2016

# Waging Wars in Cyberspace: How International Law On Aggression And Self-Defense Falls Short Of Addressing Cyber Warfare. Could Iran Legally Retaliate For The Stuxnet Attack?

Willa Rubin
*Oberlin College*

Willa Rubin

# Waging Wars in Cyberspace: How International Law On Aggression And Self-Defense Falls Short Of Addressing Cyber Warfare.

## Could Iran Legally Retaliate For The Stuxnet Attack?

Oberlin College Politics Department
Spring 2016
Honors Candidate

First Reader: Professor Ben Schiff
Second Reader: Professor Eve Sandberg
Third Reader: Professor Benjamin Kuperman

Acknowledgments:

Many thanks to Professor Ben Schiff for his help and guidance during office hours, and for his gracious feedback on even my most inadequate previous drafts.

I want to thank my second reader Professor Eve Sandberg for her thoughtful feedback on this paper and for her incredible support as my advisor over the past four years. I would also like to thank Professor Benjamin Kuperman for answering even my silliest technical questions with kindness.

Finally, I would like to extend my gratitude to my Honors Seminar advisor Chris Howell for his encouragement throughout this process, and to my fellow Honors candidates and students from whom I have learned so much during my time at Oberlin.

# Table Of Contents:

## 1. Introduction

In Spring 2015, the Oberlin College Politics department organized a symposium on National Security and the dangers of Big Data. In an interview with student press, only political science professor Robert Jervis concluded that the biggest threat to national security was still nuclear weapons. All other panel members almost instantly cited "cyber" as the greatest threat to American security. While nuclear weapons and cyber warfare can certainly be combined, most cyber attacks—if they are even considered attacks in the first place—do not cause immediate physical damage or endanger civilians. As the Stuxnet incident shows, malignant cyber operations pose unique challenges to current international law.

There is a spectrum of what actions conducted in cyberspace can do, and of reasons it may affect US national security. The revelations from Wikileaks in 2011 and Edward Snowden in 2013 show that information can be disseminated literally with the click of a button. This may endanger people's lives on important political missions. Drones are also launched and controlled remotely over networks—but it is possible for these controls to be usurped by someone with malignant intentions. "Cyber" as a potential means for conflict has been examined by legislators: for example, President Obama established a Cybersecurity Initiative in 2009, which outlined steps and listed priorities in protecting American information and communications. Cyber conflict poses unique threats, because states are not the only actors; individuals and organizations may access classified information and leak it to the public, or cause physical destruction to critical infrastructure. Perhaps most importantly, acts that can be done through

cyberspace may endanger civilians. The capacity of cyber operations must be more closely examined in international law so that states have clearer protocol to evaluate and regulate what happens in this seemingly anarchic sphere.

This paper examines the following question: How does international law of aggression and self-defense fall short in addressing cyber warfare? I consider the Stuxnet incident from 2006-2010 as a case study, and evaluate whether Iran could retaliate against the US for attacking its nuclear facility. The Stuxnet incident has not been directly discussed in other considerations of Article 51, self-defense, and aggression. Authors like Eriksson and Giacomello have examined how traditional International Relations theories and cyber operations may intersect, but have failed to add case studies to the literature. Barring the *Tallinn Manual*, edited by Michael Schmitt, cyber operations have rarely been considered under international law. Existing literature overstates the potential for cyber conflict, and does not offer specific examples to consider cyber conflict in legal terms; the articles written tend to focus on arms control for policymakers. This paper is a case study in the Stuxnet incident, but the legal implications could also be relevant for other cyber operations of this scale.

I argue that the technical capabilities of the Stuxnet worms show that it could be considered an act of aggression under the Rome Statute and that Article 51 of the UN Charter is insufficient to address malignant cyber operations.

This paper pertains to *jus ad bellum*, or the right to wage a war, over *jus in bello*, or proper conduct during a war, as I consider whether Iran could retaliate. Determining whether the launch of Stuxnet was aggression or self-defense is central to my argument; I argue that the attack was preventive, thus illegal, and not pre-emptive, which is legal. It is

true that due to the time constraints of cyber operations, it may be the case that *jus in bello* may also be relevant; it is entirely possible for future cyber attacks to harm civilians, which would not be just conduct under Fourth Geneva Convention. However, the international legal documents I examine do not provide specific time frames beyond general phrases like "imminent attack," which makes it more difficult to ascertain the exact point when a cyber attack begins and ends. As this paper shows, Stuxnet inflicted gradual, episodic damage, which has a different impact than if, for example, the US were to bomb on Iran's nuclear facility once. Cyber operations work differently than attacks via conventional weapons. This paper demonstrates that traditional definitions and laws do not fit comfortably when considering cyber warfare.

The Stuxnet incident, launched by the US and likely Israel, took place over the four-year period of 2006-2010. When I discuss how Iran could have responded, I refer to the time period after the attack was realized in 2010. It is unlikely that Iran could claim self-defense and retaliate against the US and Israel today, six years after the attack was realized.

I used a historical approach to my methodology. I examined legal precedent concerning self-defense and aggression in cases like *US v. Nicaragua* and incidents like the US Invasion of Iraq in 2003 to show how self-defense and aggression have been applied. I also examined legal documents like the UN Charter, particularly as Article 51 is central to this paper. I looked at technical reports and news articles dissecting the Stuxnet incident. I also read books and journal articles about both international relations theory and potential cyberwarfare. These have informed my analysis as I synthesized

how international relations theory and international law may be combined when considering cyber conflicts.

I first discuss the applicability of International Relations (IR) theory, and how political scientists determine the applicability of international law. Next, I introduce technological vocabulary that is key to my paper's argument. These terms include "cyber," "operation," and "attack." I then outline the events of the Stuxnet incident. I analyze the incident given the historical and legal connotations of "aggression," and reiterate that the Stuxnet incident could not be accurately portrayed as "anticipatory self-defense." Finally, I consider how my analysis would differ had there been attribution problem—or, if Stuxnet had launched by an unknown actor. I conclude that Article 51 is insufficient to address responses to aggressive cyber operations between states.

In *Lights Out*, Koppel notes that, "where FEMA's presumed 9.0 earthquake would leave a city in rubble, with thousands of dead and injured, even the most massive cyberattack would inflict very little immediate physical damage." [1] However, he adds that a cyberattack on the continental US powergrid could trigger an intense "domino-like, cascade effect," causing electrical blackout where civilians have limited access to resources they are used to like plumbing, information, heat or air-conditioning, and so forth. [2] This paper examines how a single cyber operation—Stuxnet—highlights the unique need to re-evaluate our international legal norms, customary and codified, to deal with unconventional weapons of potential mass destruction.

---

[1] Ted Koppel. *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath* (Crown, 2015), 15.

[2] Koppel, ibid, 15.

## 2. Research Limitations

I do not discuss the role of corporate non-state actors in this paper. It is certainly worth noting that transnational corporations often have stakes in cyber security matters, but understanding their role goes beyond the scope of discussing Stuxnet as the primary case study in cyber operations; the types of operations that most affect corporate non-states actors most often concern their organization's privacy and citizens' personal data. The "Right to be Forgotten" on Google and other search engines, as is being discussed in the European Union at parliamentary and judicial levels, is crucial to understanding the continued jurisdictional issues that come with managing Internet activity. However, because it does not relate to kinetic implications for weapons of mass destruction, it is outside of the scope of this thesis.

I also do not address industrial sabotage laws in this paper. Sabotage is the deliberate destruction of another state's resource to gain a political or military advantage, which is an obvious example of intervening in another state's affairs. Sabotage takes place when one state's national security interests are directly at stake. Future cyber attacks and operations may more closely resemble sabotage than conventional weapons. However, further investigation about specific sabotage instances was beyond the scope of this paper. This paper dissects Stuxnet specifically, and laws about aggression and self-defense, both of which I felt needed to be re-evaluated most in the context of future malignant cyber operations. Stuxnet was certainly intended to sabotage the production of centrifuges at Natanz, but discussing sabotage in international law more generally was beyond the scope of this paper.

I did not cover the *jus in bello* implications of cyber attacks as much as I had originally intended to. Under the Fourth Geneva Convention, civilians are to be protected during wartime. However, definitions like "civilian" and "wartime" would both need to be reevaluated in the context of cyber operations; these would both rely on the scale of the attack in question, which could not be examined without details of a specific attack. While there is certainly tension between the US and Iran, these states are not officially at war with one another. Further, the Stuxnet incident did not directly endanger civilians. Thus, the *jus in bello* implications are beyond the scope of this paper.

This highlights a similar question raised in the paper: could a malignant cyber operation be considered an attack in international law if no civilians are directly harmed? This question is more thoroughly explored in my paper in the context of the Stuxnet incident.

## 3. Context: International Relations Theory And Types of International Law

In this section, I discuss why international law is a useful and appropriate framework to consider the Stuxnet incident.

### 3. a. Context for the International Legal System:

Most states, especially smaller ones, rely on international law to help level inequalities of power as they engage with other states. Pragmatically, cyber operations confront an existing international legal system with jurisdictional problems. The Internet notoriously has no borders, and yet we must engage with other states to determine where certain cyber activity comes from. For example: If someone in Croatia stole another person's identity and used a search engine whose server is located in Norway, if that Croatian's activity were to be traced, it would look as though the activity had been initiated in Norway. In this scenario, under both the passive personality and active personality principles of Extraterritorial Jurisdiction, Norway and Croatia would both have jurisdiction in prosecuting that crime.[3] After all, "a State may exercise control over cyber infrastructure and activities within its sovereign territory."[4] Cyberspace operates beyond state borders, but the international community functions in the context of state actors.

International law is based on the repeated behaviors of powerful states. In the nineteenth century, it was used as a doctrine "to justify acquisition of territory by colonial

[3] Michael N. Schmitt. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence*. (New York, New York: Cambridge University Press, 2013): 20.

[4] Schmitt, ibid, 15.

powers."[5] Today, it is derived from codified treaties between states, or by signing massive group treaties, like to the membership of the United Nations (UN). Customary law, or an unwritten set of rules that states almost always follow, is another form of international law. Customary law:

"evolves from state practice. It does not require the formal negotiation and express consent associated with treaties. A rule of customary international law binds all states that have not objected to the rule while it is in the process of formation."[6]

Not all international law is binding per se. Soft law is another branch of international law. This ranges from "foreign investment to telecommunications to human rights," and is also considered under the umbrella of international law, though these laws are legally nonbinding."[7] Law may also originate from specific unilateral declarations by state leaders: for example, "the United States will not commit genocide."

When conflict between states arises, it can be adjudicated at the international level. The International Court of Justice (ICJ) is the judicial branch of the United Nations, and the ICJ can weigh in on these conflicts. This was originally set up as the International Court of Arbitration under the Hague Conferences of 1899 and 1907, and later in the League of Nations. The UN may also establish additional tribunals to investigate specific conflicts. The first international tribunal to be held since the Nuremberg Trials after World War II was the International Court Tribunal for the Former Yugoslavia (ICTY). Judicial decisions from the ICJ or other tribunals are another form of international law. However, these precedents are not necessarily cumulative.

---

[5] Jeffrey L. Dunoff, Steven D. Ratner, and David Wippman. *International Law: Norms, Actors, Process: A Problem-Oriented Approach* (New York, NY: Aspen, 2010): 11.
[6] Dunoff, ibid, 36.
[7] Dunoff, ibid, 36.

I mention the types of international law because it is helpful context for understanding our international institutions. However, I draw my analysis from legal cases and codified law like the UN Charter and Rome Statute, as these are most pertinent to the subject of my paper.

3. b. The Use of International Relations Theory in International Law:

There are several different theories of International Relations (IR) that are worth mentioning in this paper. They hypothesize the motives of state behavior, and by extension, whether the actions of states can be constrained by international law.

Realists assert that states are self-interested actors who act to maximize their power and preserve their existence. They resolve that the international system is anarchic. Further, they define power as material, military capability, and believe that states can measure power in relative terms—in other words, how much more power they have than another state: "States that maximize relative power are concerned primarily with the distribution of material capabilities."[8] Classical realists like Hans Morgenthau argue the self-interested nature of actors stems from human nature. Conversely, defensive (or structural) realists like Kenneth Waltz respectively believe that anarchy drives this "self-survival" instinct.[9] They argue that anarchy itself is an ordering principle: "Structure is not a collection of political institutions but rather the arrangement of them."[10] On the other hand, offensive realists like John Meirsheimer purport that, "the structure of the

[8] John J. Mearsheimer. *The Tragedy Of Great Power Politics* (New York: Norton, 2001): 36.
[9] Mearsheimer, ibid, 15.
[10] Kenneth N. Waltz. *Theory of International Politics* (Reading, MA: Addison-Wesley Pub. 1979): 81.

international system, not the particular characteristics of individual great powers, causes them to think and act offensively and seek hegemony."[11] States gain power relative to one another; states play a zero-sum game by engaging in international relations, and relative gains from state A diminish the gains from state B. Thus, the balance of power in the international system is an important consideration.

Classical and offensive realists would argue that international law does not matter because states are self-interested and have little concern for other states that do not threaten by them. By extension, they believe that a peaceful world is unrealistic. Defensive realists would say that it matters to the extent that institutions like the UN were set up with the intention of mitigating this anarchy. In keeping with this logic, Waltz would say that states wield to international law only when it is in their interest to do so.

Liberalism is another branch of IR theory, and recognizes the potential merits of international law. Liberalists agree with Waltz, but they believed that structural realism is a choice. In other words, they argue that such attention to the structure of anarchy is malleable, because people's perceptions are malleable. Like their realist counterparts, liberalists agree that states are the primary actors in the international system, but add that a state's own internal factors influence its behavior in the international arena. Within the scope of liberalism, there are several additional theories: one is Democratic Peace Theory (DPT), which purports that democracies do not go to war with one another.[12] Other liberalists argue that economic interdependence among states makes them unlikely to fight one another. Institutionalists assert that once states start pursuing their own interests

[11] Meirsheimer, ibid, 53.
[12] Meirsheimer, ibid, 16.

with treaties, this pattern of behavior gains momentum. Constructivists add that determining what constitutes appropriate behavior in the international arena may be constructed out of self-interest, but that morals, social interactions, and other non-state actors play crucial roles in international relations as well. These various branches of liberalism see international law as important. While states may exist in anarchy, that anarchy is actively being weakened by international law; the fact that the US needs to its actions like the 2003 Invasion of Iraq using international law is hard to explain through a purely material perspective.

International political theorists and law experts are often at odds with one another because of those differing underlying assumptions about the roots of state power and in how state interactions are organized. Law is a way that institutions attempt to mitigate anarchy in the international system. Realists believe law is irrelevant, because there is no material way to enforce those laws. While the underlying assumptions about states being self-interested actors may be true, international law does appear to constrain the actions of great powers. This paper explores how that structure fits with this new form of warfare.

## 4. Understanding "Cyber" Within The Scope Of This Paper

The jargon scholars use to define "cyber," and what can be done with it, evokes a different image than the vocabulary used for other weapons of mass destruction.[13] This is partly due to many academics' inadequate understanding of what can actually happen in cyberspace. A largely hyperbolic literature suggests that most scholars and policymakers are unsure of causes and effects of cyber destruction. Eriksson and Giacomello note that the traditional notions of state sovereignty in typical international law break down in the context of cyber, because it operates beyond state borders.[14] They add that the state is less powerful now than in traditional international law, because the Internet allows people to disseminate information especially quickly without the influence of the state or traditional journalistic institutions; this gives more power to the individual and to non-state organizations.[15]

In this section, I define "cyber," and I discuss its role in outlining different types of cyber operations. As part 3.b. of this section shows, none of the known or most frequent types of operations parallel what happened in the Stuxnet attack.

### 4. a. Defining "Cyber"

Valeriano and Maness defined the term "cyber" as "computer or digital interactions" between devices.[16] By extension, "cyberspace" refers to

---

[13] It is worth noting that weapons of mass destruction and cyber attacks can certainly be combined.
[14] Johan Eriksson and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?" (*International Political Science Review* 3, 2006): 224. http://www.jstor.org/stable/20445053. Accessed July 30, 2015.
[15] Eriksson and Giacomello, ibid, 224.
[16] Brandon Valeriano and Ryan C. Maness. "Cyber War versus Cyber Realities: Cyber

"all of the computer networks in the world and everything they connect and control. It's not just the Internet . . . cyberspace includes the Internet plus lots of other networks of computers that are not supposed to be accessible from the Internet."[17]

Importantly, cyberspace does not exist outside the network of machines. Human error is more likely to take place in "air gaps." "Air-gapped" technology means there is no physical connection between two devices—say, a secure server at the White House and someone's personal computer.[18] In theory, this would keep the information stored on a secure server completely separate and impossible to access from elsewhere on the network. However, machines often thought disconnected from cyberspace may not always be disconnected in practice due to human error. When devices are linked on the same network, it makes them each more vulnerable to attack than if they had been successfully air-gapped.

"Whenever Homeland Security or the Federal Energy Regulatory Commission has hired computer forensic experts to investigate this claim, however, they have found minute connections. A Verizon/Secret Service study concluded that two-thirds of companies across a spectrum of industries didn't realize that they had been breached until someone outside the company informed them. Another study, conducted by the cyber-security firm FireEye, found that it took on average 279 days before companies that had been breached came to realize it or were told by someone else" [19]

In addition to a lack of resources, air-gapping often fails to account for human error: "Every time a worker brings in a thumb drive or laptop from home and hooks it up to an 'isolated' system, the mobility of workers bridges the air gap." [20] While not directly relevant to my paper, I mention air-gapping because it is a microcosm of how easy it is for hackers to access networks they were not meant to.

---

Conflict in the International System." (*Oxford University Press Scholarship Online*, 2015): 2. Accessed August 30, 2015.

[17] Clarke and Knake (2010: 70) cited in Valeriano, ibid.

[18] Koppel, ibid, 42.

[19] Koppel, ibid, 43.

[20] Koppel, ibid, 43.

Cyberspace exists outside of state borders, yet how the international community responds to cyber conflicts exists purely within the realm of state actors. Communications for crimes conducted in cyberspace may take place over a "virtual private network, or VPN, for secure communications," and it is often unclear where cyber operations originate from. In many cases, this renders the typical jurisdictional notions associated with state sovereignty vague and often irrelevant. [21]

4. b. Conflict Vocabulary And Frequent Types Of Operations

When weapons can operate in cyberspace, beyond the jurisdiction of states and without the typical consequences of other conventional forms of attack (for instance, one state bombing another), we must reconsider the vocabulary we use to describe the possibilities for different kinds of conflict.

Scholars often use terms like "conflict" to refer to altercations between states in cyberspace. This works well because it is a general term, and does not necessarily imply kinetic damage like the word "attack" would. Most conflicts in cyberspace do not endanger people's lives in the way that, say, a bomb would. Thus, it does not imply that direct, physical warfare as we know it would result from an altercation.[22] The term "conflict" can also be synonymous with "operation," because both are less grave than a cyber attack with a direct physical result that endangers civilians.

[21] Joel Brenner. *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World* (Penguin, 2013): 28.
[22] Valeriano, ibid, 10.

It is important to note these differences because most cyber altercations that occur—barring Stuxnet—have not resulted in physical damage. For context, most cyber operations that take place are what experts call "Distributed Denial of Service," or DDOS, operations. These involve:

"Flooding sites, servers, or routers with more requests for data than the site can respond to or process (This method shuts down the site, thereby preventing access or usage."[23]

An often-cited example of a DDOS attack is the Bronze Soldier Dispute between Estonia and Russian hackers in 2007. This took place during a political dispute between Estonia and Russia over the relocation of the Bronze Soldier of Tallinn, a Soviet statue that commemorated war graves.[24] Targets in this attack included the websites of:

"the Estonian presidency and its parliament; almost all of the country's government ministries; political parties; three of the country's six big news organizations; two of the biggest banks; and firms specializing in communications."[25]

DDOS operations are among the most common types of cyber operations, but not all cyber operations are so benign.

A more grave kind of cyber operation is an "intrusion." This includes:

"Trapdoors or Trojans are unauthorized software added to a program to allow entry into a victim's network or software program. They permit future access to a site once it has been initially intruded upon. Intrusions need to be added to software, can remain dormant for a long time, and then propagate themselves without notice...They only become malicious once they become operational." [26]

Intrusions "must be installed by a user and are implemented at the whim of a hacker's command (Northcutt 2007). An operator can install the malicious program at one point in

[23] Valeriano, ibid, 10.
[24] Ian Traynor. "Russia accused of unleashing cyberwar to disable Estonia." *The Guardian*, May 16, 2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia
[25] Traynor, ibid.
[26] Valeriano, ibid, 10.

time and then activate it at a later date." [27] The purpose of these intrusions is primarily to "steal sensitive information from secured sites," including personal information of civilians. [28] The US Department of Defense has declared the use of infiltrations are an act of war. [29] Viruses and worms that affect many computers are both forms of intrusions. Viruses are: "programs that need help by a hacker to propagate and can be attached to existing programs in a network or act as stand-alone programs (they generally replicate themselves with the intention of corrupting or modifying files)." Worms do this as well, but can also self-propagate." [30]

Advanced Persistent Threats (APTs) are another kind of infiltration method. The intentions of APTs are:

"usually are more malicious and advanced and almost certainly come from states, and their targets are much more specific. The level of sophistication is unmatched, meaning highly covert and intentional state action is behind the malicious intent, making APTs the most likely to evoke strong, negative, and escalatory reactions from the target state if and when discovered." [31]

The *Tallinn Manual* notes that cyber operations often pose danger. They note that some of the most common cyber crimes are:

"Cyber espionage, theft of intellectual property, and a wide range of criminal activities in cyberspace pose real and serious threats to all States, as well as to corporations and private individuals." [32]

However, the authors note that the legal outcomes vary if peoples' lives are not directly endangered. The *Tallinn Manual* also provides a framework for approaching what

[27] Valeriano, ibid, 10.
[28] Valeriano, ibid, 10.
[29] Valeriano, ibid, 10.
[30] Valeriano, ibid, 11.
[31] Valeriano, ibid, 10.
[32] Schmitt, ibid, 4.

constitutes a "use of force" and "armed attack" in the scope of cyber operations, both of which are discussed later in this paper.

Stone argues that "the violent effects of cyber war need not be lethal to fall under the conception of war"—but in this matter, cyber operations that attempt to steal information might be equated with espionage in most circumstances.[33] In this way, cyber operations might be equated with another kind of tool to be used by state actors, particularly when these are done as defensive measures. However, espionage is not addressed in this paper because Stuxnet was not a case of usurping information; it was a direct attack intended to sabotage the continued production of centrifuges.

Evaluating different kinds of cyber operations, one must consider—at what point can these be considered an act of war? More specifically, could any of these attacks be considered a violation of the UN Charter Chapter II? When physical infrastructure is affected beyond a DDOS attack, the effect would be kinetic and invasive, which may and more closely parallel international law on conventional weapons.

In this section, I discussed what the term "cyber" means, and defined different types of cyber operations. Next, I discuss the technical parameters and legal implications of the Stuxnet worms and overall incident.

[33] Cited in Valeriano, ibid, 7.

## 5. The Stuxnet Operation

This section provides an overview of the Stuxnet operation. First, I describe the objectives of the two separate worms launched on Iran's facility in Natanz. In doing so, I outline how this attack proceeded and was undiscovered for four years. I then open my analysis towards the Charter and other legal documents as I examine how this attack would be considered under international law.

### 5. a. What Happened At Natanz: A Technical Explanation Of The Stuxnet Incident:

Stuxnet started with two worms: though the first was more discrete than the second on a technical level, they shared the same objective—to damage centrifuges at Iran's Natanz nuclear facility. Based on the motive of the attack—to alter and damage the enrichment of uranium at Iran's nuclear facility—it could be considered a complex intrusion, or even an APT.

The centrifuges at this facility were being enriched, which is arguably a core step to create a nuclear weapon.[34] By effectively "sabotage[ing] the country's uranium enrichment program, [it] prevent[ed] President Mahmoud Ahmadinejad from building a nuclear weapon."[35]

The Stuxnet worms were successful in part due to the unique conditions at

[34] Ralph Langner. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group, 2013.

[35] Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired Magazine,* July 11, 2011. Accessed December 6, 2015. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

Natanz. The plant is located 156 miles south of Tehran, and its perimeter is protected with military-level security. The facility is large, as were the trays of centrifuges it produced:

"The aluminum centrifuges, which are housed in bunkers, are 1.8 meters (5 foot 10 inches) tall and 10 centimeters (four inches) in diameter. Their purpose is to gradually increase the proportion of uranium-235, the fissile isotope of uranium. There is a rotor inside the centrifuges that rotates at a speed of 1,000 times per second. In the process, uranium hexafluoride gas is centrifuged, so that uranium-235 accumulates in the center. The process is controlled by a Siemens system that runs on the Microsoft Windows operating system."[36]

Ralph Langner, a data scientist whose research group analyzed the technical specifications of Stuxnet, gives a brief history of the Natanz nuclear facility in his report of the incident:

"The backbone of Iran's uranium enrichment effort is the IR-1 centrifuge which goes back to a European design of the late Sixties / early Seventies that was stolen by Pakistani nuclear trafficker A. Q. Khan. It is an obsolete design that Iran never managed to operate reliably. Reliability problems may well have started as early as 1987, when Iran began experimenting with a set of decommissioned P-1 centrifuges acquired from the Khan network. Problems with getting the centrifuge rotors to spin flawlessly will also likely have resulted in the poor efficiency that can be observed when analyzing IAEA reports, suggesting that the IR-1 performs only half as well – best case – as it could theoretically. A likely reason for such poor performance is that Iran reduced the operating pressure of the centrifuges in order to lower rotor wall pressure. But less pressure means less throughput – and thus less efficiency."[37]

The facility was using poorly-designed, antiquated machinery, which made it more vulnerable to attack.

---

[36] Stark, Holger. "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War." *Der Speigel,* August 8, 2011. Accessed December 6, 2015. http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html

[37] Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group (2013): 5-6.

Around the time when Stuxnet first began infecting computers in Iran—which analysts speculate was around 2006—Iran was using a Cascade Protection System in its uranium enrichment system. Centrifuges are made of extremely sensitive material, and even touching one can cause severe damage. The centrifuges at Natanz have shut-off valves for every stage of centrifuge and enrichment piping to ensure they run securely; the chemical balance of a centrifuge is crucial, and even oil from touching one can cause the system to malfunction. Individual centrifuges are shut off by the facility's valve isolation process (discussed later) if they are functioning incorrectly. When multiple centrifuges in same stage of the enrichment plant get isolated, maintenance might not have the chance to repair one or move another. If this happens too frequently, UF6 gas pressure increases—this is "the most sensitive parameter in uranium enrichment using centrifuges."[38]

The objective of Stuxnet (the worm) was to pressurize the entire system. If part of the centrifuge system is disrupted, pressure must be adjusted elsewhere or the remaining centrifuges will be over-pressurized. One of the worms sought to block the valve isolation process. [39]

"When the actual malicious process manipulations begin, all isolation valves for the first two and the last two enrichment stages are closed, thereby blocking the product and tails outflow of process gas to each affected cascade. From the remaining centrifuges, more centrifuges are isolated, except in the feed stage. The consequence is that operating pressure in the non-isolated centrifuges increases as UF6 continues to flow into the centrifuge via the feed, but cannot escape via the product and tails take-offs, causing pressure to rise continuously." [40]

---

[38] Langner, ibid, 7.
[39] The valve isolation process is the process used at Natanz, where centrifuges were isolated if they were no longer functioning.
[40] Langner, ibid, 9.

The first Stuxnet worm increased pressure as the second sped up the rotation of the centrifuges. [41] These two worms each had a specific target, and were completely autonomous, enabling them to remain undiscovered for four years. [42] At the facility, the status of each centrifuge is reflected on a central facility; green dots represent the normally-functioning centrifuges, while grey dots indicate that a centrifuge has been shut off. With the presence two worms, many centrifuges were shut off—and while the central computer should have indicated that with a grey dot, with the presence of the worm, they showed up as green.

The damage incurred was episodic, but was not catastrophic all at once. Many of the plant's centrifuges were unaffected by Stuxnet. As Ralph Langner noted in his TED Talk:

"What we also saw is that the goal of the attack was to do it slowly and creepy—obviously in an effort to drive maintenance engineers crazy, that they would not be able to figure this out quickly."[43]

The computers at Nantanz were air-gapped, yet the Stuxnet worms went around these air-gapped devices. They were likely introduced to the facility by a USB flash drive, which remained dormant in the drive until activated by the scientists who built the weapon. From there, the worms spread to other computers within the network used at Natanz.

---

[41] Langner, ibid, 5.
[42] Langner, Ralph. "Cracking Stuxnet: a 21st-century cyber weapon." TED Talk, 2011. http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon/transcript?language=en#t-175983
[43] Langner, ibid.

5. b. Attributing Stuxnet

The Stuxnet worm was first discovered by Sergey Ulasen in Belarus. Ulasen Worked at the research firm Virus Blok Ada in Minsk, "in the research and development department at the VirusBlokAda security firm in Minsk, [after having] received what seemed to be a relatively mundane email on June 17, 2010."[44] He traced back the worm to servers located in Malaysia and Denmark, where they had been registered under false domain names and forged credit cards.[45] At the time of its discovery, Stuxnet worm had infected "about 100,000 computers worldwide, including more than 60,000 in Iran, more than 10,000 in Indonesia, and more than 5,000 in India" before it was discovered.[46] [47] While the worms were likely meant to affect Natanz specifically, the code that launched the worms damaged other computer systems with the same technical, assembly-line capacities. This detail is important because there was an overall generic code, but its variables clearly indicated that it was targeting the Natanz facility:

"The big digital warhead—we had a shot at this by looking very closely at data and data structures. So for example, the number 164 really stands out in that code; you can't overlook it. I started to research scientific literature on how these centrifuges are actually built in Natanz and found that they are structured in what is called a cascade, and each cascade holds 164 centrifuges. So that made sense, that was a match....These centrifuges in Iran are subdivided into 15... stages. And guess what we found in the attack code? An almost identical structure. [of almost 15,000 individual lines of code]. So again, that was a real good match. And this gave us very high confidence for what we were looking at."[48]

[44] Stark, ibid.
[45] Stark, ibid.
[46] Stark, ibid.
[47] The reason the Stuxnet worm affected computers beyond those at Natanz was because the source code for Stuxnet was generic. In other words, the numbers and directions specifically used in Stuxnet's code could be used on any other computer with the same numeric qualifications.
[48] Langner TED Talk, ibid.

Langner said in his TED Talk that there were almost 15,000 individual lines of code, which looked like "old assembly line language."[49] However, even though certain variables (such as the numbers themselves that were used to identify a match with the Natanz facility) were clearly programmed to infect computers at Nantanz, the code itself is generic, which presents certain other dangers:

"It doesn't have anything to do, in specifics, with centrifuges, with uranium enrichment. So it would work as well, for example, in a power plant or in an automobile factory. It is generic. And you don't have—as an attacker—you don't have to deliver this payload by a USB stick, as we saw it in the case of [the] Stuxnet [operation]. You could also use conventional worm technology for spreading. Just spread it as wide as possible. And if you do that, what you end up with is a cyber weapon of mass destruction."[50]

Unlike a nuclear weapon with an immediate physical impact, Stuxnet inflicted episodic, gradual damage. As many scientists have already noted, the technical capabilities exhibited in Stuxnet indicate that it is entirely possible for a similar attack to also go unnoticed for a significant amount of time.

Stuxnet itself was sophisticated and discrete, but the operation's implications are far greater than its technical prowess: "The virus represents a fundamentally new addition to the arsenal of modern warfare. It enables a military attack using a computer program tailored to a specific target," over an extended period of time. This poses many critical questions about the future of warfare. More specifically, it raises the question of what constitutes an armed attack in a cyberwar context.[51] The data structures in the code show that this was likely targeted to this facility, but the code is generic and affected other computers with the same technical parameters as well.

[49] Langner TED Talk, ibid.
[50] Langner TED Talk, ibid.
[51] Stark, ibid.

In this section, I described how these two worms sabotaged the production of centrifuges at Iran's nuclear facility at Natanz. In the next section, I discuss the historical and legal implications for "aggression" and "self-defense" before I examine how these apply to Stuxnet.

## 6. Historical and Legal Roots Of "Aggression" And "Self-Defense"

Both aggression and self-defense concern *jus ad bellum*. Under Article 51 of the UN Charter, responding to an armed attack in self-defense is legal. Aggression, on the other hand, is when one state initiates an armed attack without the pretense of self-defense. These definitions are challenged by cyber warfare in that it can be difficult to ascertain exactly when an attack begins and ends. This also becomes complicated when considering offensive attacks that have not yet taken place. If there is little evidence of an imminent attack, it would likely constitute a preventive attack, which is within the scope of an act of aggression. However, if there is evidence and overwhelming certainty that an imminent attack will soon take place, a state can retaliate in anticipatory self-defense, otherwise known as a pre-emptive strike.

In this section, I consider the historical roots of aggression. I list the institutionalized definitions of aggression between World Wars I and II, and discuss how aggression has been codified and adjudicated.

### 6. a. Historical Roots of Aggression and Self-Defense:

"Aggression" emerged as an illegal act relatively recently. Historically, one could begin by looking at the Babylonian invasion of Judah and the subsequent destruction of the first Temple in 587 BCE. Powerful empires like that of the Romans were constantly at war as they acquired new territory.[52] Such conquests for land took a different turn after the Peace of Westphalia, announced in 1648. International relations theorists consider

[52] Sergey Sayapin. *The Crime of Aggression in International Criminal Law (*TMC Asser Press, The Hague, The Netherlands. 2014): 13.

this international agreement, negotiated as the end of the Thirty Years War and the Eighty Years War, which was negotiated by Europe's most powerful nation-states at the time.[53] This is seen by international relations experts as the root for the concept of state sovereignty—or, that states can have specific borders, not to be interrupted by another state or empire. This principle became a centerpiece of the United Nations.

As stated before, self-defense does not always need to be in response to an armed attack. In some circumstances, states can attack other states when there is evidence of an imminent attack. Consider the Caroline Affair of 1837: letters exchanged between American and British diplomats after the Affair suggested that there was a customary acceptance that anticipatory self-defense could be justified in select circumstances and that it was not inherently illegal. During the Caroline Affair, the US supplied soldiers, arms, and

"provisions using the steamboat SS Caroline to the rebel headquarters, as they were planning an invasion on Upper Canada. In response, the British seized the Caroline overnight, set it on fire, and then cast it adrift over Niagara Falls, killing two men in the process."[54]

In response, US Secretary of State Daniel Webster wrote to the British diplomat, and the US Secretary of State Daniel Webster and the British diplomat corresponded after the incident. In their letters, they concurred that anticipatory self-defense could be justified in situations where "the necessity of that self-defense is instant, overwhelming, leaving no

[53] These states included Spain, France, the Netherlands, Sweden, the Roman Empire, and various other-city states in Western Europe.

[54] Louis-Philippe Rouillard. "The Caroline Case: Anticipatory Self-Defense in Contemporary International Law", 1(2) Miskolc J. of Int'l L. 104-20 (2004), available at http://www.uni-miskolc.hu/wwwdrint/20042rouillard1.htm. In Vantanparast, Roxana. "International Law Versus The Preemptive Use of Force: Racing to Confront the Specter of a Nuclear Iran." (*UC Hastings College of the Law Hastings International and Comparative Law Review* 31, no. 783, 2008): 4.

choice of means, and no moment of deliberation."[55] [56] While it is an obscure case, the letters exchanged after the Caroline Affair show that there was a customary understanding among diplomats that states could act in self-defense when there is an imminent threat. In other words, a combatant need not wait until an attack has already been launched before it can respond in self-defense. This case was later cited by the US in its invasion of Iraq in 2003, which is discussed later in this section.

The Hague Conventions of 1899 and 1907 set up original frameworks for preventing widespread war. In tandem with the four treaties Geneva Conventions dictating just conduct during war, the Hague Conventions also established laws of war in international law. In four Conventions and three declarations, the Hague Conventions noted what kinds of conduct during war would be unacceptable; for example, Hague IV prohibited the use of poisonous gases.[57] The first Convention of 1899 also created a Permanent Court of Arbitration to settle disputes between states.[58] [59] The conferences in 1907 largely affirmed the protocols established eight years prior, but the third convention of 1907 stated permissible conduct "relative to the opening of hostilities."
The Convention stated that "hostilities between [states] must not commence without previous and explicit warning, in the form either of a reasoned declaration of war or of an

[55] Vantanparast, ibid.
[56] It is important to note that this exchange concerned a political dispute, and notably, the involved parties did not go before any international tribunal or legal system.
[57] "Pacific Settlement of International Disputes (Hague I); 29 July 1899." *The Avalon Project - Laws of War.* July 29, 1899. http://avalon.law.yale.edu/19th_century/hague01.asp.
[58] Pacific Settlement of International Disputes (Hague I), ibid.
[59] This Court was later reinstated in the UN Charter as the International Court of Justice (ICJ).

ultimatum with conditional declaration of war."[60] Many of these conventions were ignored during World War I; for instance, Germany's invasion of Belgium was without warning as mandated in Hague III of 1907, and poisonous gas was used during World War I.[61] Nevertheless, the frameworks set up in these conventions were later adapted into later conventions concerning just conduct during war, and the right to wage a war, or *jus ad bellum*.

> "The states of Europe and Latin America had already agreed, at key international conferences in The Hague in 1899 and 1907, that the *methods* by which wars were conducted should also be limited, leading to the development of the modern law of war."[62]

6. b. Institutional Definitions Between World War I and World War II

Pursuing different avenues to outlaw aggression culminated in the Treaty of Versailles of 1919, which officially terminated World War I. What was known as the "war to end all wars" had been catastrophic for Europe, leaving more than 17 million dead and another astounding 20 million wounded; more than 6 million of these deaths were civilians, and over 50% of Europe's men dead or gravely wounded.[63] Article 231 of the Treaty of Versailles did not specifically spell out terms like "crimes of aggression," but it did include a "guilt clause," where Germany was labeled the principal aggressor. In a measure that ultimately foreshadowed the Nuremberg Principles after WWII, UK Prime Minister David Lloyd George advocated prosecuting Kaiser Wilhelm as a war criminal—

---

[60] "Laws of War: Opening of Hostilities (Hague III); October 18, 1907." The Avalon Project. October 18, 1907. http://avalon.law.yale.edu/20th_century/hague03.asp.
[61] Pruszewicz, Marek. "How Deadly Was the Poison Gas of WW1? - BBC News." BBC News. January 30, 2015. http://www.bbc.com/news/magazine-31042472.
[62] Dunoff, ibid, 15.
[63] PBS. "WWI Casualty and Death Tables." https://www.pbs.org/greatwar/resources/casdeath_pop.html (accessed February 16, 2016).

in other words, to hold him individually culpable for his conduct during war. However, US President Woodrow Wilson objected, claiming it was unclear who had jurisdiction. [64] The Allied powers eventually agreed to issue an international arrest warrant for him, charging him with a "supreme offense against international morality and the sanctity of treaties"—essentially a euphemism for what the international legal community would eventually call "aggression." [65] "These changes had so little basis in international law that the Dutch, who had custody of the Kaiser, refused to turn him over, and he died in the Netherlands in 1941, untried." [66] Despite the jurisdictional ambiguity raised in this case, the concept of individual culpability for state leaders—especially for when these leaders were in power—became a central part of international legal dialogue. [67]

The Kellogg-Briand Pact (1928) was another international effort to set a series of standards criminalizing the act of invading another state. [68] Named for the US Secretary of State Frank B. Kellogg and French Minister for Foreign Affairs Aristide Briand, signees of this Treaty (the US, Germany, and France) vowed to settle disputes peacefully.[69] Various other nations in Latin America, Asia, and the Middle East also became party to it.

The Pact was a precursor to the World Disarmament Conference, organized by the League of Nations, in 1932. The objective of this conference, as its title suggests, was

---

[64] Tina Rosenberg."Tipping the Scales of Justice"*World Policy Journal* 12 (1995): 3. [Sage Publications, Inc., Duke University Press]: 55–64. http://www.jstor.org/stable/40209427.

[65] Simeon E. Baldwin. "The Proposed Trial of the Former Kaiser." *The Yale Law School Legal Scholarship Repository* (1919): 75. <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5302&context=fss_papers>.

[66] Rosenberg, ibid, 57.

[67] Baldwin, ibid.

[68] In other words, the Kellogg-Briand Pact concerned state culpability.

[69] Kellogg-Briand Pact (1928). http://www.yale.edu/lawweb/avalon/imt/kbpact.htm (accessed February 23, 2016).

to drastically eliminate the number of arms each nation had; ideally, this would limit the capacity to which states could launch armed attacks on one another. Germany, whose military had already been significantly reduced under the Treaty of Versailles, refused to sign the treaty unless other signees reduced their number of arms to Germany's levels; in the event that this was not agreed to, Germany demanded that it be allowed to rebuild its army. France, "which feared the revival of German power, argued that security must precede disarmament and called for security guarantees and the establishment of an international police force before it would reduce its own forces." [70] In the midst of this gridlock, talks were postponed until February 1933. Hitler assumed power on January 30, 1933; days after, he ordered the withdrawal of German delegates both from the conference and from the League of Nations all together. [71] Finding ways to reduce incentive and prevent war—as the Disarmament Conference clearly failed to do—was revisited after WWII again, in the crafting of the UN.

6. c. "Aggression" Defined at the UN

After World War II, the Nuremberg Principles, which were established along with crimes against humanity, genocide, and other *jus in bello* war crimes included "crimes against peace," known as Principle VI and which was later accepted by the UN General Assembly as a means for explaining "aggression." Principle VI defined "crimes against peace" as:

---

[70] Disarmament Conference, Geneva, 1933. *World Digital Library.* https://www.wdl.org/en/item/11592/ (accessed February 23, 2016).

[71] "German Aggression." *BBC*. http://www.bbc.co.uk/bitesize/standard/history/1930_1960/german_aggression/revision/1/ (accessed February 23, 2016).

(i) Planning, preparation, initiation or waging of a war of aggression or a war in violation of international treaties, agreements or assurances;
(ii) Participation in a common plan or conspiracy for the accomplishment of any of the acts mentioned under (i).[72]

It is worth noting that the Nuremberg Principles were conceived to hold individuals accountable for their roles in aiding Hitler. These principles were later codified for states to follow as well, specifically in the 1974 UN General Assembly Resolution 3314. Though "aggression" is never specifically defined in the UN Charter, its implications for states—the threat of, or actual, use of force—are both prohibited. While Resolution 3314 was technically a recommendation and not binding for UN member-states, it is customary to follow these resolutions.

The definition of "aggression," or "crimes against peace," were made binding in the Rome Statute (or the International Criminal Court [ICC] Statute) treaty in 1998, which entered into force in 2002.[73] Importantly, the Court may only begin exercising jurisdiction one year after the thirtieth ratification, and after the Assembly of States Parties has approved the commencement of jurisdiction, which it can only do after

The definition below is a separate 2010 amendment that did define the crime of aggression, which will come into force in 2017:

"1. For the purpose of this Statute, "crime of aggression" means the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations.

---

[72] "The Nuremberg Principles." International Nuremberg Principles Academy. http://www.nurembergacademy.org/the-nuremberg-legacy/the-nuremberg-principles/ (accessed February 20, 2016).
[73] Rome Statute of the International Criminal Court. https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf

2. For the purpose of paragraph 1, "act of aggression" means the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. Any of the following acts, regardless of a declaration of war, shall, in accordance with United Nations General Assembly resolution 3314 (XXIX) of 14 December 1974, qualify as an act of aggression:

(a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;

(b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;

(c) The blockade of the ports or coasts of a State by the armed forces of another State;

(d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;

(e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;

(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;

(g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein."[74]

This definition expands upon and renders binding the otherwise non-binding UN General Assembly (UNGA) Resolution 3314 (1974) that recommended aggression be considered a crime.[75] However, the Court will not be able to exercise jurisdiction over the crime of aggression until "at least 30 States Parties have ratified or accepted the amendments [concerning the crime of aggression]; and a decision is taken by two-thirds

[74] Article 8. Rome Statute of the International Criminal Court. https://www.icc-cpi.int/nr/rdonlyres/add16852-aee9-4757-abe7-9cdc7cf02886/283503/romestatuteng1.pdf

[75] The UN General Assembly Resolution 3314 is a nonbinding resolution intended to help the Security Council make such determinations. It was adopted by the Assembly in 1974. It can be found here: http://legal.un.org/avl/pdf/ha/da/da_e.pdf

of States Parties to activate the jurisdiction at any time after 1 January 2017."[76] It is also important to note that states cannot be tried at the ICC; this Court is reserved solely for cases concerning the culpability of individuals.

6. d. "Aggression" Adjudicated:

The International Court of Justice (ICJ) case, *Nicaragua v. United States of America*, was the first major judicial decision that solidified the working definition from Resolution 3314.[77] While the case itself was complex, it first and foremost questioned the legality of one state clandestinely intervening in another's domestic affairs.

This case built upon the UNGA Resolution 3314 (1974) definition of aggression was *Nicaragua v. United States*, which went to the International Court of Justice (ICJ). At the ICJ, Nicaragua asserted that the US had been supporting covert paramilitary operations for supporting the Contras in their rebellion against the socialist Sandinista National Liberation Front administration (FSLN). [78] Originally, the US declared that its support for the Contras, which it admitted was taking place, was self-defense: "the Reagan team equated the emergence of radical nationalism in Central America with Soviet-Cuban expansionism." [79] The Sandinistas admittedly:

---

[76] "The Crime of Aggression." *Coalition for the International Criminal Court.* http://www.iccnow.org/?mod=aggression

[77] Note that the ICJ is the judicial branch of the United Nations, and its resolves disputes between states. Questions of individual culpability can be referred to the aforementioned International Criminal Court (ICC).

[78] Marc Edelman. "Soviet-Nicaraguan Relations and the Contra War." *International Journal on World Peace* V, no. 3 (1988): 45-67. http://search.proquest.com/docview/1311295479/141138AA5D83A65D5FB/22?accountid=12933 (accessed February 23, 2016).

[79] North, Liisa, and Tim Draimin. "The Decay of the Security Regime in Central

"looked to the Soviet Union and Cuba for assistance. In addition, the Sandinistas supported like-minded revolutionary movements in other countries. In particular, they provided safe haven and other assistance to Marxist rebels seeking to overthrow the government of El Salvador."[80]

Two years after the Sandinistas came into power after overthrowing the regime of Anastasio Somoza in 1979, the US found its pro-Marxist ideologies and tactics in the region threatening. At the beginning of the Reagan administration, the US began to support a group of rebels, called the contras, with financial, political, and military assistance.[81] In 1984, Nicaragua appealed to the ICJ, intending to file suit under Article 36(2) of the Court's Statute. When the US saw that Nicaragua intended to sue, it asserted instead that the ICJ lacked jurisdiction. "When the Court ruled that it did have jurisdiction, the United States refused to participate further in the case, and on October 7, 1985, terminated its acceptance of the Court's jurisdiction under Article 36(2)."[82]

The ICJ continued to investigate Nicaragua's claims because "the ICJ cannot render a default judgment." [83] The US claimed that the FSLN's attempts to undermine El Salvador, Costa Rica, and Honduras were a threat to the region, and added that only monetary and military support from the US would protect it from a similar movement closer to the US. The ICJ ultimately found that the US had violated customary international law concerning non-intervention. [84] The Court specifically ruled that

---

America." *International Journal* XLV, no. Spring (1990): 231. http://search.proquest.com/docview/61133476/141138AA5D83A65D5FB/18?accountid=12933 (accessed February 23, 2016).

[80] Dunoff, ibid, 868.
[81] Dunoff, ibid, 868.
[82] Dunoff, ibid, 868.
[83] Dunoff, ibid, 868.
[84] "Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States)." 1986 ICJ 14 (June 27). In Dunoff, ibid, 869.

military and paramilitary activities sponsored by the US "constitute[d] a clear breach of the principle of non-intervention." [85] It added:

"While the arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so in respect of all the assistance given by the United States Government. In particular, the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua[,]...does not in itself amount to a use of force." [86]

Further, it found that the US could not claim that it was acting as a part of collective self-defense, because there was no direct evidence that the Nicaraguan Civil War satisfied the conditions for collective self-defense as outlined in customary international law. While the Court affirmed that paramilitary support for the contras could be considered a threat or actual use of force, assistance to this group would still not satisfy the conditions for an "armed attack," since it was indirect. It considered the response from Washington, however, "disproportional" to the attack allegedly made on El Salvador. To reiterate, while the US claimed supporting the contras in their war against the communist Sandinistas was self-defense, the ICJ rejected this claim.

The Stuxnet incident could be seen as similar to arming the Contras. The US arming Nicaraguan Contras was justified on highly preventive grounds. Stuxnet was also a highly preventive attack, albeit clandestine. Both could be seen as aggression, as the ICJ stated in this case. In this case, the ICJ stated that there needed to be a more direct link between imminent threat compromising US national security and what was happening in Nicaragua in order for the US to make an effective self-defense claim; since

[85] Nicaragua v. United States, ibid, 870.
[86] Dunoff, ibid, 871.

it was unable to do that, the ICJ would likely find the Stuxnet incident to also be an act of aggression.

The US invaded Iraq in 2003, claiming that there was sufficient evidence of weapons of mass destruction that would likely be used against them. Predicated on faulty evidence, the US asserted that its invasion of Iraq was "anticipatory self-defense." It looked to the Caroline Affair as a precedent, and invaded, despite lacking approval from the UN. Intelligence for this operation proved faulty, and retroactively, we can consider this invasion a preventive attack and thus an act of aggression. Had there been higher certainty about the intelligence regarding Iraqi weapons of mass destruction, an anticipatory self-defense claim would be more reasonable, and the invasion could then be justified under international law. If the evidence had been overwhelming, perhaps the US would have gained from the UN to strike first against Iraq.

Since there was inadequate evidence supporting the Americans' intervention in Iraq in 2003, it suffices to say that it could not justify this invasion as anticipatory self-defense.

## 7. Stuxnet As An Act Of Aggression

In this section, I apply the historical and legal connotations of "aggression" and "self-defense" to the Stuxnet incident. I argue that launching these worms was an act of aggression, not self-defense.

### 7. a. Invoking Article 51: Self-Defense

Particularly based on the ICJ's Nicaragua ruling, it is clear that the US would be unable to claim collective self-defense with Israel for launching Stuxnet. There was no imminent attack prepared by the Iranians; thus, the US could not have claimed self-defense. More broadly, it is also difficult to ascertain whether a cyber operation such as Stuxnet, with such a gradual impact, could be seen as clear anticipatory self-defense.

Despite famously aggressive speech over decades by Iranian leadership towards the US and its allies, there was no specific, imminent threat that would warrant an attack in self-defense. The weapon that Iran was allegedly building was far from being a real threat, and "there is no rule in customary international law permitting another State to exercise the right of collective self-defense on the basis of its own assessment of the situation." [87]

Self-defense can only be undertaken in the event of an armed attack. The term "armed attack" is typically applied in situations where there is a clear, kinetic result of an attack that has clearly endangered human lives.[88] The Stuxnet operation did have a kinetic result of disrupting the production of centrifuges at Iran's nuclear facility at

[87] Dunoff, ibid, 872.
[88] Charter of the North Atlantic Treaty Organization. http://www.nato.int/cps/is/natohq/topics_110496.htm?

Natanz, so could be considered a US/Israeli attack on Iran. The lack of a prior "armed attack" or even imminent threat from Iran would not warrant the aggression from the US and Israel. Because there was neither prior attack nor an imminent one, the American and Israeli actions were likely disproportionate, and a breach of international law.

However, the Stuxnet operation more resembles industrial sabotage than an act of war. Could a cyber operation ever be considered analogous to a kinetic weapon causing physical damage? The answer depends upon the nature of the cyber operation. Some such operation could resemble the Stuxnet worms. Other operations might look more like a *Wargames* scenario, where a perpetrator might knowingly (or not) be on the brink of setting off nuclear weapons through cyberspace. As discussed earlier in this paper, most cyber operations are generally benign and do not endanger civilian lives. Clearer specification under international law of what constitutes an armed attack, aggression, aggression and how to determine and who judges the facts are needed to address threats like Stuxnet.

The operation did have a kinetic result, but this physical damage is clearly not the same as an attack that endangers civilians. More centrally, however, we can ascertain that the Stuxnet operation was an act of aggression.

7. b. Could The US Be Tried For Aggression?

In the case of the Stuxnet operation, the US or Israel could not be tried per se, as neither has joined the ICC or ratified the amendment—but a chief operative who dictated the attack at a top chain of command could be. While Iran is a member of the UN, it has not joined the ICC either. For this case to go to the ICC, Iran would need a referral from

the UN Security Council [UNSC]. Given that the US has veto power on the Security Council, this is entirely unlikely.

Although an American or Israeli citizen would not be able to be tried and convicted under this amendment, it is clear that, according to the definition of an "act of aggression," the Stuxnet operation could be seen as, at least, an "act of aggression," as defined in the 1974 General Assembly Resolution as well. It satisfies points (a), as this operation was clear, intentional industrial sabotage, violating Iran's state sovereignty under the UN Charter.

7. c. A Preventive Attack Without The Rome Statute

Since neither the US nor Israel is party to this amendment, operatives for either country technically could not be tried. The following scenario presumes that they were—and shows that even in that instance, neither the US nor Israel officials could make a self-defense claim under the UN Charter. [89]

Theoretically, these nations could say—as they have—that Iran constitutes a danger to the national security of both states. Further, they could assert that they had no choice but to do everything possible—however discretely—to prevent such an attack from occurring. In any place, despite alarming statements from its political leadership, Iran did not pose an imminent threat to the US or Israel when the Stuxnet worms were launched. Even if the US and Israel were right that Iran posed a threat to the national

[89] To reiterate, the ICC only has jurisdiction over individuals. Government officials or individual policymakers could go before the Court. While states may sign the Rome Statute and join the ICC, a state (as an entity—barring its officials) cannot be prosecuted there per se.

security of both states, without the presence of an imminent attack from Iran, this would still not warrant a military response—and it certainly could not be called self-defense.

Responding to an armed attack in self-defense (or, state A initiating an attack first when there is an obvious threat with compelling evidence showing that State A will be attacked imminently) is permitted under Article 51 of the UN Charter—in other words, a pre-emptive attack. The US and Israel might argue that the Stuxnet operation was an act out of collective self-defense. Given the kinetic result that occurred because of the Stuxnet operation, it could be considered an attack. However, the legitimacy of the self-defense claim would depend upon Iran's capabilities and intentions in the purported development of a nuclear weapon. At the time of the Stuxnet operation, Iran had not produced as much as a nuclear explosive, let alone a weapon. Since Iran was so far from having a developed weapon and posing an imminent threat, the Stuxnet operation was accomplished as a preventive, and not a pre-emptive, measure. Pre-emptive measures are legal; preventive ones are not. An attack cannot be considered "aggression" if it effectively a pre-emptive measure in self-defense—and this is central to understanding why the Stuxnet operation was not legal.

At what point does responding to aggression become self-defense? The table on the next page distinguishes between the different stages of this process.

Distinguishing aggression:

| **STAGE** | **STATE 1** (IRAN) | **STATE 2** (US) |
|---|---|---|
| 1 | Weapons precursor development (say, enrichment capability) | Preventive attack: Aggression |
| 2 | Weapons deployment (say, testing weapons prototype components) | Preventive attack: Aggression |
| 3 | Weapons deployment (say, sending weapons to air bases on missile sites) | Preventive attack: Aggression |
| 4 | Military mobilization (rising hostility, declarations of intent, offensive mobilization and development) | If there is high certainty: Pre-emptive attack: Self-defense<br><br>If there is low certainty: Preventive attack: Aggression. |
| 5 | Attack (aggression) | Clear self-defense |

To best understand the difference between pre-emptive and preventive attacks, the question of "imminence" must be considered. A simple example of an imminent attack would be that there is an attack that will certainly occur in the immediate future. No

specific amount of time (like days, for instance) is defined as "imminent" in the charter or elsewhere. However, the purpose of using the phrase, however ambiguous, is to help states determine if there is sufficient evidence to conclude that one state will attack another.

When Stuxnet was launched, Iran was still clearly in the first stage of developing a weapon. This shows that the US and Israel made a preventive (and therefore, illegal) attack against Iran, before Iran had ample chance to prepare an imminent attack. Even with the legal question of pre-emptive v. preventive attacks aside, this could also be shown in the nature of the Stuxnet operation, and the fact that it had a gradual impact on the construction of these centrifuges.

Using the framework for assessing aggression—and whether or not self-defense claims can be made under the UN Charter and Rome Statute—we can determine that the employment of Stuxnet against Natanz facility was a preventive attack, and thus an act of aggression.

## 8. Why Iran Cannot Legally Retaliate For Stuxnet

Could Iran legally retaliate for Stuxnet—and would such action be self defense? Again, Article 51 of the UN Charter comes into play:

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."[90]

Article 51 mandates that if states respond to an attack in self-defense, their response must be proportional. But what does "proportionality" mean practically for cyber operations? This section investigates the limitations of "proportionality" in response to a cyber attack. In doing so, it also addresses language in Article 51 of the UN Charter like "use of force" and "armed attack" which are also vague in terms of cyber attacks.

### 8. a. Proportionality

Proportionality "provides the basis for determining the validity of a measure taken by a State to derogate from the human rights of those humans within the State's scope of authority."[91] The US Army Counterinsurgency (COIN) Manual reduces proportionality to mathematics: "Proportionality is usually calculated in simple utilitarian terms: civilian

[90] Chapter VII, Article 51 of the UN Charter. http://www.un.org/en/sections/un-charter/chapter-vii/index.html. Accessed February 8, 2016.

[91] Newton, Michael and Larry May. "Proportionality in International Law." From Proportionality in Human Rights Law and Morality. *Oxford University Press* (2014): 1-27.

lives and property lost versus enemy destroyed and military advantage gained."[92] The European Court of Human Rights states that, concerning *jus in bello*: "The force used must be strictly proportionate to the achievement of the permitted aims."[93]

While the US arguably committed an act of aggression against Iran, it is unclear whether Iran could legally respond in a proportional manner. It also raises the following question: What would a proportional response be in the event of a destructive cyber operation? For example, could a state's response to a cyber operation only be via another cyber operation?

Iran has a limited range of legal options by which to respond to American aggression. As a member of the UN, Iran would need to go to the UN Security Council (UNSC) and obtain a vote from the P5 members[94] to make its actions justifiable under Article 51. The US would obviously veto such a measure. If Iran's act is self-defense, it doesn't have to go to the UNSC first. It can act while going to the UNSC. But since the attack was over (and not hugely destructive), would a response even be self-defense—especially six years after the attack was realized?

But this also raises an important question in addressing Article 51 in the future: when coping with cyber operations that take place over a long period of time—especially operations that happen clandestinely, as in Stuxnet—how can the UN seek to rectify acts of aggression between states that occur in cyberspace?

---

[92] Newton and May, ibid, 26.
[93] *Khatsiyeva and others v. Russia.* Cited in Newton and May, 7.
[94] The "P5" refers to the United Kingdom, France, China, Russia, and the United States. These are the only states with permanent seats on the UNSC, and all have veto power—a privilege that other rotating members of the Council do not have.

There are other additional constraints that limit Iran's range of options. The Joint Comprehensive Plan of Action from Summer 2015 between the Iran, the P5+1 (1 referring to Germany) and the European Union lifts sanctions on Iran in exchange for close monitoring of its nuclear program. Iran claims that it was expanding its nuclear program for peaceful purposes; the international community disagreed. Responding to a cyber operation that took place a number of years ago, before the introduction of certain sanctions from the UN and EU, seems out of sync with its current relationships with these countries.

From the language of Article 51, it is unclear in the context of non-conventional weaponry (namely, via cyber operations) what an "armed attack" would actually constitute. Stuxnet was the first cyber operation launched that had a direct, physical result, directed at one member of the UN by another, but it lacked civilian casualties. Its effect was gradual and happened over the course of many years. Thus, it does not necessarily suffice to say that Iran was the victim of an "armed attack."

The question of what constitutes an armed attack is also problematic. Article 51 and the rest of the UN Charter were signed into force in 1945, after two uses of atomic bombs on Japan by the US. "Armed attack" clearly refers to conventional weapons, and weapons of mass destruction, being used by state actors. But when applied to cyber attacks that do not wreak the same immediate havoc as a bomb, does Article 51 and "armed attack" even suffice to discuss cyber warfare?

Another central question surfaces from Article 51: would a cyber attack be considered a real, tangible "threat" to international peace and security? Perhaps not in any immediate, as cyber attacks as we know them in spring 2016 have not have physical

impacts. But future attacks could lead to a chain of reactions that could lead to massive destruction. Ted Koppel gives a picture of an American doomsday in the opening of *Lights Out,* which I paraphrased in this paper's Introduction. While an attack on the US power grid is certainly different than a clandestine attack on Iranian centrifuge production, this shows that Article 51 is insufficient to address responses to aggressive cyber operations between states.

It is worth noting that there is a difference between a response that is legal and a response that has an effect. There are four possibilities for types of responses:

Legal?

| | **YES** | **NO** |
|---|---|---|
| **YES** | Yes, Yes | Yes, No |
| **NO** | No, Yes | No, No |

Effective?

This table shows that legal responses are not effective in all scenarios. However, all of these scenarios would be difficult to gauge depending on if cyber attacks without an immediate physical impact would be considered having a truly catastrophic effect.

If Iran were to respond in self-defense shortly after the attack was realized, determining what that response would look like, based on Article 51 and regarding proportionality, is very difficult to determine. Unless Iran were to respond with an equally destructive cyber attack, it is unlikely that a kinetic response would be satisfactory for a proportional effect.

8. b. Scale and Use of Force

Another concept that is crucial to understanding Stuxnet is the implication of the use of force. The *Tallinn Manual* notes that: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[95] However, it adds that the UN Charter offers no specific criteria to determine what exactly constitutes a "use of force," which makes ascertaining whether a cyber operation could be considered such ambiguous—unless it amounts to a military result. This was controversial for the drafters of the UN Charter:

"The question was whether 'force' included 'all forms of pressure, including those of a political or economic character, which have the effect of threatening the territorial integrity or political independence of any State' was answered in the negative. Accordingly, whatever 'force' may be, it is not mere economic or political coercion. Cyber operations that involve, or are otherwise analogous to, these coercive activities are definitely not prohibited uses of force."[96]

The use of force can be seen as analogous to methods of coercion; beyond the pursuit of political or economic means, the use of force in cyber operations would then refer to activities with a military result.

The authors of the *Tallinn Manual* writes that in order to determine what would constitute a "use of force" in cyber operations, several factors must be considered to determine the degree of attempted coercion. These include:

[95] Schmitt, ibid, 45.
[96] Schmitt, ibid, 46.

(a) "*Severity.* Consequences involving physical harm to individuals or property will in and of themselves qualify the act as a use of force. Those generating mere inconvenience or irritation will never do so." [97] [98]
(b) *Immediacy* of the effects.[99]
(c) *Directness*, which determines the chain of causation. This includes the impact of an explosion, i.e. armed force that "directly harms people or objects," versus an activity that occurs as a result of economic sanctions.
(d) *Invasiveness*, "As a rule, the more secure a targeted cyber system, the greater the concern as to its penetration."[100] In other words, attacking high-profile targets raises the stakes of the attack, and makes it more likely to be considered a misuse of force.
(e) *Measurability of effects:* "the more quantifiable and identifiable a set of consequences, the easier it will be for a State to assess the situation when determining whether the cyber operation in question has reached the level of a use of force."[101]
(f) *Military character:* Or, determining if there is a viable connection between the cyber operation in question and a state's military apparatus.
(g) *State involvement*: This is along the general continuum of whether an invasive operation in question was conducted by a state.
(h) *Presumptive legality*: "Acts that are not forbidden are permitted; absent an express treaty or accepted customary law prohibition, an act is presumptively legal."[102]

This is a substantial list of criterions to consider a "use of force" in a cyber attack—but even this criteria clearly applies to the assumptions of existing international law. There is still language about immediacy (b), how grave the effects are (e), involvement of the state (g), and so forth, all of which are relevant to Article 51 of the UN Charter. There is no single way to categorize a cyber attack. This is a problem for international lawmakers because it means each attack must be categorized on a case-by-case basis; apart from the US Department of Defense declaration that infiltrations are illegal, there is no norm to define attacks that will only happen more frequently, and likely become more serious as

[97] Schmitt, ibid, 48.
[98] This includes the scope, duration, and intensity of the response.
[99] As the Stuxnet worm affected the Natanz facility gradually and over a number of years, this long-term, continual effect could be seen as an attempted use of force.
[100] Schmitt, ibid, 49.
[101] Schmitt, ibid, 50.
[102] Schmitt, ibid, 51.

technology becomes more advanced. At what point would a cyber attack amount to a "use of force" under Article 51? Even the writers of the *Tallinn Manual*, whose goal was to determine the applicability of international law in cyber operations, were:

> "divided as to whether the notion of armed attack, because of the term 'armed', necessarily involves the employment of 'weapons'. The majority took the position that it did not and that instead the critical factor was whether the effects of a cyber operation, as distinct from the means used to achieve those effects, were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack."

The term "armed attack" also implies that a physical attack has already taken place. In a cyber operation like Stuxnet, when would that be delineated? This was a continual attack that progressively inflicted damage on Natanz. Would this refer to when the worms were first launched, or after they inflicted a certain amount of damage?

> "However, as noted by the International Court of Justice, not every use of force rises to the level of an armed attack. *(Nicaragua* judgment, para. 191). The scale and effects required for an act to be characterized as an armed attack necessarily exceed those qualifying the act as a use of force. Only in the event that the use of force reaches the threshold of an armed attack is a State entitled to respond using force in self-defense."[103]

The many definitional problems of Article 51 make it challenging for Iran to retaliate in self-defense. Beyond the scope of Stuxnet, this also makes it difficult to determine what retaliation for different types of attacks would look like in the future. This shows that the standard rhetoric and procedures for states responding to typical warfare do not fit neatly with this growing field of malignant operations.

[103] Schmitt, ibid, 55.

## 9. Conclusion

This paper argues that the Stuxnet operation launched by the US on Iran's nuclear facility would be considered an act of aggression under the Rome Statute.

After listing my research limitations, I established which sources were most relevant to my analysis. I defined terms central to my paper's argument like "cyber," which solidify the parameters of my argument. I showed how the vocabulary used by experts in international law is inconsistent with language directly related to cyber technologies.

I discussed the relevant branches of IR theory and sources of international law. I examined theories such as realism and liberalism and showed how these theorists debate the utility of international law. Next, I provided a technical explanation of the damage incurred by the Stuxnet worms, and discussed how it was discovered. I also described how the code was discovered as a generic source code that could have—and did—affected any computer with the same technical parameters as the computers used at Natanz. In the subsequent section, I gave a historical overview of the roots of aggression in international law. I tracked its sources, as well as terminology pertaining to pre-emptive and preventive attacks. In applying this to Stuxnet in the following section, I determine that this operation would be seen as an act of aggression; a non-existent capability from Iran cannot constitute an imminent threat to US national security. In the final chapter, I determined that Iran's range of options to retaliate is limited by practical constraints.

Aggression is a *jus ad bellum* concept, as it concerns the right to wage a war. The Stuxnet incident took place over four years. Perhaps Iran could have responded shortly after the attack was realized; six years later, there is probably no legitimate military response. Chapter VII of the UN Charter states that the UNSC must find and authorize a use of force, or states can retaliate in self-defense. However, the chapter does not mention how much time a state has to respond in self-defense. Once the possibility to call an attack self-defense is precluded, cyber engagements render how we understand the laws of war incomplete. This shows that terms like "aggression," "self-defense," and "warfare" do not fit comfortably with cyber warfare. If international law is meant to mitigate the anarchy that exists in the international system, this new kind of warfare certainly warrants a closer look and Convention by lawmakers.

The questions raised in this paper that concern hazardous cyber operations are to be taken seriously by policy experts. Right now, cyber operations continue to exclusively be evaluated on a case-by-case basis, through the lens of conventional weapons and warfare. However, cyber conflicts are far from conventional weapons and warfare. The practical implications of cyber operations do not meet the standard definitions in international law. The Stuxnet incident could be seen as successful, at least in part before the Joint Comprehensive Plan of Action from Summer 2015, which constrained the development of Iranian uranium enrichment in exchange for lifting sanctions. Such similar operations are likely to continue occurring as technology continues to advance—and perhaps as individuals and organizations become more powerful in the international sphere. The power of international law is the power states make of it to constrain

malignant behavior. So much can be done via cyberspace, so it is crucial that the international community take action to have some set of restraints.

Some might consider this futile; as technology continues to develop, the international community will need to constantly evaluate its own law. Furthermore, one could say that this might preclude customary practices from accumulating and becoming international law. That said, having some regulation in place is a more viable alternative than having no basis for constraints at all, or no working definition about what constitutes an attack in the event of particularly malignant cyber operations. It is true that the scale of a cyber operation may determine whether or not it is congruous with an act of war in traditional definitions. Therefore, having some general criteria to clarify different types of legal responses under the Charter would set an important precedent as cyber conflicts happen even more frequently.

International lawmakers must take the Stuxnet operation as a warning. Many scholars argue that Stuxnet introduced a new type of warfare into our international arsenal. Without a scale or clearer guidelines for each specific kind of cyber operation, per the degree to each type of cyber operation endangers civilians, the more challenging it will be to designate and regulate activity that takes place in such an anarchic sphere as cyberspace.

## Bibliography:

### Legal Sources: Charters and Statutes


Charter of the International Military Tribunal at Nuremberg (82 U.N.T.S. 279 [1945]). http://avalon.law.yale.edu/imt/imtconst.asp

Charter of the North Atlantic Treaty Organization (1949). http://www.nato.int/nato_static/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf

Charter of the United Nations (1945). https://treaties.un.org/doc/Publication/CTC/uncharter.pdf

Convention (I) for the Pacific Settlement of International Disputes (Hague I). July 29, 1899. Available through *The Avalon Project: Yale Law School.* *http://avalon.law.yale.edu/19th_century/hague01.asp*

"Case Concerning the Military and Paramlitary Activities in and Against Nicaragua (*Nicaragua v. United States of America*)." International Court of Justice, 1986. http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence*. New York, New York: Cambridge University Press, 2013.


### Journal Articles


Baldwin, Simeon E. "The Proposed Trial of the Former Kaiser." *The Yale Law School Legal Scholarship Repository* (1919): 75-82. Web. <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5302&context=fss_papers>.

Buchan, Russell. "Explaining Liberal Aggression: The International Community and Threat Perception." *International Community Law Review* 12 (2010): 413-36. EBESCO.

Eriksson, Johnan and Giampiero Giacomello. "The Information Revolution, Secutity, and International Relations: (IR) Relevant Theory?" *International Political Science Review 3* (2006): 221-44. Accessed July 30, 2015. http://www.jstor.org/stable/20445053.

Farer, Tom. *A Paradign of Legitiamte Intervention, supra,* at 317-318.

Grossman, Levi. "Cyberattack Attribution Matters Under Article 51 of the UN Charter." *Brooklyn Journal of International Law* 36, no. 3 (2011): 1151-180.

Koskenniemi, Martti. "Histories of International Law: Significance and Problems for a Critical View." *Temple International and Comparative Law Journal*. Vol. 27, Issue 2. (2013): 215-240.

Kydd, Andrew H., and Barbara F. Walter. "The Strategies of Terrorism." *International Security* 31, no. 1 (Summer 2006): 49-80.

Langner, Ralph. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group, 2013.

Newton, Michael and Larry May. "Proportionality in International Law." From Proportionality in Human Rights Law and Morality. *Oxford University Press* (2014): 1-27.

Paulus, Andreas. "Second Thoughts on the Crime of Aggression." *The European Journal of International Law* ,Vol. 20 no. 4 (2010). 1117-1128. EBESCO.

Ratner, Steven R. "Aggression." *Crimes of War.* http://www.crimesofwar.org/a-z-guide/aggression/

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1-2 (2014): 4-37. Accessed October 27, 2015. http://dx.doi.org/10.1080/01402390.2014.977382.

Rosenberg, Tina. 1995. "Tipping the Scales of Justice". *World Policy Journal* 12 (3). [Sage Publications, Inc., Duke University Press]: 55–64. http://www.jstor.org/stable/40209427.

Sayapin, Sergey. *The Crime of Aggression in International Criminal Law.* TMC Asser Press, the Hague, The Netherlands. 2014.

Simma, Bruno. "NATO, the UN and the Use of Force: Legal Aspects." *European Journal of International Law*, 1999. http://www.ejil.org/pdfs/10/1/567.pdf

Solis, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War*. Cambridge: Cambridge University Press, 2010.

Toukan,, Abdullah, and Anthony H. Cordesman. "Study on a Possible Israeli Strike on

Iran's Nuclear Development Facilities." *Center for Strategic and International Studies*, March 14, 2009, 3-114. Accessed March 9, 2016. http://csis.org/files/media/csis/pubs/090316_israelistrikeiran.pdf.

Valeriano, Brandon, and Ryan C. Maness. "Cyber War versus Cyber Realities: Cyber Conflict in the International System." Oxford University Press Scholarship Online, 2015. Accessed August 30, 2015.

Vantanparast, Roxana. "International Law Versus The Preemptive Use of Force: Racing to Confront the Specter of a Nuclear Iran." *UC Hastings College of the Law Hastings International and Comparative Law Review* 31, no. 783 (2008). Lexis Nexis.

News Articles:

Ashford, Warwick. "Problems in Attributing Cyber Attacks Could Foil US Sanctions against Hackers." *Computer Weekly*, 2015.

Borger, Julian. "Iran Nuclear Deal: World Powers Reach Historic Agreement to Lift Sanctions." *The Guardian.* July 14, 2015. http://www.theguardian.com/world/2015/jul/14/iran-nuclear-programme-world-powers-historic-deal-lift-sanctions.

Fathi, Nazila. "Ahmadinejad Sees Nuclear Energy in Iran by 2009." *The New York Times.* January 30, 2008. http://www.nytimes.com/2008/01/31/world/middleeast/31iran.html?ex=1359522000.

Good, Chris. "How Many Nuclear Weapons Does the US Have? Don't Ask A Congressman." *ABC News*, June 21, 2013. http://abcnews.go.com/blogs/politics/2013/06/how-many-nuclear-weapons-does-the-us-have-dont-ask-a-congressman/

Mazzetti, Mark. "U.S. Finds Iran Halted Its Nuclear Arms Effort in 2003." *The New York Times.* December 03, 2007. http://www.nytimes.com/2007/12/04/world/middleeast/04intel.html?ex=1354510800.

Nakashima, Ellen, and Joby Warrick. "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say." *Washington Post.* June 2, 2012. Accessed June 7, 2015. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Perlroth, Nicole. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back." *The New*

*York Times*. October 23, 2012. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0.

Pruszewicz, Marek. "How Deadly Was the Poison Gas of WW1? - BBC News." *BBC News*. January 30, 2015. http://www.bbc.com/news/magazine-31042472.

Sanger, David E. "Limiting Security Breaches May Be Impossible Task for U.S. and China." *The New York Times*. September 25, 2015. Accessed September 25, 2015. http://mobile.nytimes.com/2015/09/26/world/asia/limiting-security-breaches-may-be-impossible-task-for-us-and-china.html?emc=edit_th_20150926.

Stark, Holger. "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War." *Der Spiegel.* August 8, 2011. http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html.

Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." *The Guardian*, May 16, 2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired.* July 11, 2011. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

Books:

Brenner, Joel. *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World*. Penguin, 2013.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. Oxford: Oxford University Press, 2009.

Cole, Darrell. *Just War and the Ethics of Espionage*. Routledge, 2015.

Dunoff, Jeffrey L., Steven D. Ratner, and David Wippman. *International Law: Norms, Actors, Process: A Problem-Oriented Approach*. New York, NY: Aspen, 2010.

Koppel, Ted. *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*. Crown, 2015.

Ruys, Tom. *"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice*. New York: Cambridge University Press, 2010.

Mearsheimer, John J. *The Tragedy Of Great Power Politics*. New York: Norton, 2001.

Morgenthau, Hans. *Politics Among Nations*. 4th ed. New York, 1948.

Singer, P.W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press, 2014.

Waltz, Kenneth N. *Theory of International Politics*. Reading, MA: Addison-Wesley Pub. 1979.

Walzer, Michael. *Just and Unjust Wars: A Moral Argument With Historical Illustrations*. New York: Basic Books, 1977.

Videos:

Langner, Ralph. TED Talk. 2013. http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber weapon/transcript?language=en#t-175983