Gady, *Japan Hit by Cyberattacks at an Unprecedented Level*, DIPLOMAT (Feb. 20, 2015), http://thediplomat.com/2015/02/japan-hit-by-cyberattacks-at-an-unprecedented-level/ [https://perma.cc/CW2W-B377].

States.[128] In August 2014, the United States joined Japan to create the US-Japan Cyber Defense Policy Working Group based at the Pentagon, which is co-chaired by the Japanese Ministry of Defense and U.S. Department of Defense. The topics centered around capacity for building cyber defenses, and information sharing.[129]

A few months later, Japanese Prime Minster Shinzo Abe, Australian Prime Minister Tony Abbott, and President Barack Obama met in Brisbane, Australia, during the G20 Leaders' Summit pledging their "firm commitment to deepen the already strong security and defense cooperation" especially in cyber capacity building."[130] During this meeting, the topics of discussion remained on cyber defense and information sharing as well as the Interim Report on the Revision of the U.S.-Japan Guidelines for Defense Cooperation, released in October 2014. This report emphasized that Washington and Tokyo will deepen their cooperation on cyber-security by sharing information on cyber threats and vulnerabilities.[131] In December 2014, the Japanese government met with the French government for a cyber-dialogue in Paris discussing critical infrastructure protection, the establishment of international norms, and joint efforts towards cyber-security capacity building.[132] Shortly after this visit, Japan met with Estonia to open up a cyber-dialogue between the two states with a similar agenda as the previous meetings.[133]

Japan responded to the mass influx of attacks by building partnerships with key nations to establish a cyber-defense pact. Japan sees cooperation with Europe on cyber-security in particular as more important than ever.[134] In a commitment in the Cyber-Security Strategy, Japan pledges to, "actively participate in the promotion of the Convention on Cybercrime" by assisting countries to become State Parties to the Budapest Convention and by conducting defense capacity-building activities. [135] The Budapest Convention is the formal name of the Convention on Cybercrime, and the only binding international instrument on cybercrime.[136] It serves as a guideline for any state developing legisla-

[128] *Id.*

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] INTERNATIONAL STRATEGY ON CYBERSECURITY COOPERATION: J-INITIATIVE FOR CYBERSECURITY, INFO. SECURITY POL'Y COUNCIL JAPAN 5 (2013), http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf [hereinafter INFO. SECURITY POL'Y COUNCIL JAPAN] [http://perma.cc/ 8TPQ-MZ44].

[136] *Budapest Convention and Related Standards*, COUNCIL OF EUROPE, http://www.coe.int/en/web/cybercrime/the-budapest-convention (last visited Mar. 17, 2017)

tion against cybercrime, and also serves as a framework for international cooperation between states party to this treaty.[137]

Japan's effort is partially based on a new cyber-security strategy adopted in June 2013. In their strategy, the Japanese government strongly supports a free, open and secure Internet, as well as the multi-stakeholders approach in governing the Internet.[138] The strategy outlines four basic aims: 1) "Ensuring Free Flow of Information," 2) "Responding to Increasingly Serious Risks," 3) "Enhancing of Risk Based Approach," and 4) "Acting in Partnership on Shared Responsibilities."[139] This strategy places a premium on cooperation with concurring countries, as depicted in the strategy outlining Japan's international strategy on cyber-security cooperation, compiled by the Information Security Policy Council, which is the lead agency on cyber-security issues in Japan.[140]

Japan is already part of various regional and international cyber-security cooperation initiatives on both the technical as well as the political level, such as the UN Group of Governmental Experts on Cyber-security.[141] Japan's actions reflect recent tensions in the Pacific, with China looming as they reach agreements with free nations to establish pacts to keep their virtual borders secure and free from oppressive regimes. The Internet has grown from a way for scientists to share data to a necessity for the citizens to exercise basic human rights. Like the Arab Spring, people are able to pierce the veil of their government's façade to show the world what truly lies behind the curtain.

II. WAR CRIMES IN CYBERSPACE

In order to promote security and deter States from cyber-attacks, the Rome Statute needs to expand Article 8 to include what can qualify as a war crime in cyberspace, specifically if the Internet is considered to be an undefended place.[142] If the threat of cyber-attacks is to be taken seriously by the ICC, then

[http://perma.cc/ K7JX-UK9F].

[137] *Id.*

[138] Franz-Stefan Gady, *Japan and Europe Step Up Cooperation in Cyberspace,* DIPLOMAT (January 13, 2015), http://thediplomat.com/2015/01/japan-and-europe-step-up-cooperation-in-cyberspace/ [http://perma.cc/ J977-6GYY]; CYBERSECURITY STRATEGY: TOWARDS A WORLD-LEADING, RESILIENT AND VIGOROUS CYBERSPACE, INFO. SECURITY POL'Y COUNCIL JAPAN 3 (2013), http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf [http://perma.cc/T5CB-AVM5].

[139] Gady, *supra* note 138.

[140] *Id.*; INFO. SECURITY POL'Y COUNCIL JAPAN, *supra* note 135.

[141] Gady, *supra* note 138.

[142] As listed in Rome Statute of the International Criminal Court, Article 8, "war crimes" include the following:

> (i) Willful [sic] killing;

the ICC needs to discuss the inclusion of acts of aggression under the jurisdiction of the ICC. In addition to including acts of aggression, which would expand to crimes committed in a State's Internet territory, the ICC also needs to broaden the war crimes listed in Article 8 of the Rome Statute because the current definitions of war crimes are too narrow to expand to cyber-attacks and cyber warfare. Even if the ICC expands its definitions under Article 8, there needs to be a further review on how to find the identities of the attackers and how the victim state can recover from the harm done.

International humanitarian law has regulated what weapons are unlawful based on the legality of the weapon system itself. Article 35(2) of Additional Protocol I states that these unlawful weapons are bound by customary international law.[143] What makes a weapon "unlawful" is if it causes "superfluous injury or unnecessary suffering."[144] As the Wassenaar Arrangement seeks to label certain lines of code as a weapon, it begs to question: How can code cause superfluous injury or unnecessary suffering?

There is an important factor when analyzing a cyber-attack as a war crime, and this is that there are distinctions between cyber-attacks and computer attacks. The two major distinctions that define a computer attack are 1) a computer attack may cause interference with fundamental information systems, which cause extensive difficulties to a target state but does not pose a direct threat to life, and 2) the cyber-attacks which directly threaten or appear to threaten life.[145] While hacking into a target State's official government website

> (ii) Torture or inhumane treatment, including biological experiments;
> (iii) Willfully [sic] causing great suffering, or serious injury to body or health;
> (iv) Extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly;
> (v) Compelling a prisoner of war or other protected person to serve in the forces of a hostile Power;
> (vi) Willfully [sic] depriving a prisoner of war or other protected person of the rights of fair and regular trial;
> (vii) Unlawful deportation or transfer or unlawful confinement;
> (vii) Taking of hostages.

Rome Statute of the International Criminal Court, *supra* note 28, at art. 8, ¶ 2.

[143] *See* Geneva Convention IV, Protocol I, Article 35 (2).

[144] INTERNATIONAL COMMITTEE OF THE RED CROSS, *Rule 70. Weapons of a Nature to Cause Superfluous Injury or Unnecessary Suffering,* https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule70 (last visited May, 15, 2017) [https://perma.cc/A2N2-FJMC].

[145] *Id.* Separate cyber cooperation agreements and dialogues exist with international organizations such as ASEAN, APEC, OECD, and NATO. *See, e.g.*, Cleveland Thomas, *Cyber Security: Collaboration,* INTERNATIONAL TELECOMMUNICATIONS UNION http://www.ctu.int/wp-content/uploads/2017/03/Cyberthreat-Public-Private-

does not directly threaten human life, the hacking of a target's electronic motoring of subway traffic system can cause fatalities.

To create a machine gun is not an act of war, it is not even an international crime. Code is not on the list of banned weapons, and code is not even considered to be a weapon. The Rome Statute focuses on war crimes, acts of aggression, and other crimes against humanity including banned weaponry,[146] but is not broad enough to include non-physical weapons such as lines of computer code. In the 1990's the Wassenaar Arrangement brought its own attack on cryptography and how defensive code could be viewed as weaponry, and the Tallinn Manual is NATO's way of expanding on the dated Rome Statute.[147]

A. The Rome Statute: How can a Cybercrime become a War Crime?

The Rome Statute is designed to protect victims and states from acts of violence through the use of deterrence. However, deterrence in the cyber world is not acknowledged when cyber-attacks and cyber warfare are not defined in the Rome Statute.[148] Can Russia's cyber-attacks against Estonia and Georgia be viewed as acts of war even though nothing physical was destroyed?[149] Can Stuxnet be defined under Article 8 of the Rome Statute to be a war crime that willfully causes great suffering?[150] In order to answer these questions, there needs to be discussion on how the Rome Statute can broaden itself to include the fluidity and ever-evolving dynamics of cyber-attacks and cyber weapons.

The ICC only has jurisdiction for crimes against humanity, war crimes, and genocide committed after July 1, 2002[151] and ICC jurisdiction must be accepted in the countries in question. Acts of aggression are included in the subject-matter jurisdiction of the ICC,[152] but the ICC can only prosecute individuals suspected of committing the crime of aggression.[153] However, based on the outcome of the Review Conference, the ICC cannot exercise jurisdiction over

Collaboration.pdf (last visited May, 15, 2017).

[146] Rome Statute of the International Criminal Court (Rome, 17 July 1998) UN Doc. A/CONF.183/9 of 17 July 1998, *entered into force* 1 July 2002.

[147] *About Us*, THE WASSENARR ARRANGEMENT (Feb. 19, 2017), www.wassenaar.org/about-us [https://perma.cc/XUW8-HFTC].

[148] Rome Statute of the International Criminal Court (Rome, 17 July 1998) UN Doc. A/CONF.183/9 of 17 July 1998, *entered into force* 1 July 2002.

[149] *See generally* Markoff, *supra*, note 25.

[150] Rome Statute of the International Criminal Court, *supra* note 28 at art. 8, ¶ 2(a)(iii). *See generally* Ralph Langner, *Stuxnet's Secret Twin,* FOREIGN POLICY (Nov. 19, 2013), http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/ [https://perma.cc/BHT4-WPMD].

[151] Rome Statute of the International Criminal Court (Rome, 17 July 1998) UN Doc. A/CONF.183/9 of 17 July 1998, *entered into force* 1 July 2002.

[152] Rome Statute of the International Criminal Court, *supra* note 28 at art. 5, ¶ 1(d).

[153] *Id.* at art. 25, ¶ 1.

the crime of aggression without a further decision to take place after January 1, 2017.[154] This means that if the United States was involved in Stuxnet, then they can become a member state but still opt out in order to best protect its nationals. To determine if the ICC can prosecute the cyber-attacks similar to those in Georgia and Estonia, these attacks would need to qualify as war crimes under Article 8 of the Rome Statute.

Article 8 of the Rome Statute focuses on war crimes such as the destruction of property and the attack of undefended places.[155] The Statute is meant to provide order and justice to the international community, but without broadening to include the ever-changing realm of the Internet and technological advances then international communities are left vulnerable to the continuance of cyber-attacks such as what occurred in Estonia and Georgia. Article 8 (2)(a)(iv) of the Rome Statute states: "[the] extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly" constitutes a war crime. In both attacks on Estonia and Georgia, their web sites and their financial sectors were severely clogged to the point where citizens could not access their bank accounts. [156] The hackers had no military need to attack the government websites or to threaten the traffic systems, but this act can be seen as excessive destruction because of how unjustified it was in order to accomplish their goals of weakening both States. Georgia's war illuminates how cyber-attacks that impacted civilians and government created a weakened State which allowed for Russia to make their first moves to invade.

Stuxnet is another example of how one weapon was able to cripple Iran's nuclear infrastructure without physically setting foot into Iran. The Stuxnet malware created extensive destruction of property but can be seen as created within the law.[157] The worm is malicious software, but there is no type of illegal software named by the ICC or within treaties such as the Convention on Certain Conventional Weapons and the Geneva Protocol. In fact, code is not even considered to be a weapon under the banned weapons treaty.[158] The

[154] Stephanie Maupas, *After 15 years, ICC States Still Debating Crime of Aggression*, JUSTICE INFO, http://www.justiceinfo.net/en/component/k2/after-15-years,-icc-states-still-debating-crime-of-aggression.html (last visted May, 15, 2017) [https://perma.cc/GKS7-Z4WK].

[155] *Id.* at art. 8, ¶ 2(a)(iv), art. 8, ¶ 2(b)(v).

[156] Landler & Markoff, *Estonia I*, *supra* note 65; Ophardt, *supra* note 17, ¶ 21 (Botnets—infected computers—"can be rented for close to four cents a machine, providing the equipment needed for a DDoS attack to any paying party for use against any desired target.").

[157] Langner, *supra* note 148.

[158] Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (Protocol IV, entitled Protocol on Blinding Laser Weapons)

Rome Statute needs to broaden this definition of unlawful destruction in order to include cyber weapons capable of mass destruction.

In order to promote security and deter States from cyber-attacks, the Rome Statute must be amend Article 8 to include what can qualify as a war crime in cyberspace, specifically if the Internet is considered to be an undefended place. Article 8 (2)(b)(v) of the Rome Statute[159] lists as war crimes attacks on undefended places, and the five elements to determine what qualifies as an attack on an undefended place are:

> 1) The perpetrator attacked one or more towns, villages, dwellings or buildings, 2) Such towns, villages, dwellings or buildings were open for unresisted occupation, 3) Such towns, villages, dwellings or buildings did not constitute military objectives, 4) The conduct took place in the context of and was associated with an international armed conflict, 5) The perpetrator was aware of factual circumstances that established the existence of an armed conflict.[160]

Here it is apparent that in order to be considered an "undefended place" the place must be physical. How can this apply to that of a cyber-attack against a State's information operation centers? For clarification, the category of information operations consists of any "operation[] to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[161] These elements can be found in various types of war crimes, such as tampering with a State's mass transit system causing subway trains to crash into each other or setting up barricades to limit the ability for information to enter and leave a target state through the internet.[162] The physical attack on the subway trains can be viewed as an attack of an undefended place under Article 8 (2)(b)(v), but the initial attack on the computer systems controlling the subways cannot be treated as a war crime against an undefended place because the Internet does not have territorial guidelines that can confine it to a "place" as described within the Rome Statute.[163]

(Vienna, 13 Oct. 1995) UN Doc. CCW/CONF.I/16 Part I), *entered into force* 30 July 1998.

[159] *Id.* at art. 8, ¶ 2(b)(v).

[160] *Id. See also*, INTERNATIONAL CRIMINAL COURT ELEMENTS OF CRIMES part II. B., https://www.icc-cpi.int/NR/rdonlyres/336923D8-A6AD-40EC-AD7B-45BF9DE73D56/0/ElementsOfCrimesEng.pdf [https://perma.cc/AHB2-RH67].

[161] Schmitt, *supra* note 4, at 888.

[162] John F. Murphy, *Computer Network Attacks by Terrorists: Some Legal Dimensions* 5 (Vill. U. Sch. L. Pub. L. & Legal Theory Working Paper Series, Paper No. 2000-1, 2000), http://ssrn.com/abstract=208671 [http://perma.cc/ 55VJ-48AJ].

[163] *See* INT'L COMM. OF THE RED CROSS, THE LAW OF ARMED CONFLICT: LESSON ONE 10-1 (2002), https://www.icrc.org/eng/assets/files/other/law1_final.pdf [https://perma.cc/X37R-474D].

The cyber-attacks Russia directed at Georgia can be seen as crimes committed in war based on the severity of shutting down Georgia's connection to the Internet and nearly severing the State's entire electrical grid. However, according to Article 8(2)(b)(v) because the Internet is not considered to be a place, and there are no definitions for territory applicable to the Internet, Russia's actions will go unpunished and Georgia and other States are left unable to use any type of defensive strike against Russia in the wake of an imminent cyber-attack.

B. The Tallinn Manual

In 2009, the NATO Cooperative Cyber Defense Centre of Excellence hosted an independent International Group of Experts (the "Experts") to produce a manual on the law governing cyber warfare.[164] After the terrorists attack on September 11, 2001, terrorism diverted attention from cyber warfare until the massive cyber attacks against Estonia and a year later in Georgia during its armed conflict with Russia in 2008, as well as cyber weapon used to destroy Iran's nuclear centrifuges in 2010.[165] When the customary international laws were formed, cyber weaponry was far from the horizon and there has been no update t assure that in the event of another cyber armed conflict that there will be swift repercussions and that other States can assist with defending without escalating the attack.[166]

The United States attempted to solve the question of how to apply international law to cyberspace, and the result was "long-standing international norms guiding State behavior – in times of peace and conflict – also apply in cyberspace," but the US understood that technology was evolving faster than the law, and so they added that the *International Strategy for Cyberspace* acknowledges that 'unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.'[167]

The scope of the Tallinn Manual encompasses both the *jus ad bellum*, the international law governing the resort to the use of force, and *the jus in bello*, which is the law in war.[168] Within this manual, the question of legality con-

[164] An international military organization based in Tallinn, Estonia was accredited in 2008 by NATO as a "Centre of Excellence" (hereafter referred to as "NATO CCD COE"). Tallinn Manual, *supra* note 18, at 1. The Tallinn Manual is not an official document, but is only the product of a group of independent experts acting solely in their personal capacity. The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. The authors of the Tallin Manual are known as the "Experts." *Id.* at 11.

[165] *Id.* at 1-2.

[166] *Id.* at 3.

[167] *Id.*

[168] *Id.* at 4.

cerning cyber intelligence is examined only as it pertains to *jus ad bellum*, or as if it applies in the context of an armed conflict governed by the *jus in bello*.[169] The Experts unanimously concluded that the "general principles of international [humanitarian] law can apply to cyberspace,"[170] but just because the Experts believe that IHL can apply to cyberspace does not mean that if one of the Parties to the Conflict commit a war crime that they would be prosecuted by the ICC, or that they have certain guidelines to stay within, such as what cyber weapons they can use and what scale to use when determining methods and means of cyber warfare. The Tallin Manual has zero authority, no states have signed this to mean it to be taken as law, and in the case of a cyber armed conflict there is nothing to hold any State accountable for their actions.[171] By not uniting under the Tallin Manual to write this into International Humanitarian Law, the international community is effectively allowing for States to attack one another without any fear of repercussions.

C. The Wassenaar Arrangement

The Wassenaar Arrangement, also known as Export Controls for Conventional Arms and Dual-Use Goods and Technologies, is presently composed of 41 countries and focuses on the regulation of export controls.[172] These export controls are implemented by each individual Participating State. Although the scope of export controls in Participating States is determined by Wassenaar Arrangement lists, practical implementation varies from country to country in accordance with national procedures.[173] While the United States has its rules based within the Wassenaar Arrangement, other countries are in the process of developing their own rules around the Wassenaar Arrangement, potentially putting researchers overseas in the same troubled boat as those in the US.[174]

In December 2013, the arms control list was updated to encompass certain surveillance and intelligence-gathering software.[175] This marked the first time

[169] *Id.*

[170] TALLINN MANUAL, *supra* note 18, at 5.

[171] TALLINN MANUAL, *supra* note 18, at 1. The Tallinn Manual is not an official document, but is only the product of a group of independent experts acting solely in their personal capacity. The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. The authors of the Tallin Manual are known as the "Experts." *Id.* at 11.

[172] *About Us*, THE WASSENARR ARRANGEMENT (Feb. 19, 2017), www.wassenaar.org/about-us [https://perma.cc/XUW8-HFTC].

[173] *Id.*

[174] Kim Zetter, *Why an Arms Control Pact Has Security Experts Up in Arms*, WIRED (June 24, 2015, 7:00 AM), https://www.wired.com/2015/06/arms-control-pact-security-experts-arms/ [https://perma.cc/JQA7-XFBM].

[175] *Id.*

the Wassenaar Arrangement implemented controls on software since it restricted the export of certain types of encryption products in 1998.[176] The Wassenaar Arrangement specifically calls for export restrictions on systems, equipment, and components that are designed to generate, operate, deliver, or communicate with "intrusion software."[177]

The United States Department of Commerce recommended easing export controls after a joint study with the National Security Agency found that the export restrictions harm businesses within the United States.[178] The Wassenaar Arrangement does not restrict intrusion software itself, just the command and delivery systems that install or communicate with intrusion software.[179] This can be interpreted to encompass exploit codes, which are codes that hackers use against vulnerabilities in systems to install malicious tools, such as intrusion software.[180] Despite the rules agreed upon in the Wassenaar Arrangement, the Department of Commerce has said that exploits are not covered under the Wassenaar Arrangement; therefore, the exploits to the intrusion software are accepted.[181]

The good news for the security community is that anti-virus scanners would not be controlled. Nor would technology "related to choosing, finding, targeting, studying and testing a vulnerability," according to Randy Wheeler, director of the Bureau of Industry and Security, in June 2015. [182] This means "fuzzers" and other programs used by researchers would not be impacted by the Wassenaar Arrangement.[183] Exploits also would escape being banned by the Wassenaar Arrangement, but products that have zero-day exploits or rootkits in them or that have built-in capability for using zero-days and rootkits with them, would be automatically denied for export. The problem with this, however, is that the United States Department of Commerce has yet to define what

[176] *Id.*

[177] *Id.* Intrusion software is defined as anything designed to "avoid detection from monitoring tools or to defeat protective countermeasures," which can also modify or extract data from a system or modify the system. *Id.*

[178] *Overview per country*, BERT-JAAP KOOPS (Feb. 2013), http://www.cryptolaw.org/cls2.htm [https://perma.cc//FU8X-Y6KS].

[179] Zetter, *supra* note 174.

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] *Id.* Fuzzing is an art of automatic bug finding, which is to discover and identify software implementation faults. A fuzzer is a program that injects automatically semi-random data into a program or a stack to detect viruses or malware. *Fuzzing*, OWASP, https://www.owasp.org/index.php/Fuzzing (last visited Feb. 19, 2017) [https://perma.cc/9XXV-3ECZ].

it means by zero-day and root kit.[184] Under the proposed rules some penetration-testing tools would be controlled if they contain zero days. For example, The Metasploit Framework is a tool distributed by the US company Rapid7 that uses multiple types of exploits to test systems, including zero-days.[185] What does this mean? Simply that these penetration testers, commonly referred to as "pen-testers," would be punished for doing their job, which is to test the protection of a network or an isolated computer.[186] To punish a pen-tester for detecting security faults would be the same as punishing a security guard for fixing flaws in the building she protects.

Before malware could take down a nuclear power plant, the main focus of the international community was cryptography. In 1993, the Clinton Administration announced the Escrowed Encryption Initiative (EEI), usually referred to as the Clipper Initiative, after its first implementation in the Clipper chip.[187] A classified, secret-key algorithm, SKIPJACK, has been implemented in an Escrowed Encryption Standard (EES).[188] "The reported basic idea of the EEI is to provide citizens with a safe cryptosystem for securing their communications without threatening law enforcement."[189] "The EES procures law enforcement access by means of a Law Enforcement Access Field (LEAF) that is transmitted along with each encrypted message; the field contains information identifying the chip used."[190]

> Law enforcement agencies wire-tapping communications encrypted with EES can decipher tapped messages by obtaining the two parts of the chip's master key that are deposited with two escrow agencies (National Institute of Standards and Technology and the Treasury Department's Automated Sys-

[184] *See* Zetter, *supra* note 174. *See also* Margaret Rouse, *Rootkit*, SEARCH MIDMARKET SECURITY (Jan. 31, 2008), http://searchmidmarketsecurity.techtarget.com/definition/rootkit?vgnextfmt=print ("A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network.") [https://perma.cc/C4PM-DR2F].

[185] Zetter, *supra* note 174.

[186] Definition of pen-testing: "Penetration testing (pen-testing or pentesting) is a method of testing, measuring and enhancing established security measures on information systems and support areas." *Penetration Testing (Pen- Testing)*, TECHNOPEDIA, https://www.techopedia.com/definition/16130/penetration-testing-pen-testing (last visited May, 15, 2017) [https://perma.cc/DLD5-CL83].

[187] *Wassenaar Arrangement / COCOM*, CRYPTO LAW SURVEY, http://www.cryptolaw.org/cls2.htm (last visited Mar. 12, 2017) [https://perma.cc/455U-F665].

[188] *Id.*

[189] *Id.*

[190] *Id.*

> tems Division), provided they have a court order for the tapping.[191]

D. Autonomous Weapons and Extraterritorial Killings

Extrajudicial killings are illegal under the Law of Armed Conflict. To kill someone without giving them the chance to surrender or the right of self-defense is an improper application of the Law of Armed Conflict, but what about when a target is killed by a drone or by a robotic soldier?

Before extrajudicial killings by robots and drones are examined, it is important to understand how the Law of Armed Conflict establishes lawful targets. In the Law of Armed Conflict, there are four core principles that must be met in order to have a lawful targeting mission, those four are as follows: distinction, military necessity, unnecessary suffering, and proportionality. [192] Distinction is simple to understand, as the established target must be known. Military necessity must be a tactical gain for the opposing side to dissimilate. Unnecessary suffering and proportionality are similar, in that the attack must minimize collateral damage.[193]

Article 52(2) of Protocol Additional to the Geneva Conventions limits attacks to only military objectives, specifically only to "objects which by their nature, location, purpose or use make an effective contribution to military action" and "whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." [194] For brief clarification, an "attack" is an act of violence against the opposition forces, and this can either be defensive or offensive.[195] Article 52 does not differentiate between an international armed conflict and a non-international armed conflict, which solidifies that a state cannot use a weapon on its own people or attack civilian objects regardless of purpose.[196]

There are four possible ways to establish if a target is a military objective under Article 52 of Additional Protocol I, and those four are the following: Nature, Location, Purpose, Use. Nature means the essence of the target, basically whatever the opposing force uses to carry out their operations, which is intrinsic in the entity itself.[197] Location refers to ports, capitals, borders, or any nat-

[191] *Id.*

[192] *See* Geneva Convention IV, Protocol I, Article 48, 52(2), 57.

[193] Statute of the International Criminal Court, U.N. Doc. A/CONF.183/9, Article 8, par. 2(a)(iii) (July 17, 1998).

[194] *See* Geneva Convention IV, Protocol I, *supra* text accompanying note 104.

[195] *See id.* at art. 49.

[196] *See* Geneva Convention IV, Protocol I, *supra* text accompanying note 104.

[197] LTC RICHARD P. DIMEGLIO, JA, USA MAJ SEAN M. CONDRON, JA, USA MAJ OWEN B. BISHOP, JA, USAF MAJ GREGORY S. MUSSELMAN, JA, USA MAJ TODD L. LINDQUIST, JA, USA MAJ ANDREW D. GILLMAN, JA, USAF MAJ WILLIAM J. JOHNSON, JA, USA MAJ DANIEL E. STIGALL, JA, USAR , LAW

ural location used for military objectives as seen in the use of hills in the Korean War. Purpose refers to the future use of the object, but it can be superseded by Use. Use refers to the intended use of an object, such as how a school is not a target but becomes one when it is used as a training camp for forces. [198]

One major concern is that technology will replace soldiers entirely, which is already seen in drones taking pilots out of the warzone. Human Rights Watch, and the International Human Rights Clinic at Harvard Law School, published *Losing Humanity: The Case against Killer Robots*.[199] Human Rights Watch's position on them is forceful and unambiguous:

> "Fully autonomous weapons would not only be unable to meet legal standards but would also undermine essential non-safeguards for civilians. [Therefore, they] should be banned and . . . governments should urgently pursue that end."[200]

The main flaw with Human Rights Watch's argument is that they do not see the distinctions in International Humanitarian law's ban on weapons *per se* and weapons that are unlawful on the use of certain otherwise legal weapons. A tank is not banned, but the use of the tank can be unlawful if it is used in genocide or just on one civilian. But, weapons like biological weapons can never be used lawfully because its nature is banned. Because the Human Rights Watch takes the nature out of the weapon ban for autonomous weapons, Michael Schmitt argues in his criticism of their report that their "analysis fails to take account of likely developments in autonomous weapon systems technology or is based on unfounded assumptions as to the nature of the systems . . . much of *Losing Humanity* is either counter-factual or counter-normative."[201] This call for banning autonomous weapons when none exist is impeding the creation of any type of autonomous weapon that could minimize collateral damage in war-

OF ARMED CONFLICT DESKBOOK 35 (2012) https://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2012.pdf [https://perma.cc/T6HW-59X4].

[198] *Id.*

[199] Michael N. Schmitt*, Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, HARV. NAT'L. SECURITY J. FEATURES (2013), http://harvardnsj.org/wp-content/uploads/2013/02/Schmitt-Autonomous-Weapon-Systems-and-IHL-Final.pdf [http://perma.cc/AV4E-6DXH].

[200] *See* HUMAN RIGHTS WATCH, *supra* note 19. *See also* Jeffrey S. Thurnher, *No One at the Controls: Legal Implications of Fully Autonomous Targeting*, 67 JOINT FORCE Q. 77 (2012); Markus Wagner, Comment, *Taking Humans Out of the Loop: Implications for International Humanitarian Law,* 21 J. L. INFO. & SCI.: SPECIAL EDITION: THE LAW OF UNMANNED VEHICLES 155 (2011/2012); Kenneth Anderson & Matthew Waxman, *Law and Ethics for Robot Soldiers*, HOOVER INST.: POL'Y REV. (Dec. 1, 2012), http://www.hoover.org/research/law-and-ethics-robot-soldiers [http://perma.cc/VZY9-ELU6]; Landler & Markoff, *Estonia I*, *supra* note 65; Schmitt, *supra* note 199.

[201] Schmitt, *supra* note 199, at 3.

fare.

Before examining the law of armed conflict and how autonomous weapons should be classified, it is important to understand that a weapon system is, which is simply a weapon and the items associated with its use and purpose.[202] The Department of Defense of the United States defines an autonomous weapon as "a weapon system that, once activated, can select and engage targets without further intervention by a human operator."[203] This portion of the definition alone would exclude drones, since an individual controls them. However, the Department of Defense further defined autonomous weapons to include "human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation."[204] This is broad enough to include drones as well as to include defensive weapons such as Israel's Iron Dome, which is able to automatically target and destroy incoming rockets.

Weapons that, by nature, cause superfluous injury or unnecessary suffering are banned under Article 35(2) of Additional Protocol I to the 1949 Geneva Conventions, and is also confirmed in customary law. [205] Because this is customary international law, it binds States that are not Party to the Protocol. This Article essentially bans any method of warfare that creates unnecessary suffering or superfluous injury, which extends from combatants to civilians. What is left out is if these weapons are also banned during a non-international armed conflict, but since it is customary international law that certain weapons—such as biochemical weapons—are unlawful then this ban still applies.

One danger presented by autonomous weapons is the element of distinction between civilians and military targets, such as in indiscriminate attacks. Article 51(4) of Additional Protocol I states that indiscriminate attacks are prohibited, and defines indiscriminate attacks as those:

> "(a) which are not directed at a specific military objective; (b) which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction."[206]

[202] *Id.*

[203] U.S. DEP'T OF DEF., DIRECTIVE 3000.09: AUTONOMY IN WEAPON SYSTEMS (2012).

[204] *Id.*

[205] *See* Geneva Convention IV, Protocol I, Article 35(2)

[206] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, INT'L

This simply means that in the process of targeting, the target must be a military objective and it must be proportional to achieve the goal. Article 48 of Additional Protocol I requires only military objects to be targeted and the prohibition on indiscriminate attacks are addressed in Additional Protocol I, Article 51(4) as not meeting a military objective as in Article 52 of Additional Protocol I, and if the attack is carried out with the knowledge that the civilian population or a civilian object is affected.[207] Article 35 of Additional Protocol I dealt with known weaponry, but this Article left no room to adapt new means of warfare, and simply states that the basic rules for weapons is that: 1) In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited; 2) It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering; 3) It is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment.[208]

Article 36 of Additional Protocol I expands on Article 35 and requires that in the development or the study of new weaponry, a High Contracting Party is then under the obligation to determine if it would be prohibited by treaty or by international law.[209] This allows for weapons such as malware to be used; however, this does not ban certain code or malware including the encryption code banned by the Wassenaar Arrangement. The danger of Article 35 is that the weapon used is at the discretion of the High Contracting Party, meaning that since the weapon used is new technology, then it will be considered either lawful or unlawful *per se* based on the damage and suffering it creates after it is used in the armed conflict.

Civilians are protected from targeted killings, unless and for such a time that they take a direct part in hostilities. Article 51(4) explains that indiscriminate attacks are prohibited. Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which

COMM. OF THE RED CROSS, https://www.icrc.org/ihl/WebART/470-750065 (last visited Mar. 12, 2017) [https://perma.cc/B89N-JLYJ].

[207] Geneva Convention IV, Protocol I, *supra* note 104.

[208] Geneva Convention IV, Protocol I, *supra* note 104.

[209] *Id*. Article 36 states:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

Id. at art. 36.

cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.[210] *De facto* expansion of Article 51(3) is often illustrated when a missile fired by a drone kills a terrorist not involved in a firefight.

Article 53(5) is problematic for the new wave of warfare. Article 53(5) defines indiscriminate attacks as (a) an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects; and (b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[211] So after understanding how International Humanitarian law establishes what is and what is not legal in armed conflict, it is important to apply these laws to current advancements in technological warfare.

On November 12, 2015, Amnesty International published ten reasons the U.N. needs to ban "killer robots."[212] The first reason to ban such autonomous weapon systems is to be preemptive because this is no longer science-fiction as seen in the ShadowHawk drone by Vanguard Industries. This drone is frightening to Amnesty and other human rights groups, because it can be armed with a grenade launcher, a shotgun with laser designator, or less-lethal weapons such as a Taser or bean-bag round launcher.[213] This fear focuses on a human's ability to take a drone and attach a weapon to it, but no matter what happens a drone is always at the control of a programmer. This fear can be easily squelched by holding humans accountable for what weapons they can use, which, as mentioned before, is customary international law.

Amnesty claims that by allowing a robot or machine to kill or use force is an "assault on human dignity."[214] Rasha Abdul Rahim explains that by allowing "robots to have power over life-and-death decisions crosses a fundamental moral line. They lack emotion, empathy and compassion, and their use would violate the human rights to life and dignity." [215] While drones, other machines, and even software lack intrinsic senses of emotion and compassion, they can

[210] *Id.* at art. 26.

[211] *Id.*

[212] Rasha Abdul Rahim, *Ten Reasons Why It's Time to Get Serious About Banning 'Killer Robots'* AMNESTY INT'L (Nov. 12, 2015, 11:14 AM), https://www.amnesty.org/en/latest/news/2015/11/time-to-get-serious-about-banning-killer-robots/ [http://perma.cc/PR6X-NEYW].

[213] *Id.*

[214] *Id.*

[215] *Id.*

be programmed to follow complex logic problems. While a robot can essentially have the capabilities of following the logic behind ethics and morality, it is against international law to have extrajudicial killings, as previously mentioned, and he also mentions that robots cannot follow international law.[216] Mr. Rahim's criticism is based on an incorrect assumption of how computer programs work. A gun is a machine, a tank is a machine, a drone is a machine. Machines are operated, and there is little difference, if any, between an operator and a computer programmer. To say that a gun kills someone is to take the human operator out of the equation and thereby frees one from liability of the machine one controls. "Killer Robots" are at the mercy of how they are programmed, and computer code does not create itself unless its programmer gives it guidelines to do so.

Amnesty claims that according to the "Drone Paper" by The Intercept, "90% of people killed by U.S. drone strikes were unintended targets."[217] A bomb hits more than its intended target, and that is because bombs are used to create mass destruction. A drone can take many forms, but when in an armed conflict unfortunately there will be collateral damage. This comes from the law of armed conflict, in times of targeting a military objective or an individual, there are tests that need to be used before striking. When the target is of mass importance, then the collateral damage unfortunately increases. Drones are not fool proof, but neither are bombs. The only way to avoid collateral damage is to end armed conflicts.

The concern of most critics regarding autonomous and semi-autonomous weaponry is that there is not enough emotional intelligence in these weapons, and that only human soldiers should be able to make the life or death decisions in war because combatants cannot surrender to a robot, they cannot plead with a robot, they cannot be detained by a robot alone. [218] The response to that criticism is simple: drones and other autonomous and semi-autonomous weapons are used when carrying out a targeted killing, so therefore the drone should be viewed just as a sniper and his rifle.

There is immense value to creating autonomous weapons. Replacing a soldier in the battlefield with a robot would mean that there would be little loss of life. One key example would be replacing soldiers with robots at military checkpoints: here instead of a young soldier sweltering under the desert sun carrying about 85lbs of equipment and on edge looking out for the next threat, a robot could take her place and instead work under a program to evaluate each car and passenger, and then either lock the threat or let the car through the barricade. The issue with robots replacing soldiers is the same issue facing President Obama's drone strikes in the Middle East, which is the notion that drone

[216] *Id.*

[217] *Id.*

[218] *Id. See supra,* note 172 and accompanying text.

strikes are extrajudicial killings. Drones are considered semi-autonomous, since individuals operate them and can override the controls. Before drones were used, fighter jets and snipers were utilized in the battlefields to take out military targets, and there was never an outcry that the soldiers were far removed from the enemy for it to be considered indiscriminate.

Drones, when used in armed attacks, are remotely operated weapon systems, which means they are constantly under human command and control when in the process of identifying targets. The main difference between a drone and an aircraft is that the drone is built to be able to hover over a target for hours, even days, which would be impossible with a human pilot. Drones should be viewed as a rifle in the eyes of the international community because by nature, a drone is not a weapon that produces unnecessary suffering. There are many ways a rifle can be used unlawfully, such as killing a civilian, but a rifle can be made and used lawfully as well, and so too can a drone. But when examining the extraterritorial targeting by the use of a drone, there are two steps: determine the *jus ad bellum* (when force may be resorted) and then to establish *jus in bello* (how a drone may be used to target).

As previously mentioned, targeting killings are lawful under International Humanitarian Law, but they must be contained within an armed conflict, the victim must be a specific individual, they must be engaged directly in hostilities and must be beyond a reasonable possibility of arrest, and only a senior military officer authorizing the killing and the proportionality must be high among the authorizing commanders consideration.[219] The argument for the ban of drones typically stems from the lack of awareness that an individual constantly controls the drone. A drone is programmed just as a computer or an iPhone is programmed: a programmer writes code as another person creates the hardware, and then this combines to create a drone which can operate based solely on the program established within the code. A drone cannot operate outside of its programming, just as how a computer cannot work outside of its administrator's commands. Because the drones work within a finite program, an individual is used as its administrator to control its movements and establish where and when it will target.

Another common criticism against drones in warfare is that there is lag time between the individual giving the command to the drone and the drone processing the command.[220] This is problematic to some because it means that in a span of 15 seconds, the individual target can move or surrender or a child can wander into the area. The argument against that critique is simple: there is no

[219] Geneva Convention IV, Protocol I, *supra* note 104, at art. 51.

[220] Mark Mazzetti, *The Drone Zone*, N.Y.Times (Jul 6, 2012) http://www.nytimes.com/2012/07/08/magazine/the-drone-zone.html [https://perma.cc/47NA-86VR].

other weapon out there that operates without some type of lag time.[221] A sniper could get the command to shoot, but between the sniper responding to the go-ahead and pulling the trigger, a pregnant woman could trip and bump into the target. There are too many hypotheticals to point out when trying to articulate how slippery a slope it is to ban a drone because of lag time.

But what about computer code without the hardware? What about Stuxnet's destruction of an economic target? What about zombie bots used in DDoS attacks as seen in Estonia and Georgia? How can code be a weapon when there is no way for numbers and letters to leap off a screen and kill civilians or soldiers? Stuxnet's attack on Iran's nuclear power plant qualifies as an armed attack by an anonymous state or non-state, which is the first time in history an armed attack occurred without anyone aware of it happening or who is the exact perpetrator.

F. Moving Forward: The Shift From Offensive to Defensive

The first step to protecting consumers from careless corporate cyber security has arrived in the United States. The Cyber Security Information Sharing Act was passed by the Senate on October 27, 2015.[222] This legislation is meant to be a "comprehensive step toward securing private data networks" to prevent malicious hacking based on "cyberthreat indicators" shared by companies within one another.[223] The goal is to have companies share these cyber threat indicators with one another in order to help prevent another Sony hack.[224] Surprisingly, this legislation is not sponsored by the Department of Commerce or the Department of Homeland Security—instead this is sponsored by North Carolina Republican Richard Burr, chairman of the Senate Select Committee on Intelligence (SSCI), and Dianne Feinstein of California, the committee's

[221] *Id.*

[222] Boris Segalis, Andrew Hoffman & Kathryn Linsky, *Federal Cybersecurity Information Sharing Act Signed into Law*, DATA PROTECTION REPORT (Jan. 3, 2016), http://www.dataprotectionreport.com/2016/01/federal-cybersecurity-information-sharing-act-signed-into-law/ [https://perma.cc/ZPR6-UZY5].

[223] Gregg Levine, *Despite Privacy Concerns, Cybersecurity Bill Poised for Passage*, AL JAZERA ENGLISH (Oct. 21, 2015), http://america.aljazeera.com/articles/2015/10/26/despite-concerns-cybersecurity-bill-heads-to-vote.html [http://perma.cc/4JBH-3WK4].

[224] Sony's network was breached by the so-called Guardians of Peace, which have been assumed to be based out of North Korea. This hack came from North Korea's anger towards the Sony film "The Interview" where the Central Intelligence Agency hires two bumbling journalists to assassinate the North Korean Leader, Kim Jong-un. This is a key boogie-man story come true for corporations, since now they have seen the horrors that can come from poor security. Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED, (Dec. 13, 2014), http://www.wired.com/2014/12/sony-hack-what-we-know/ [https://perma.cc/2ZKA-2CFM].

ranking Democrat.[225]

The fear of many is that the legislation encourages companies to share personal data of its customers.[226] The argument that it would hinder the privacy rights of consumers seems valid, [227] but this argument falls flat.[228] In a free market, consumers can choose not to submit information they do not want to based on the notion that they can always choose to walk away entirely and support a different business. [229] The main problem is that the American people do not understand privacy on the Internet.

III. CONCLUSION

When the Rome Conference took place, the notion of a computer virus wiping out the entire electrical grid of a country seemed unfathomable.[230] But since the aftermath of Georgia and Estonia,[231] it is apparent how important it is to have a solidified international law concerning what is and what is not an act of warfare in cyberspace. Richard Clarke, the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism at the National Security Council has warned of the severity of cyber-crimes of war and has spoken about its gravity:

"[CEOs of big corporations] think I'm talking about a 14-year-old hacking into their Web sites. I'm talking about people shutting down a city's electricity. . . shutting down 911 systems, shutting down telephone networks and transportation systems. You black out a city, people die. Black out lots of cities, lots of people die. It's as bad as being attacked by bombs."[232]

There is no greater threat in modern times than that of a cyber-attack on a State.[233] In order to promote security and deter States from cyber-attacks, the Rome Statute needs to expand Article 8 to include what can qualify as a war crime in cyberspace, specifically if the Internet is considered to be an undefended place.

If the threat of cyber-attacks is to be taken seriously by the International Criminal Court, then the ICC needs to discuss the inclusion of acts of aggres-

[225] Levine, *supra* note 223.

[226] *Id.*

[227] *Id.*

[228] *Id.*

[229] *Id.*

[230] *See* Ophardt, *supra* note 17, ¶ 63.

[231] *Id.*

[232] *Id.*; Tim Weiner, *The Man Who Protects America from Terrorism*, N.Y. TIMES, (Feb. 1, 1999), http://www.nytimes.com/1999/02/01/world/the-man-who-protects-america-from-terrorism.html?pagewanted=all [https://perma.cc/8XAG-HCQZ].

[233] *See* Markoff, *supra* note 25.

sion under the jurisdiction of the ICC. In addition to including acts of aggression, which would expand to crimes committed in a State's Internet territory, the ICC also needs to broaden the war crimes listed in Article 8[234] because the current definitions of war crimes are too narrow to expand to cyber-attacks and cyber warfare. Even if the ICC expands its definitions under Article 8, there needs to be a further review with how to find the identities of the attackers. To this day, the people behind the attacks against Estonia and Iran are still unknown[235] and without knowing the attackers, it is impossible to determine if it falls under the jurisdiction of the ICC. If hackers are to be held accountable, and if justice for these cyber-crimes is sought, then both the ICC and global technology need to be capable of discovering the origin of the attacks as well as how to define an act of war in cyberspace.

While the International Criminal Court needs to add an amendment to Article 8 to include cyber-warfare that could leave a state powerless or without economic capabilities, the Wassenaar Arrangement is on its way to banning all means of cyber weaponry.[236] The issue is that drastically banning zero-days and exploits would prevent any type of technological advancements. Additionally, banning the advancement of technology through the use of zero-days and other encryptions could mean that the international community will suffer as a whole. On the one hand, it is noble to imagine a world in which bombs only fell over computer networks; a world so advanced that soldiers no longer need to be in the line of fire. This is the type of world that would have little actual physical violence; it would be entirely virtual. But there are associated dangers that cannot be ignored. Banks and the stock market, for example, are entirely virtual, and we would run the high risk that cyber-warfare would turn from military targets to economic targets in order to weaken the opposing state.

While the ICC needs to address how humanitarian law applies in cyberspace, the United States needs to evaluate if the risks associated with signing the Rome Statute outweigh the need for global accountability for cyber-crimes. By participating in the Wassenaar Arrangement, the United States is broadcasting its stance against cyber weapons and encryption that would make it easier for terrorist cells to communicate,[237] but by taking a backseat to the ICC the United States is allowing such attacks to go unpunished. In order to protect its invisible borders, the United States needs to be the example for other free nations to show that an act of aggression can be invisible, and that such attacks

[234] Statute of the International Criminal Court, U.N. Doc. A/CONF.183/9, Article 8, par. 2(a)(iii) (July 17, 1998).

[235] Levine, *supra* note 223.

[236] *See Wassenaar Arrangement?*, *supra* note 19. The Wassenaar Arrangement, "promote[s] transparency . . . and greater responsibility in transfers of conventional arms and dual-use goods and technologies." *Id.*

[237] *See id.*

will not go unpunished. With that said, how can the United States and other nations make the leap to putting acts of cyber warfare with that of war crimes? How can the ICC include such crimes, and how can evidentiary rules adapt to invisible trails on the Internet? Internet legal scholars might just have to "wait-and-see"[238] how the United States government handles the impending threats of cyber-attacks.[239]

Before the ICC can determine if cyber-attacks are acts of war, there needs to be an examination if two states can be in an armed conflict even if one state is unaware, such as when Iran was unaware it was being attacked for over a year by another state.[240] The ICTY defined an armed conflict existed "whenever there is a resort to armed force between States."[241] Can there be an armed conflict when one side is unaware it is being attacked? This might be the mimic of the age old question: *if a tree falls in the forest, and no one is there to hear it, did it really happen?* Another question for scholars is how targeting in international humanitarian law adapts when defending against a cyber-attack.[242] At what point can a state fight back when the attack is not physical? Can a physical attack be a proportionate response to a cyber-attack? Just as white hat hackers test weakness to better fortify firewalls, so too do legal scholars when challenging outdated laws to better encapsulate the ever-changing field of technology.

[238] Weissbrodt, *supra* note 17.

[239] *See id. See generally* BLANK & NOONE, *supra* note 4; Barnett, *supra* note 4, at 31-32; O'Connell, *supra* note 17; Ophardt, *supra* note 17; Solce *supra* note 4, at 301; Schmitt, *supra* note 4, at 894.

[240] Zetter, *supra* note 3.

[241] Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

[242] Geneva Convention IV, Protocol I, *supra* note 104, at art. 52. Article 52.2 defines a target as a military objective, which means it must make an effective contribution to the military effort and its destruction must create a definite military advantage. *Id.*