Michael Fronte
Contemporary Issues as to Nuclear Weapons and International Law in the Post 9/11 World
Professor Charles Moxley

Megabyte vs. Megaton: Cyber Attacks, Nuclear Weapons, and the *Jus ad Bellum*

I. Introduction.

In June 2009, several Iranian companies with ties to the nuclear industry were infected with a mysterious computer virus.[1] This virus soon spread to the uranium enrichment plant in Natanz, after being inserted into the plant's network via a USB drive supplied by an unwitting company employee. Once inside the plant's network, the virus slowly began to carry out its objective. Corrupting the plant's control systems, the virus began to wreak havoc on the uranium enrichment centrifuges by causing them to randomly speed up and slow down.[2]

By November, the virus had successfully caused over 1,000 centrifuges to break down, and in January 2010 plant employees and inspectors from the International Atomic Energy Agency began to notice that the remaining centrifuges were starting to fail at an unprecedented rate.[3] What they were not aware of, at the time, was that the facility was under attack by a cyber weapon that the world has come to know as Stuxnet.

The Stuxnet attack, which has since been attributed to the United States and Israel[4], was the culmination of efforts beginning in 2006 to develop a cyber weapon that would assist in crippling Iran's efforts at nuclear proliferation.[5] It's success, though, has a much larger

[1] Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon,* WIRED (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[2] *Id.*
[3] *Id.*
[4] John Leyden, *US Officials Confirm Stuxnet was a Joint US-Israeli Op,* THE REGISTER (June 1, 2012), https://www.theregister.co.uk/2012/06/01/stuxnet_joint_us_israeli_op/.
[5] The development of Stuxnet was part of a larger program called "Olympic Games," which began under the Bush Administration and continued into the Obama Administration. David E. Sanger, *Obama Order Sped Up Wave of*

significance in that it was one of the first instances where cyber weapons were used to target physical nuclear infrastructure and cause it to break down.[6] The attack has thus heightened concerns over the risks that cyber weapons pose to nuclear weapons, especially given the recent global rise in the use of cyber attacks and cyber exploitation.[7]

In light of these concerns, this paper will analyze the risks that cyber attacks and exploitations pose to nuclear weapons and their supporting infrastructure. In doing so, this paper will also analyze the current state of international law surrounding cyberspace, particularly the application of the *jus ad bellum* to cyberspace. This area of law is notoriously ambiguous, and has essentially centered on a debate over whether new cyber treaties are needed or whether the existing legal regime can be harmonized with cyberspace.

The paper will thus proceed in three main parts. Part II will analyze the current threats that cyber attacks and exploitations pose to nuclear weapons. It will begin with a brief discussion of the primary cyber weapons employed by states and non-state actors, and will then focus on the cyber threats posed by both state and non-state actors. Part III will then analyze the application of the *jus ad bellum* to cyberspace.[8] This Part will focus on three specific issues that

---

Cyberattacks Against Iran, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[6] Prior to Stuxnet, cyber attacks were primarily used to cripple computer data, such as the massive 2007 cyber attack on Estonian banking, government, and communication networks. *See* Damien McGuinness, *How a Cyber Attack Transformed Estonia,* BBC (Apr. 27, 2017), http://www.bbc.com/news/39655415. Cyber attacks had also been used to disable networks in preparation for kinetic attacks, such as when Israel in 2007 hacked Syria's air defense radar to allow for an airstrike on a suspected Syrian nuclear reactor. *See* Sharon Weinberger, *How Israel Spoofed Syria's Air Defense System,* WIRED (Oct. 4, 2007), https://www.wired.com/2007/10/how-israel-spoo/; *see also* John Markoff, *Before the Gunfire, Cyberattacks,* N.Y. TIMES (Aug. 12, 2008) (describing the cyber attacks which took place before and during the 2008 Russian invasion of Georgia), http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[7] Based on this concern, over thirty countries now have taken steps to integrate cyber into military planning, including the United States. Stephen J. Cimbala, *Nuclear Deterrence in Cyber-ia: Challenges and Controversies*, 30 AIR & SPACE POWER J. 54, 55 (2016).

[8] It is important to note that there is a distinction between the *jus ad bellum*, which governs a state's right to initially use force, and the *jus in bello,* which regulates a state's conduct after hostilities have commenced. While this paper will focus on the *jus ad bellum,* there has been scholarly discussion on the application of the *jus in bello* to cyber space as well. *See, e.g.,* Stephen Petkis, Note, *Rethinking Proportionality in the Cyber Context,* 47 GEO. J. INT'L L.

pose difficulties in applying current law to cyberspace: self-defense, attribution, and cyber espionage. Finally, Part IV will discuss the possible benefits that a cyber treaty or treaties would offer, as well as the issues that would remain unresolved even with the creation of a treaty regime.

II. Threat Analysis.

A. Basic Definitions.

According to Thomas D'Agostino, the former head of the National Nuclear Security Administration, America's nuclear weapons face millions of cyber attacks daily from a "full spectrum" of attackers.[9] However, before describing in depth these cyber threats against nuclear weapons, it is worth discussing the difference between cyber attack and cyber exploitation. Further, it will be helpful to briefly describe the different types of cyber weapons commonly employed.[10]

1. Attack vs. Exploitation.

Currently, there is no international consensus on the definition of a cyber attack. Rather, scholars, experts, and governmental authorities have all offered definitions that differ in scope.[11]

1431 (2016); Michael Gervais, *Cyber Attacks and the Laws of War,* 30 BERKELEY J. INT'L L. 525 (2012); Michael N. Schmitt, *Cyber Operations and the* Jus in Bello: *Key Issues,* 41 ISR. Y.B. HUM. RTS. 113 (2011).

[9] Jason Koebler, *U.S. Nukes Face Up to 10 Million Cyber Attacks Daily,* U.S. NEWS (Mar. 20, 2012), https://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily. The attackers range from foreign governments to "fairly sophisticated" non-state actors. *Id.* However, despite the massive volume of attacks, only about 1,000 attacks a day are classified as "successful" penetrations. *Id.* These attacks also primarily consist of information theft or probing actions to detect vulnerabilities in the network. *Id.*

[10] An extensive explanation of how cyber weapons operate is beyond the scope of this paper. For more detail on cyber weapons, see *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD (2008), http://www.oecd.org/sti/40724457.pdf.

[11] From a scholarly point of view, Oona Hathaway et al. argue that cyber attack should be defined as "[a]ny action taken to undermine the functions of a computer network for a political or national security purpose." Oona A. Hathaway et al., *The Law of Cyber Attack*, 100 CALIF. L. REV. 817, 826 (2012). In a much more restrictive manner, security expert Richard A. Clarke defines cyber attack as "[a]ctions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or destruction." RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010); *see also* Peter J. Denning & Dorothy E. Denning, *The Profession of IT: Discussing Cyber Attack*, 53 COMM. OF THE ACM 29 (2010) (defining cyber attack as "deliberate actions against data, software, or hardware in computer systems or networks. The actions may destroy, disrupt, degrade, or deny access" and cyber exploitation as "intelligence-

There is more consensus, however, that a cyber attack is different from cyber exploitation. Because this paper will discuss each threat separately, cyber attack need only be defined to distinguish it from cyber exploitation. The former Vice-Chairman of the U.S. Joint Chiefs of Staff, General James Cartwright, provided such a distinction in a 2010 Memorandum addressed to the Joint Staff Directorates and Combatant Commands. This Memorandum defined cyber attack as "A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions."[12] In contrast, the Memorandum defined cyber exploitation as "Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data about target or adversary automated information systems or networks."[13] The main distinction between attack and exploitation, then, is the impact on the network or system. A cyber attack actively disables or interferes with a network or system, whereas cyber exploitation merely gathers information from the network or system.[14]

---

gathering rather than destructive activities. Cyber exploitation usually seeks the least intrusive, least detectable interventions into computing systems. The purpose is to acquire data without being seen or getting caught."). In contrast, Ashton Scheshan Gangadeen seems to eliminate the distinction between attack and exploitation by defining cyber attack as "the deliberate exploitation of computer information systems, infrastructures, computer networks, and/or personal computer devices by individuals or organisations using malicious codes in order to hack, steal, alter, or destroy). Ashton Scheshan Gangadeen, *Types of Cyber Attack,* SUPINFO INTERNATIONAL UNIVERSITY (Feb. 28, 2016), http://www.supinfo.com/articles/single/1626-types-of-cyber-attack.

[12] JAMES E. CARTWRIGHT, MEMORANDUM FOR CHIEFS OF THE MILITARY SERVICES, COMMANDERS OF THE COMBATANT COMMANDS, DIRECTORS OF THE JOINT STAFF DIRECTORATES 3 (2010), http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf. The Combatant Commands are U.S. military entities that oversee different regions of the globe. They consist of Northern Command (North America), Southern Command (South America), Pacific Command, European Command, Africa Command, and Central Command (The Middle East).

[13] *Id.* at 4 (defining "Computer Network Exploitation").

[14] Of course, the distinction between a cyber attack and cyber exploitation can be blurred where the cyber operation both gathers information and disables or interferes with a network. From the victim state's point of view, it can also be difficult to accurately assess whether a cyber operation is an attack or merely exploitation.

2. Cyber Weapons.

When state and non-state actors do carry out cyber attacks, there are a variety of tools that they can employ. One of the most widely used weapons is the Distributed Denial of Service (DDoS) attack. A DDoS attack uses computer code to take control of thousands of computers, which are then known as "zombies" or "bots." These infected computers are then programmed to simultaneously visit targeted websites, thereby disabling the servers by flooding them with traffic.[15] DDoS attacks are very attractive because they are cheap and difficult to trace back to the original attacker, as the computers infected can be scattered around the world.[16]

Aggressors may also make use of malicious programs, commonly known as malware.[17] Malware can disrupt computer functions through viruses and worms, or can allow a remote controller to take control of the computer.[18] For example, an attacker might use malware to infiltrate a computer network and then execute a desired operation. Such was the case during initial stages of Operation Iraqi Freedom, where the U.S. military infiltrated the Iraqi Defense Ministry email system and instructed Iraq commanders to peacefully surrender.[19]

B. Cyber Threats to Nuclear Weapons.

1. Threats From States.

The primary cyber threats that nuclear weapons face from state actors come in the form of disabling attacks. These attacks are aimed at eliminating or crippling a state's nuclear arsenal

[15] Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602, 623 (2011).
[16] Hathaway et al., *supra* note 11, at 838.
[17] The first malware was coded in 1986 by two brothers in Pakistan. Within a year of coding, the malware was virtually able to spread around the world. Catherine A. Theohary & Anne I. Harrington, *Cyber Operations in DOD Policy and Plans: Issues For Congress* 3, CRS R43848 (2015).
[18] Raboin, *supra* note 15, at 613.
[19] Hathaway et al., *supra* note 11, at 839. From a legal point of view, this example is interesting in that it is unclear as to whether the *jus ad bellum* or *jus in bello* would apply to the situation. The critical question is whether the U.S. was already engaged in hostilities when it infiltrated the email system. The infiltration did occur before the main U.S.-led invasion. *Id.* However, it could be argued that at the time of the infiltration hostilities had already commenced, given that CIA and Special Forces teams had been operating inside Iraq since 2002. *See* MIKE TUCKER & CHARLES S. FADDIS, OPERATION HOTEL CALIFORNIA: THE CLANDESTINE WAR INSIDE IRAQ (2010).

by preventing a state from launching, targeting, or detonating its nuclear weapons. This could be accomplished by using cyber weapons to directly disable nuclear weapons, or to indirectly disable the command, control and communications (C3) networks that nuclear weapons rely on. Cyber attacks could also be used to increase a state's chances of a successful nuclear strike by disabling an enemy state's missile defense systems.

The C3 of nuclear weapons states is particularly vulnerable to cyber attacks. While most nuclear weapons networks in the United States are "air gapped," meaning they are not connected to the mainstream Internet, this may not be the case for other states. More recent nuclear weapons states such as India and Pakistan, for example, may not have the extensive C3 security employed in the United States.[20] Further, cyber weapons are currently being developed to "jump" the air gap, and there have been cases in the past where C3 in the U.S. has been penetrated. In the 1990s, for example, hackers were able to penetrate the U.S. Navy's radio transmitters to ballistic missile submarines at sea.[21] Thus, with the proper technology and planning, it could be possible for a state to hack into a rival's communication system and generate false voice orders to stand down or not fire their weapons. Alternatively, the communication system could be penetrated and simply jammed to prevent launch orders from reaching personnel manning the nuclear triad.

A less likely, but still possible, scenario is where a state directly hacks another state's nuclear weapons and prevents them from launching. This has been a particular concern in the United Kingdom, whose entire nuclear arsenal consists of Trident missiles loaded onto a fleet of four Vanguard-class submarines. Recently, the British government chose to install a customized

[20] Erik Gartzke & Jon R. Lindsay, *Thermonuclear Cyberwar,* 3 J. CYBERSECURITY 37, 44 (2017).
[21] Bruce G. Blair, *Why Our Nuclear Weapons Can Be Hacked,* N.Y. TIMES (Mar. 14, 2017), https://www.nytimes.com/2017/03/14/opinion/why-our-nuclear-weapons-can-be-hacked.html. Thankfully, the Navy has redesigned the launch procedure so that orders must be verified before launch. *Id.*

form of the Windows operating system onto the submarines, rather than the older but less vulnerable Linux system.[22] As a result, critics now fear that the nuclear submarines are vulnerable to cyber attacks that can disrupt or disable their targeting systems.[23]

Besides targeting nuclear weapons themselves, a state could also target a rival's early warning systems or radar. Doing so could potentially cripple the rival's ability to detect incoming missiles or bombers, thereby making a successful first strike much more likely. Cyber attacks on early warning systems have taken place in the past, albeit on a smaller scale. In 2007, for example, Israel used a cyber attack to blind Syrian radar and prevent it from detecting Israeli fighter jets that were used to bomb a suspected Syrian nuclear reactor.[24] Russia in particular has also expressed concern over this scenario, as its early warning systems have been deteriorating since the fall of the Soviet Union.[25]

If the threats outlined above are carried out, they further run the risk of triggering an escalation that results in total nuclear war. This can result even where a cyber attack on a state's nuclear system is on a limited scale. Given the nature of cyber weapons, which are difficult to quickly and accurately detect and assess, a limited attack on C3 might be perceived as a prelude to a full kinetic strike. Military commanders and national leaders might then be convinced to launch all their nuclear weapons before a total disruption occurs (the classic "use 'em or lose 'em" scenario).

To illustrate this risk, assume that Syria had nuclear weapons when Israel conducted its air strike. The Syrian government might have interpreted the disruption of its radar as a prelude

---

[22] Andrew Futter, *Is Trident Safe from Cyber Attack?,* EUROPEAN LEADERSHIP NETWORK (Feb. 2016), https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/Is-Trident-safe-from-cyber-attack-1.pdf.
[23] *Id.*
[24] *See* Weinberger, *supra* note 6.
[25] JASON FRITZ, HACKING NUCLEAR COMMAND AND CONTROL 11 (2009), http://www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.pdf.

to a full-scale Israeli offensive. It might then have launched its hypothetical nuclear weapons, prompting a full nuclear exchange between Israel and Syria. The possibility of escalation also is heightened by the high-alert status in which the U.S. and Russia keep thousands of their nuclear weapons. A limited cyber attack by one of these states against the other, then, could potentially cascade into a full nuclear exchange in a matter of minutes.[26]

Even if these threats are not actually carried out, the mere possibility of occurrence can still result in a breakdown of stability between the nuclear powers. The idea of deterrence and Mutually Assured Destruction hinges on the principle that each side has no advantage and both are equally able to destroy the other. However, if one side theoretically has the ability to disable the other's nuclear weapons or prevent them from launching, that side would have the advantage in a nuclear war through a successful first strike or prevention of a second strike.[27] Theoretical cyber threats can thus be used as a justification for states to upgrade or expand their nuclear arsenals to make up for the threat posed by cyber attacks. Russia, for example, considers U.S. disruption of its C3 to be a huge threat, and has recently undertaken efforts to strengthen its nuclear arsenal.[28]

2. Threats From Non-State Actors.

Cyber threats can also come from non-state actors that are affiliated with or controlled by a state, as well as those that operate independently such as terrorist organizations. Because affiliated actors share similar objectives with state actors, this Section will focus on the cyber

[26] In light of this possibility, General James Cartwright has proposed that the U.S. response time for its nuclear weapons be changed from 3-5 minutes to as long as 24-72 hours. Franz-Stefan Gady, *Could Cyber Attacks Lead to Nuclear War?,* THE DIPLOMAT (May 4, 2015), https://thediplomat.com/2015/05/could-cyber-attacks-lead-to-nuclear-war/.

[27] This of course ignores the idea of Self Assured Destruction – the idea that even a one-sided use of nuclear weapons would create enough smoke and fire to cause nuclear winter. *See* Alan Robock & Owen Brian Toon, *Self-Assured Destruction: The Climate Impacts of Nuclear War,* BULLETIN OF THE ATOMIC SCIENTISTS (Sept. 1, 2012), https://thebulletin.org/2012/september/self-assured-destruction-climate-impacts-nuclear-war.

[28] Mark Hensch, *Putin: Russia Must Strengthen its Nuclear Arms,* THE HILL (Dec. 22, 2016), http://thehill.com/policy/international/russia/311536-putin-russia-must-strengthen-its-nuclear-arms.

threat to nuclear weapons by terrorists or other independent actors. These threats primarily come in the form of enabling attacks that aim to remotely detonate nuclear weapons or cause a state to launch its nuclear weapons at a particular target.[29]

Given that there are over 20,000 nuclear weapons in the world today located throughout Europe, the United States, and Asia, terrorist groups seeking to use nuclear weapons have a wide range of possible targets.[30] One of the largest cyber threats to nuclear weapons, besides direct sabotage and detonation, is the potential for terrorist groups to spoof a state's nuclear forces and convince them that they are under attack. For example, if the U.S. Minimum Essential Emergency Communications Network (MEECN) that links the elements of the nuclear triad were hacked, a terrorist group could generate false voice commands to launch or merely convince nuclear commanders that an attack was underway.[31]

Terrorist groups could also spoof a state's radar or early warning systems to indicate an incoming attack, thereby convincing the leadership of the necessity to launch. Early warning systems in the past have almost caused nuclear war as a result of bugs in the system[32], and Tom

[29] Such a possibility is enticing to terrorist groups because it could enable them to cause two enemy states to destroy themselves. Jihadists groups such as ISIS and al Qaeda, for example, detest both the United States and Russia. Causing these states to launch nukes at each other, then, would allow for the destruction of both enemies at once. Of course, it is also plausible that some states might want to conduct enabling attacks as well. Causing an enemy state's nuclear missiles to detonate on its own soil could reduce the need for the attacking state to use its own nuclear weapons, or at least would reduce the amount of weapons needed to be launched. Further, a state that has no nuclear weapons (or a limited arsenal) could theoretically use cyber attacks to hijack another state's nuclear weapons and use them for its own purposes.

[30] FRITZ, *supra* note 25, at 7-8.

[31] *See* Gartzke & Lindsay, *supra* note 20.

[32] In 1983, for example, the Soviet early-warning system detected an incoming American missile attack at a time of particular tension between the two countries. The Soviet leadership did not authorize a launch however, thanks to Air Defense officer Stanislav Petrov, who believed the attack was false and did not report it up the chain of command. Simon Shuster, *Stanislav Petrov, the Russian Officer Who Averted a Nuclear War, Feared History Repeating Itself,* TIME (Sept. 19, 2017), http://time.com/4947879/stanislav-petrov-russia-nuclear-war-obituary/. In 1980, a faulty computer chip caused U.S. early warning systems to display an incoming Soviet missile attack. While Strategic Air Command and the National Military Command Center were placed on high alert, they were eventually ordered to stand down once the warning systems showed no further signs of attack. UNION OF CONCERNED SCIENTISTS, CLOSE CALLS WITH NUCLEAR WEAPONS 4 (2015). A more recent example also took place in the U.S. in 2010, where a launch control facility lost communications with 50 high-alert ICBMs for an hour due

Collina of the Ploughshares Fund has stated that the biggest threat of nuclear war comes from a mistaken launch caused by bad data.[33] Thus, it is possible that these systems can be manipulated to indicate a nuclear attack. This is a particular concern when China or India are involved. Both countries use the same missile delivery systems for their nuclear warheads as they do for conventional warheads.[34] Thus, an erroneous launch of Chinese or Indian conventional weapons could still be wrongly interpreted as a nuclear attack and cause nuclear escalation.[35] Finally, the spoofing threat is also heightened by the superpowers' high-alert status. In the United States, for example, NORAD has only minutes to assess whether an attack is incoming, and after a short briefing the President also has several minutes to authorize a launch.[36] A terrorist group that successfully spoofs U.S. or Russian early warning systems, then, would only have to maintain this ruse for about 15 minutes until the missiles begin to fly.

Besides causing a launch or detonation, non-state actors (and some states) could potentially use cyber weapons to assist in the theft of a nuclear weapon. This is a particular concern with Indian nuclear weapons. To maintain unpredictability, India rotates its nuclear missiles throughout the country and makes use of dummy warheads for training purposes.[37] A

---

to a faulty circuit card. As a result, the launch facility lost the ability to detect and cancel any unauthorized launches. *Id.* at 4-5.

[33] Luke Moretti, *Safeguarding America's Nuclear Weapons From Emerging Cyber Threats,* WIVB 4 (Apr. 27, 2017), http://wivb.com/2017/04/27/safeguarding-americas-nuclear-weapons-from-emerging-cyber-threats/.

[34] FRITZ, *supra* note 25, at 13-14.

[35] *Id.* The U.S., as part of its Prompt Global Strike program, is also considering arming ballistic missiles with conventional warheads. However, military officials have recognized the potential issue that the use of such weapons could be mistaken as nuclear launches by states such as Russia and China. *See* Craig Whitlock, *U.S. Looks to Nonnuclear Weapons as Deterrent,* WASHINGTON POST (Apr. 8, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/04/07/AR2010040704920.html; AMY F. WOOLF, CONVENTIONAL WARHEADS FOR LONG-RANGE BALLISTIC MISSILES: BACKGROUND AND ISSUES FOR CONGRESS, CRS RL33067 (2009).

[36] BRUCE G. BLAIR, ACHIEVING THE VISION OF A WORLD FREE OF NUCLEAR WEAPONS: INCREASING WARNING AND DECISION TIME ('DE-ALERTING') (2008), http://disarmament.nrpa.no/wp-content/uploads/2008/02/Paper_Blair.pdf.

[37] *Id.* at 14; VERGHESE KOITHARA, MANAGING INDIA'S NUCLEAR FORCES 159 (2012).

terrorist group, then, could potentially use a cyber attack to relay false orders and cause a real nuclear weapon (believed to be a dummy) to be transported to a desired location.[38]

3. The Threat of Espionage.

Cyber exploitation, or espionage, is likely the most realistic threat facing nuclear weapons today, given that many of the threats discussed above require massive resources and can be prevented or mitigated by defensive measures such as human control and verification procedures.[39] Espionage against nuclear weapons, however, dates back to long before the development of the Internet and can be beneficial for both states and non-state actors.[40]

For states, cyber exploitation can be used to steal information on enemy nuclear weapon designs and their locations, as well as enemy early warning systems and defensive weaponry. An early example of such cyber exploitation occurred in 1986, when East German agents hacked into U.S. defense networks in an attempt to acquire information about President Reagan's Strategic Defense Initiative.[41] Such information can then be used to enhance the state's first strike capabilities or be used to develop strategies to eliminate the enemy's second strike capabilities. Returning to the U.K.'s Trident missiles, critics of the new Windows system also fear that a state could hack into the network to find the location of the four Vanguard submarines.[42] This could then be used to target the submarines and prevent Britain from having a second strike opportunity.

---

[38] FRITZ, *supra* note 25, at 14.
[39] *See infra* Part V.
[40] Nuclear espionage has occurred as far back as the 1940s, when scientists such as Theodore Hall and Klaus Fuchs stole information about the atomic bomb while working in the Manhattan Project and delivered it to the Soviet Union. *See* CHRISTOPHER ANDREW & VASILI MITROKHIN, THE SWORD AND THE SHIELD: THE MITROKHIN ARCHIVE AND THE SECRET HISTORY OF THE KGB 131-32 (1999).
[41] More recently, Chinese hacking groups have penetrated the networks of U.S. defense contractors to gain information on the THAAD and AEGIS missile defense systems. Chinese hackers also penetrated the network of the National Nuclear Security Administration during a 2005 operation called "Titan Rain." JASON R. FRITZ, CHINA'S CYBER WARFARE: THE EVOLUTION OF STRATEGIC DOCTRINE 46-47 (2017).
[42] Futter, *supra* note 22.

Non-state actors could also use cyber exploitation to steal a nuclear weapon. Terrorists, for example, could use cyber exploitation tools to develop fake identifications that could be used to physically steal a bomb. Cyber exploitation could then be used to gain access to any Permissive Action Link (PAL) codes that are required to detonate the weapon.[43] Alternatively, terrorists could use cyber exploitation to steal instructions on how to build a bomb. They could also use cyber exploitation to steal information necessary to gain access to radioactive material from civilian nuclear plants, which are less heavily guarded but still use similar types of radioactive material that are used in warheads.[44] Such stolen radioactive material could then be combined with conventional explosives to make a simpler, but still deadly, dirty bomb.[45]

As shown by the previous Sections, nuclear weapons and their supporting systems face a large number of cyber threats that could potentially result in escalation to nuclear war. While some of these threats are more credible than others[46], they have nonetheless prompted many nations to take steps towards upgrading their militaries' cyber defenses and capabilities.[47] More

[43] FRITZ, *supra* note 25, at 19.
[44] Civilian nuclear facilities in particular can be vulnerable to cyber exploitation and cyber attacks. Besides the Natanz facility that fell victim to Stuxnet, other facilities in the U.S., Korea, and Germany have also been penetrated by cyber weapons. *See* VESSELIN GIAUROV, THE CYBER-NUCLEAR SECURITY THREAT: MANAGING THE RISKS 4 (2017).
[45] FRITZ, *supra* note 25, at 19-20.
[46] Some scholars have argued that truly devastating cyber attacks such as those described above are currently not very realistic, given that they would require months of planning and would require an attacker to first penetrate the target system and then probe it for a weakness, all without being detected. *See* James Andrew Lewis, *Truly Damaging Cyberattacks Are Rare*, WASHINGTON POST (Oct. 10, 2013), https://www.washingtonpost.com/postlive/truly-damaging-cyberattacks-are-rare/2013/10/09/ae628656-2d00-11e3-b139-029811dbb57f_story.html?utm_term=.0c1a9c436aa3. Further, only a handful of countries currently possess the capabilities to carry out such attacks. *Id.* (listing the U.S., Britain, China, Russia, and Israel). Cyber threat skeptics have also pointed out that there has been no recorded instance of terrorist cyber attacks against nuclear power plants or related systems. *See* Dr. M. N. Sirohi, CYBER TERRORISM AND INFORMATION WARFARE (2015).
[47] In the United States, for example, President Obama in 2009 authorized the creation of the U.S. Cyber Command (CYBERCOM), which took over cyber defense responsibilities from the Air Force. U.S. GOVERNMENT ACCOUNTABILITY OFFICE, DEFENSE CYBERSECURITY: DOD'S MONITORING OF PROGRESS IN IMPLEMENTING CYBER STRATEGIES CAN BE STRENGTHENED 1 (2017). In 2015, the Department of Defense also published a Cyber Strategy that declared five strategic goals for cyberspace, such as the preparation of weapons and personnel to operate in cyber-degraded environments. *See* THE DEPARTMENT OF DEFENSE CYBER STRATEGY (2015)*; see also* DEPARTMENT

importantly for this paper, they have also heightened the legal debate over how and whether international law can be used to regulate cyber attacks and exploitation. This will be the subject of the next Part.

III. Legal Issues Concerning Cyber Weapons.

In light of the threats outlined above, there has been much debate among legal scholars over whether international law can be effectively used to regulate cyber attacks and cyber exploitation, or whether a new treaty regime is needed. This Part will discuss the ways in which international law, specifically the *jus ad bellum,* can be applied to cyberspace. More importantly though, it will discuss the challenges and ambiguities surrounding the application of the *jus ad bellum* to cyberspace. As such, this Part will in turn discuss three areas that present major issues to the application of the *jus ad bellum* to cyberspace: self-defense, attribution, and espionage.

A. Self-Defense.

1. The *Jus ad Bellum.*

The *jus ad bellum (*right to use force) governs relations between states and determines situations in which it is deemed lawful to use force.[48] It is not a codified body of law, but rather primarily consists of portions of the United Nations Charter as well as customary international

---

OF DEFENSE DEFENSE SCIENCE BOARD, TASK FORCE ON CYBER DETERRENCE (2017) (identifying many of the threats already discussed and recommending, *inter alia,* an annual assessment of the cyber resilience of the nuclear forces.). In Russia, President Putin has recently issued Presidential Decree No. 646, which updates Russia's cyber strategy that was originally implemented in 2000 and first updated in 2014. Eugene Gerden, *New Cyber Defense Doctrine Approved by Russian Government,* SC MEDIA (Jan. 6, 2017), https://www.scmagazineuk.com/new-cyber-defence-doctrine-approved-by-russian-government/article/630032/. In China, the Ministry of National Defense released a military strategy white paper in 2015 that recognized the growing threats in cyberspace. The strategy stated in part that "[a]s cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation." *Document: China's Military Strategy,* USNI NEWS (May 26, 2015), https://news.usni.org/2015/05/26/document-chinas-military-strategy. However, as of July 2017 only about 38% of all states have a published cyber strategy, with an additional 12% of states in the process of developing one. *Half of All Countries Aware But Lacking National Plan On Cybersecurity, UN Agency Reports,* UN NEWS CENTRE (July 5, 2017), http://www.un.org/apps/news/story.asp?NewsID=57119#.WgDi3xNSx1M.

[48] Dimitar Kostadinov, *Fitting Cyber Attacks to Jus ad Bellum- Instrument Based Approach*, INFOSEC INST. (July 11, 2013), http://resources.infosecinstitute.com/fitting-cyber-attacks-to-jus-ad-bellum-instrument-based-approach/.

law.[49] Arguably the two most relevant articles of the U.N. Charter, for both the *jus ad bellum* and this paper, are Article 2(4) and Article 51.

Under Article 2(4), "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity and political independence of any state."[50] 2(4) thus imposes a blanket prohibition on any use of force by one state against another. This prohibition is then subject to an exception in Article 51, which states that "[n]othing 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."[51] When analyzed together, a critical distinction appears between Article 2(4)'s reference to "use of force" and Article 51's reference to "armed attack." This distinction has been interpreted to mean that certain activities can constitute a use of force without rising to the level of armed attack. Therefore, under the U.N. Charter a nation is entitled to defend itself only when it is subject to force that crosses the armed attack threshold.[52]

2. Application to Cyberspace - Choosing the Right Approach.

Though Articles 2(4) and 51 are easily stated, their application to both real and hypothetical cyber attacks has been notoriously difficult. This is because the nature of cyber weapons makes it unclear as to whether a use of force has occurred and whether such force has risen to the level of armed attack. Unlike a kinetic attack with explosives, which can easily be detected and its effects easily assessed, the commencement of a cyber attack can be difficult to detect in a short amount of time. Further, the total effects of a cyber attack can be difficult to

[49] *Id.*
[50] U.N. Charter art. 2, ¶ 4.
[51] U.N. Charter art. 51. The prohibition on the use of force, and the right of self-defense, are also both considered part of customary international law. Thus, they are binding on all states, even those that are not parties to the U.N. Charter. Further, states are additionally permitted to use force if such force is authorized by the Security Council. *See id.* arts. 42 & 45.
[52] *See* Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 VILL. L. REV. 569, 587 (2011).

assess, and there may also be unintended effects that cause a cyber attack to spread rapidly beyond its primary target. Stuxnet, for example, eventually spread to other computers in the Middle East despite only being targeted towards the Natanz facility.[53]

Given such difficulties, there has been much debate over how a cyber attack should be analyzed to determine whether a use of force, and then an armed attack, has occurred. The current law, enshrined in the *Case Concerning the Military and Paramilitary Activities In and Against Nicaragua* before the International Court of Justice (ICJ), provides little guidance.[54] In that case, the ICJ held that the United States committed uses of force against Nicaragua when, *inter alia,* it laid mines in Nicaraguan harbors and when it organized or encouraged the *contra* rebels to take part in acts of civil strife.[55] However, the ICJ provided little in the way of defining "use of force," nor did it explicitly lay out the types of attacks that would be considered uses of force. Further, when determining whether the U.S. uses of force rose to the level of armed attack, the ICJ merely held that only the "most grave" uses of force rise to the level of armed attack.[56] The ICJ then provided the example of an armed attack where regular armed forces attack across an international border, or where irregular forces sent by a state commit an attack whose "scale and effects" would have made it an armed attack if carried out by regular forces.[57]

The ICJ's ruling obviously leads to ambiguities when applied to cyber attacks. First, it is unclear as to whether the *Nicaragua* case holds that only kinetic, or at least traditional, uses of force can be considered armed attacks, given that the ICJ used the example of sending troops

---

[53] *See* Vincent Manzo, *Stuxnet and the Dangers of Cyber War,* THE NATIONAL INTEREST (Jan. 29, 2013), http://nationalinterest.org/commentary/stuxnet-the-dangers-cyberwar-8030.
[54] Case Concerning the Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States), [1986] I.C.J. 14.
[55] *Id.*
[56] *Id.* at para. 191.
[57] *Id.* at para. 195. In contrast, the ICJ suggested that mere "frontier incidents" conducted by regular armed forces would be considered a use of force but not an armed attack. However, the court neglected to elaborate on what constitutes a "frontier incident."

across the border. Second, the decision on its own is unclear as to whether the gravity or "scale and effects" of a use of force take only physical effects into account. As a result, three proposed approaches have been put forth for determining whether a cyber attack is a use of force or armed attack.

The first, known as the instrumentality approach, focuses on the type of weapon used.[58] Under this approach, the use of some types of weapons but not others will trigger the use of force and possibly armed attack. While this approach could provide a sense of clarity, it would be ineffective for regulating cyber attacks. First, it could be used to hold that only kinetic weapons trigger the use of force, thereby giving states free reign to conduct cyber attacks. Second, attempts to include some cyber weapons but not others would present too many technical issues, especially given that cyber weapons can be upgraded and evolved from previous versions.

The second approach is known as the strict liability approach. Under this approach, cyber attacks are automatically considered armed attacks and trigger the right to self-defense.[59] However, this approach is also problematic. While this approach would relieve states from having to undertake a difficult legal analysis of whether a cyber attack rose to the level of armed attack, it could also potentially result in hasty action and escalation. This is particularly a concern where nuclear weapons are the target. For example, if State A's nuclear weapons were penetrated by a cyber weapon looking for information, State A might erroneously interpret this as a cyber attack rather then cyber exploitation. Then under strict liability, State A could claim that it was suffering an armed attack against its nuclear weapons and retaliate with a conventional strike that could escalate into nuclear war.

[58] David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 MINN. J. INT'L L. 347, 363 (2013).
[59] JACKSON MAOGOTO, TECHNOLOGY AND THE LAW ON THE USE OF FORCE: NEW SECURITY CHALLENGES IN THE TWENTY-FIRST CENTURY 57 (2015).

The third approach is known as the consequences-based approach. This approach, echoing the *Nicaragua* case, focuses on the effects of a cyber attack to see whether these effects rise to the level of a kinetic use of force. This approach has the widest base of support and has been adopted in the influential *Tallinn Manual on the International Law Applicable to Cyber Operations* (the "*Tallinn Manual"*).[60] Created by a group of international law experts supervised by NATO and the Red Cross, the *Tallinn Manual* is a scholarly project that lays out proposed black letter rules concerning the application of international law to cyberspace.

Regarding use of force, Rule 69 of the *Tallinn Manual* states 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."[61] The rule then provides a non-exhaustive eight-factor test for determining whether a cyber attack is a use of force. The factors are: 1) Severity: while attacks involving physical harm will be uses of force, the "scope, duration and intensity" of non-physical effects can also rise to the level of force; 2) Immediacy: cyber attacks that manifest consequences sooner are more likely to be considered uses of force; 3) Directness: the more causation between an initial cyber attack and its consequences, the more likely it will be considered a use of force; 4) Invasiveness: the more secure the system that the cyber attack penetrates, the more likely it will be considered a use of force; 5) Measurability: the more quantifiable and identifiable the consequences, the more likely the cyber attack will be considered a use of force; 6) Military Character: the greater nexus between a cyber attack and a military operation, the more likely it will be considered a use of force; 7) State Involvement: the greater nexus between a state actor and a cyber attack, the more likely it will be considered a use

[60] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2d ed. 2017).
[61] *Id.* at 330.

of force; and 8) Presumptive Legality: cyber attacks that are presumptively legal under international law are less likely to be considered uses of force.[62]

Regarding armed attack, Rule 71 of the *Tallinn Manual* states in part that "[w]hether a cyber operation constitutes an armed attack depends on its scale and effects."[63] Thus, the *Tallinn Manual* takes the ICJ approach to assessing whether a use of force rises to the level of armed attack. The *Manual* further establishes clear cases where a cyber attack would be considered an armed attack, such as when a cyber operation "seriously injures or kills a number of persons or . . . causes significant damage to, or destruction of, property."[64] However, the *Manual* admits that the current law is "unclear as to the precise point at which the effects of a cyber operation qualify that operation as an armed attack."[65]

The consequences-based approach of the *Tallinn Manual*, while it offers the most comprehensive approach to analyzing cyber attacks, leaves many issues unsettled. First, while the use of force factors may implicate a range of cyber attacks, it is unclear as to how many factors need to be satisfied, as well as at what point a cyber attack actually satisfies each factor. Second, the *Manual*'s approach to the "armed attack" analysis does little to resolve the ambiguities. The *Manual*'s clear examples of armed attack involve death or physical destruction. However, there are possible cases where cyber attacks may only disrupt a network or device's data or operating system, such as an attack that spoofs an early warning system or disrupts a nuclear missile's targeting system. These attacks could have drastic effects, but the

[62] *Id.* at 334-36. Based on these factors, there was uniform agreement among the *Tallinn Manual* experts that the Stuxnet attack, which physically damaged the uranium centrifuges, was a use of force. Disagreement arose, however, over whether the attack actually rose to the level of an armed attack. *Id.* at 342.
[63] *Id.* at 339.
[64] *Id.* at 341.
[65] *Id.*

Manual does not provide a view as to whether such attacks could be considered armed attacks.[66] Rather, the *Manual* points out that some experts believed that physical harm to persons or property is a condition precedent to an attack being classified as an armed attack.[67] Such an approach, though, would mean that many potentially devastating cyber attacks on nuclear weapons or missile defense, which could have little physical impact, would not entitle a victim state to exercise its right of self-defense. In view of this, other experts believed that a cyber attack's classification as an armed attack depends on the extent of its total effects, whether physical or non-physical.[68]

While the latter view is more expansive, it leads to further issues as to which "effects" are to be taken into account when classifying an attack as an armed attack. For example, assume that a state launches a Stuxnet-style attack on another state's nuclear facility and disables its centrifuges. As a result, the victim state is unable to produce enriched uranium for use in nuclear weapons. At the same time though, the victim state is now unable to supply fuel for its nuclear power plants, leading many citizens to suffer from a lack of electricity. When evaluating the attack, the question then arises as to whether the indirect effects on civilians from the loss of electricity would be considered an "effect." If it is considered an effect, it is more likely, depending on how the civilians were impacted, that the attack would be considered an armed attack.[69]

---

[66] The comments to Rule 71 admit that "the case of cyber operations that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects, remains unsettled." *Id.* at 342.
[67] *Id.*
[68] *Id.* at 342-43. As an example, these experts said that a cyber attack against a major international stock exchange would cause catastrophic effects that would qualify it as an armed attack.
[69] In the *Tallinn Manual,* the experts were able to agree that only the "reasonably foreseeable consequences" should be considered when evaluating the effects of a cyber attack. *Id.* at 343. However, the hypothetical above raises an additional issue as to whether intent plays a role in the evaluation as well. If intent was required, then the hypothetical attack above might not be considered an armed attack if it was only intended to cripple the victim state's ability to produce a nuclear weapon. A majority of the *Tallinn Manual* experts believed, though, that intent is irrelevant when classifying an operation as a cyber attack. *Id.* at 343-44.

3. A Valid Response.

Assuming that a cyber attack does rise to the level of armed attack, further issues are presented regarding the validity of a response in self-defense.[70] Self-defense under the *jus ad bellum* must satisfy the elements of necessity and proportionality. Necessity requires that non-forceful responses must be futile or have been exhausted in an unsatisfactory manner.[71] Proportionality requires that the response have a modicum of symmetry with the original armed attack.[72]

Turning to necessity, the element further requires that a response not be carried out too late after an armed attack has occurred. This immediacy requirement poses a problem for cyber attacks. There is currently no international standard as to how quickly a response must take place after an armed attack occurs.[73] One possible point of reference is that the U.S. response to 9/11 occurred over a month after the attacks occurred. However, a comparison to responses to kinetic attacks would be inappropriate for assessing immediacy for cyber attacks. This is because a cyber attack might not be discovered until weeks or months after it began. With Stuxnet, for example, the scientists at Natanz were unaware for months that the virus was

[70] If a use of force does not rise to the level of armed attack, a state could potentially respond by employing countermeasures against the attacking state. Countermeasures are actions, otherwise unlawful, that a victim state can carry out against the attacking state for the purpose of inducing the attacking state to cease its illegal activities. *See* UNITED NATIONS, MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTENTIONALLY WRONGFUL ACTS 304-06 (2012), http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf. The *Tallinn Manual* permits the use of countermeasures in Rule 20, which states that "[a] State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another state. TALLINN, *supra* note 60, at 111; *see also id.* at 116 ("Countermeasures, whether cyber in nature or not, may only be taken to induce a responsible State to comply with the legal obligations it owes an injured State."). However, the *Manual* does not grant states the right to enact countermeasures against non-state actors, unless there has been attribution to a state. *Id* at 113. For further discussion on the use of countermeasures in the cyber context, see Marco Roscini, *Cyber Operations as Nuclear Counterproliferation Measures,* 19 J. CONFLICT & SEC. L. 133 (2014); Kenneth Watkin, *The Cyber Road Ahead: Merging Lanes and Legal Challenges,* 89 INT'L L. STUD. 472, 500-04 (2013); Mary Ellen O'Connell, *Cyber Security Without Cyber War,* 17 J. CONFLICT & SEC. L. 187 (2012).

[71] Weissbrodt, *supra* note 58, at 364-65.

[72] *Id.*

[73] YAROSLAV RADZIWILL, CYBER-ATTACKS AND THE EXPLOITABLE IMPERFECTIONS OF INTERNATIONAL LAW 146 (2015).

affecting the centrifuges. Further, the perpetrator of a cyber attack, thanks to anti-attribution technology, might not be discovered for weeks, months, or possibly years after the cyber attack has subsided. Thus, any immediacy evaluation regarding cyber attacks should employ some form of reasonableness standard, given the unique detection and attribution issues posed by cyber attacks.

Turning to proportionality, the law is also unclear as to whether cyber attacks can only be responded to with retaliatory cyber attacks. If this is the case, it is further unclear as to whether a state which has no comparable cyber capabilities to its attacker can respond with kinetic force, and if so how much kinetic force would be considered proportionate to a purely cyber attack. If cyber attacks can be responded to with other methods of force, a question arises as to whether nuclear weapons could be used in response to a cyber attack. Such a question would most likely arise if a state's nuclear weapons suffered a crippling cyber attack, or if the state suffered a massive cyber attack that crippled critical national infrastructure. The Department of Defense's Task Force on Cyber Deterrence has in fact considered this question, and has recommended that the United States reserve the right to respond to a cyber attack with a full range of capabilities. Further, the Department's Task Force on Resilient Military Systems more explicitly considered the possibility of the use of nuclear weapons in response to a full-spectrum cyber attack.[74]

The ICJ's *Legality of the Threat or Use of Nuclear Weapons* decision may help to answer this question. In that case, the ICJ held that the use of nuclear weapons would generally be unlawful, but did not answer the question of whether nuclear weapons could be used in "extreme

[74] DEFENSE SCIENCE BOARD, *supra* note 47, at 14; DEPARTMENT OF DEFENSE DEFENSE SCIENCE BOARD, TASK FORCE REPORT: RESILIENT MILITARY SYSTEMS AND THE ADVANCED CYBER THREAT 85 (2013). In Russia too, at least one academic has suggested that Russia has the right to respond to a cyber attack with nuclear weapons. Scott J. Schackelford, *From Nuclear War To Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 216 (2009).

circumstances" where the very survival of the nation was at stake.[75] Thus, the use of nuclear weapons, given their massive destructive power, inability to distinguish civilians, and lingering radioactive effects, would most likely be disproportionate to a cyber attack that was targeted against data systems, limited in its scope, and reversible. It remains unclear, though, whether a full-scale cyber attack that totally disables a state's infrastructure and results in civilian deaths[76], or a cyber attack that totally disables the state's conventional military apparatus, could qualify as "extreme circumstances" that would enable the state to respond with nuclear weapons. Yet even if such a cyber attack does qualify as "extreme circumstances," the fact that the ICJ declined to rule on this issue means that the legality of a nuclear response remains questionable.

Self-defense also raises an issue regarding whether a response against an independent non-state actor is permitted. Currently, there is ambiguity over whether an independent non-state actor can commit an armed attack against a state, thereby justifying a response against the actor. Among legal scholars, there is growing recognition that states have the right to act in self-defense in response to an armed attack committed by a non-state actor, even if that response takes place in the territory of another state. The majority of experts who created the *Tallinn Manual,* for example, endorsed this view in the commentary to Rule 71.[77] These experts argued that there is emerging state practice accepting such a right to respond to a non-state actor, and cited the U.S. response to al Qaeda after 9/11 as an example.[78] However, the ICJ has yet to

[75] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, [1996] I.C.J. 226, para. 97.
[76] While no state currently appears to have the ability to launch such a devastating cyber attack, such an attack that results in widespread death is plausible. For example, a cyber attack could be used to shut down hospitals and power grids, disable air traffic control to cause aerial collisions, cause nuclear power plants to melt down, and disrupt the banking and financial system to cause general panic.
[77] *See* TALLINN, *supra* note 60, at 345.
[78] *Id.* Other scholars have also approved of this view in a non-cyber context. *See, e.g.,* David Kretzmer, *The Inherent Right to Self-Defense and Proportionality in* Jus ad Bellum, 24 EURO. J. INT'L L. 235, 244-47 (2013); Christopher Greenwood, *International Law and the Pre-Emptive Use of Force: Afghanistan, Al-Qaeda, and Iraq,* 4 SAN DIEGO INT'L L.J. 7 (2003); Carsten Stahn, *Terrorist Acts as "Armed Attack:" The Right to Self-Defense, Article 51 (1/2) of the UN Charter, and International Terrorism,* 27 FLETCHER FORUM OF WORLD AFFAIRS 35 (2003).

endorse this view. In its advisory opinion *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* the ICJ held that "[a]rticle 51 . . . recognizes the existence of an inherent right of self-defense in the case of armed attack by one State against another State. However, Israel does not claim that the attacks against it are imputable to a foreign state."[79] Thus, the ICJ seems to believe that only states can commit armed attacks against other states.[80]

Based on the increasing ability of non-state actors to carry out devastating attacks against states, it makes sense to give states the right to respond to an armed attack by a non-state actor. However, even if this does crystalize as an international norm, such a response would still have to satisfy necessity and proportionality. Because necessity requires the exhaustion of non-forceful responses, the victim state should first be required to work with the state harboring the attacker to respond to the threat. Then, if a forceful response is necessary, under proportionality this response should take care to limit its focus to the non-state actor and limit damage to civilian and state property. This would be a particular issue for a cyber response, given that cyber attacks have the potential to spill over into civilian networks and cause indiscriminate damage.

B. Attribution.

In order for a state to respond to an armed attack, it must know who actually carried out the armed attack. However, the attribution of an armed attack to a particular actor has been described by cybersecurity expert Daniel Silver as the most important obstacle to applying the *jus ad bellum* to cyberspace. This is because cyber attacks are extremely difficult to accurately attribute. Thanks to the use of proxies, anonymizers, spoofed IP addresses and weapons that hijack computers in remote locations, cyber attackers are able to hide their identities and make it extremely difficult, or sometimes impossible, to trace the attack back to them. Such attribution

[79] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, [2004] I.C.J. 136, para. 139.
[80] A minority of experts endorsed this view as well in the *Tallinn Manual.* TALLINN, *supra* note 60, at 345.

difficulties raise issues for cyber attacks that are committed by state actors as well as non-state actors.

1. State Actors.

In the 2003 *Case Concerning Oil Platforms,* the ICJ held that a state invoking self-defense has the burden of demonstrating that another state committed an armed attack against it.[81] However, the evidentiary standard for this demonstration remains unclear. In *Oil Platforms,* the ICJ did suggest that attribution must be supported by a "balance of evidence," though it was not explicit as to whether this was a formal legal standard of proof.[82] In *Nicaragua,* the ICJ stated that, in determining whether a claim is well founded in facts and law, the Court must decide whether the facts are supported by "convincing" evidence.[83]

Thus, there are potentially two competing standards of proof for determining attribution to a state, and the choice of which to use could have major ramifications in the case of a cyber attack. Because the attribution of a cyber attack may be difficult to obtain in a reasonable amount of time with certainty, a lower standard of proof such as the "balance of factors" standard would enable states to more effectively respond to cyber attacks without being inhibited by stringent legal obstacles.

At the same time though, a more restrictive evidentiary standard such as the "convincing evidence" standard might be preferable in more dire situations such as when nuclear weapons are targeted. Anti-attribution technologies, as well as the ability to make a cyber attack appear as if it originated in another state, increase the risk that a state will erroneously act in self-defense against an innocent state. When nuclear weapons are targeted in a cyber attack, such error could

[81] Case Concerning Oil Platforms (Iran v. United States), [2003] I.C.J. 161, para. 57.
[82] *Id.*; Christian Payne & Lorraine Finlay, *Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack*, 49 GEO. WASH. INT'L L. REV. 535, 558 (2017).
[83] Case Concerning Military and Paramilitary Activities In and Around Nicaragua (Nicaragua v. United States), [1986] I.C.J. 14, para. 29.

potentially have drastic consequences through a missile launch or heavy kinetic strike that escalates into a war. Thus, a higher evidentiary standard could be imposed in more dangerous situations such as when nuclear weapons or other military assets are attacked. This would prevent a state from acting in self-defense until it is sufficiently certain that the cyber attack was launched by the target state.

2. Non-State Actors.

Arguably one of the most critical legal issues involving cyber attacks today is the standard for proving responsibility when a non-state actor that is controlled by a state commits a cyber attack. Currently, only state actors have the massive resources and technical expertise to carry out the harmful cyber attacks presented in Part II. However, states today primarily rely on non-state actors to carry out cyber operations, so as to further reduce the chance of detection. The Estonia attack, for example, has been attributed to Russian political hacker gangs rather than any Russian military or government agencies.[84] Thus, once an attack can be attributed to a non-state actor, the key question becomes how much proof is needed to hold a state actor responsible for the attack.

Under Article 8 of the International Law Commission's Draft Articles on State Responsibility, "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[85] However, the Draft Articles did not define "control," and as a result two different standards have developed based on the ICJ's *Nicaragua* case and the *Prosecutor v. Tadic* case before the International Criminal Tribunal for the Former Yugoslavia (ICTY).

[84] Mark Galeotti, *The Kremlin's Newest Hybrid Warfare Asset: Gangsters,* FOREIGN AFFAIRS (June 12, 2017), http://foreignpolicy.com/2017/06/12/how-the-world-of-spies-became-a-gangsters-paradise-russia-cyberattack-hack/.
[85] Draft Articles On Responsibility of States For Intentionally Wrongful Acts art. 8.

In *Nicaragua,* the ICJ held that attributing the actions of the *contras*, and therefore overall responsibility, to the United States required proof that "[the U.S.] had effective control of the military or paramilitary operations in the course of which the alleged violations were committed."[86] The ICJ then found that the U.S. was responsible for the *contras'* actions by "training, arming, equipping, financing, and supplying the contra forces, or otherwise encouraging, supporting, and aiding military and paramilitary activities in and against Nicaragua."[87] The ICJ's "effective control" test, therefore, places a high burden on a victim state to show extensive support by a state to a non-state actor.

In *Tadic,* the ICTY when discussing state responsibility held that "control by a State over subordinate armed forces or militias or paramilitary units may be of an overall character (and must comprise more than the mere provision of financial assistance or military equipment or training). This requirement, however, does not go so far as to include the issuing of specific orders by the state, or its direction of each individual operation."[88] Thus, the *Tadic* "overall control" test does not impose as many factors to take into account when analyzing state responsibility and is considered to be a lower standard than the "effective control" test. As a result, it has been argued that the "overall control" test should be used in cyber attack attribution cases given the difficulties of accurately tracing the origins of the attack. The advantages and disadvantages of adopting this test are similar to those discussed above regarding the adoption of an evidentiary standard for state actors. A lower "overall control" test would obviously give states more of an opportunity to respond to a cyber attack where it does not have as much evidence that a non-state actor was controlled by a state. At the same time though, the lower standard again raises the risk of an erroneous attribution escalating into a war.

[86] *Military and Paramilitary Activities*, at para. 115.
[87] *Id.* at para. 3.
[88] Prosecutor v. Tadic, No. IT-94-1-A, para. 137 (1999).

Situations may also arise where a state maintains little to no links with a non-state actor in order to establish plausible deniability. In these instances, attribution under either the "effective control" test or the "overall control" test would be near impossible to prove. As a result, several scholars have proposed new standards that would make it easier for a state to attribute a non-state actor's cyber attack back to the host state. Michael Schmitt, who played a large role in the creation of the *Tallinn Manual,* has advocated a standard where a state will be responsible if it fails to take reasonably available measures to stop cyber attacks originating in its territory.[89] Vincent-Joel Proulx, in contrast, has imposed a stricter liability standard by shifting the burden to the host state to show that it has taken reasonable measures to prevent attacks by those acting within its territory.[90]

While both proposals again provide more opportunity to respond to a cyber attack, they raise concerns over what exactly would constitute "reasonable measures." Discovering a terrorist network that is stockpiling weapons in preparation for an attack is much easier to detect than a group preparing to launch a cyber attack on another state. For one, members of the group never have to physically meet to carry out the cyber attack. In addition, a state may contain millions of computers, any one of which can contain a cyber weapon easily hidden in an email or data file. Thus, standards requiring states to take "reasonable measures" to detect and combat cyber attacks emanating from their territory might consequently end up placing too high a burden on these host states.

C. Espionage.

The unique characteristics of cyber espionage warrant some attention to potential legal issues surrounding the tactic. There has been great disagreement over whether peacetime

[89] Schmitt, *supra* note 52, at 580.
[90] Vincent-Joel Proulx, *Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?*: 23 BERKELEY J. INT'L L. 615, 656 (2005).

espionage is legal under international law.[91] Some scholars have maintained that peacetime espionage is illegal under international law, based on theories such as violation of the principle of non-intervention in the territory of another state.[92] Others have taken a more neutral view that espionage is neither legal nor illegal under international law.[93]

In contrast to these viewpoints, some scholars have argued that peacetime espionage is actually permitted under international law.[94] As a result, states will typically criminalize espionage under domestic laws, prosecute spies caught within their jurisdiction, and rely on extradition treaties to bring in spies operating outside their jurisdiction.[95] Under this view, cyber espionage is often considered to be no different than traditional espionage and therefore permitted under international law.[96] The *Tallinn Manual* seems to endorse this approach in its Rule 32, which states that "[a]lthough peacetime cyber espionage by States does not *per se* violate international law, the method by which it is carried out might do so."[97]

---

[91] The distinction between peacetime and wartime espionage is critical, as espionage conducted during a war is regulated by the laws of war. *See* Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law,* 28 MICH. J. INT'L L. 625, 626-27 (2006).

[92] *See, e.g.,* Russel Buchan, "Cyber Espionage and International Law," *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 180-89 (Nicholas Tsagourias & Russel Buchan eds., 2015); Ingrid Delupis, *Foreign Warships and Immunity for Espionage,* 78 AM. J. INT'L L. 53 (1984).

[93] *See, e.g.,* Daniel B. Silver, *Intelligence and Counterintelligence, in* NATIONAL SECURITY LAW 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005); Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach,* 19 AM. U. INT'L L. REV. 1091 (2004).

[94] *See, e.g.,* Cmdr. Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law,* 46 A.F. L. REV. 217 (1999); Lt. Col. Geoffrey B. Demarest, *Espionage in International Law,* 24 DENV. J. INT'L L. & POL'Y 321 (1996).

[95] In the U.S., espionage is criminalized under 18 U.S.C. Section 792 *et seq.* Aldrich Ames, for example, pled guilty to conspiring to spy for a foreign government (the Soviet Union) in violation of 18 U.S.C. Section 794(c). Ames v. United States, 155 F. Supp. 2d 525 (E.D. Va. 2000). In a more cyber-relevant example, the FBI has alleged that Edward Snowden violated 18 U.S.C. Section 798, which prohibits, *inter alia,* the furnishing of communications intelligence or cryptographic information for the benefit of a foreign nation to the detriment of the United States. 18 U.S.C. § 798(a)(1)-(3); *see also* Tung Yin, *Is Edward Snowden Guilty of US Espionage Charges?,* JURIST (July 16, 2013), http://www.jurist.org/forum/2013/07/tung-yin-edward-snowden.php.

[96] *See, e.g.,* DEPARTMENT OF DEFENSE LAW OF WAR MANUAL para 16.3.2 (2016) ("to the extent that cyber operations resemble traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, then such cyber operations would likely be treated similarly under international law.").

[97] TALLINN, *supra* note 60, at 168.

However, if espionage is currently not illegal under international law, the differences between cyber espionage and traditional espionage have led some to argue that cyber espionage should be more heavily regulated. For one, modern technology enables computers to store massive amounts of data. Consequently, cyber espionage enables a perpetrator to quickly download and steal massive amounts of data. Traditional human espionage, by contrast, requires an agent to physically acquire information by copying it, photographing it, or memorizing it.

Further, cyber espionage makes it much easier for a perpetrator to remotely steal information without ever stepping foot on the victim state's territory. As a result, the victim state is often unable to automatically prosecute the perpetrator, and has to rely on the cooperation of the state where he is located. The biggest issue, however, is that cyber espionage tools are often difficult to distinguish from cyber attack tools and can potentially be upgraded to carry cyber attack capabilities. As a result, cyber espionage carries the risk of escalation where a state erroneously believes that it is incurring a cyber attack rather than mere espionage. This is especially the case where the targets of cyber espionage are sensitive military assets or networks, such as nuclear weapons.

One interesting proposal in response to such issues has been made by Ido Kilovaty. Kilovaty has proposed that a special category of espionage, "espionage with hostile intent" be made illegal under international law.[98] Such illegal espionage would be against sensitive targets such as nuclear stockpiles, early warning systems, and missile defense systems.[99] However, even if such illegality deters some states from committing cyber espionage against nuclear weapons, the potential consequences if a state violates this proposal are unclear. If such a principle were incorporated into the *jus ad bellum,* for example, it is unlikely that mere cyber

[98] Ido Kilovaty, *World Wide Web of Exploitations – The Case of Peacetime Cyber Espionage Operations Under International Law: Towards a Contextual Approach*, 18 COLUM. SCI. & TECH. L. REV. 42, 69 (2016).
[99] *Id.*

espionage against a state, without more destruction, would be considered an armed attack to justify self-defense.[100] Further, it is unlikely that the majority of cyber capable states, all of whom benefit from cyber espionage operations, would be willing to prohibit such a valuable method of information-gathering.

As Part III has shown, many scholars have vigorously attempted to harmonize cyber attacks and cyber espionage with the existing *jus ad bellum.* However, the innate characteristics of cyber attacks and cyber espionage can make current laws difficult to apply in many situations. Thus, some scholars have instead advocated the creation of new law through treaties on cyber attacks and espionage. These treaties will be the subject of the next Part.

IV. Cyber Treaties.

Due to the legal issues outlined above, some scholars and several states (notably Russia) have proposed that new treaties on cyber warfare are needed to make up for current gaps in international law.[101] These treaty supporters argue that an international agreement would be useful to establish clearer boundaries in cyberspace. Due to the current lack of consensus outlined above, each country is essentially left to determine on its own what it considers to be an armed attack in cyberspace. Supporters of a treaty argue that this is dangerous because it fosters instability. If each country is essentially free to determine what is an armed attack based on its own national security interest, such lack of a standard allows countries to constantly push the envelope in their cyber attacks. This in turn makes it more likely to lead to an armed conflict if a

[100] Though a state could potentially respond to such illegal cyber espionage with countermeasures. *See supra* note 70.
[101] Russia most recently in 2011 proposed an international convention to regulate "information security." *See Convention on International Information Security,* MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION (Sept. 22, 2011), http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

country chooses to interpret a cyber attack, or possibly even cyber espionage, as an armed attack.[102]

Supporters of a treaty thus argue that an agreement would clear up this confusion by more clearly defining when a cyber attack meets the armed attack threshold. For example, a treaty could create a list of targets considered off limits to cyber operations, such as critical infrastructure as well as nuclear weapons, power plants, and their supporting systems.[103] It could then establish that any cyber attack conducted against these targets is considered an armed attack.[104] Finally, a treaty could prevent increased militarization of cyberspace by regulating and restricting each nation's activities in cyberspace. It could also foster cooperation among countries and allow them to focus on other issues such as cyber crime and cyber terrorism.[105]

Those who argue that a treaty is not feasible tend to make several arguments. First, opponents argue that a treaty regulating or prohibiting cyber weapons would be logistically difficult. For one, it would be very difficult to regulate cyber weapons that can be cheaply produced, easily distributed, and constantly evolved.[106] Nuclear weapons, for example, are more easily regulated by treaties because they are difficult to produce and only available to a handful of nations. In contrast, malware is much easier to create and send around the globe, and can be used both by nations as well as individuals and non-state actors.

---

[102] BENJAMIN MUELLER, ON THE NEED FOR A TREATY CONCERNING CYBER CONFLICT 10 (2014), http://www.lse.ac.uk/IDEAS/publications/reports/pdf/SU14_2_Cyberwarfare.pdf. For example, in 2008 the Agent.btz malware infected the U.S. State and Defense departments' classified communications channels. As the malware crippled military command and control systems, a debate ensued over whether the infection should be considered an attack justifying a military response or mere espionage. The U.S. ultimately decided to consider the act as cyber espionage. *Id.* at 5.

[103] George Finney, *Should There be a CyberWar Treaty?,* SECUREWORLD (2016), https://www.secureworldexpo.com/blog/should-there-be-a-cyberwar-treaty.

[104] The *Tallinn Manual*'s Rule 140 requires that states take "special care" when conducting cyber attacks on select targets such as nuclear power stations. The Rule, however, does not explicitly define such attacks as rising to the level of armed attack. TALLINN, *supra* note 60, at 529-31.

[105] MUELLER, *supra* note 102, at 12.

[106] Louise Arimatsu, *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations*, *in* 2012 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 91, 100 (C. Czossek et al. eds., 2012).

In addition, a treaty would be difficult to enforce due to the attribution problem discussed in the previous Part. Nuclear weapons treaties, in contrast, are more easily enforced because states can monitor each other's nuclear weapons programs and arsenals, which are not easily hidden. In contrast, cyber weapons can be hidden or disguised, and states are unlikely to disclose their cyber capabilities as doing so would enable the development of defensive programs that render such capabilities useless.[107] Further, the use of a nuclear weapon, whether for testing or offensive purposes, leaves a huge impact that can generally be traced back to a state. Cyber weapons, in contrast, can go undetected when used and if discovered are difficult to trace back to a state. Thus, without any reliable method of enforcement, a treaty would be useless.

Opponents also argue that a treaty developing standards would be difficult to create in that asymmetries exist between different nations' interests and values in cyberspace. Countries that are very vulnerable to cyber attacks due to their dependence on networks would want a treaty restricting cyber operations. In contrast, countries with advanced cyber capabilities but less vulnerability would be less likely to give up their cyber advantage through a treaty.[108] Further, countries that value Internet freedom would be less likely to agree to a treaty that addresses the attribution problem through increased government oversight of the Internet. For example, a 2009 Russian treaty proposal called for restraining cyber offensive capabilities in part by increased government oversight of the Internet.[109] The U.S., citing censorship concerns, rejected the proposal and called for greater international law enforcement cooperation in lieu of a

[107] Grant Hodgson, *Cyber Attack Treaty Verification*, 12 ISJLP 231, 256-57 (2016).
[108] Lawrence L. Muir, Jr., *The Case Against an International Cyber Warfare Convention*, THE WAKE FOREST L. REV. (Dec. 9, 2011), http://wakeforestlawreview.com/2011/12/the-case-against-an-international-cyber-warfare-convention/.
[109] John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on a Treaty for Cyberspace*, N.Y. TIMES (June 27, 2009), http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=1.

treaty.[110] Therefore, as countries differ in both their values and dependence on cyberspace, opponents argue that a treaty is unlikely to come to fruition.

While a cyber treaty banning or regulating cyber weapons themselves would most likely be ineffective, a treaty that could establish standards would be valuable for reducing the threats outlined in Part II and clearing up the ambiguities discussed in Part III. As one possibility, a treaty could reduce the threat of nuclear escalation by adopting a strict approach prohibiting any form of cyber operation (attack or espionage) against nuclear arsenals and delivery systems, nuclear C3, early warning systems, and nuclear power plants. This would prevent the use of cyber operations, no matter how small or non-damaging, from being misinterpreted as part of a larger attack. Second, the treaty could require each state to publish and submit its view as to when it would consider a cyber attack to be an armed attack justifying self-defense. This would allow each state to tailor its standard based on its own interests. It would also provide stability by creating a centralized location where each state can know for certain what other states would consider to be a cyber armed attack.

Such a treaty, however, would not be without flaws. First, as discussed above, it is highly unlikely that states would give up the freedom to commit cyber espionage against nuclear weapons and related systems. Yet without a total prohibition on all cyber operations, some standardized definition of cyber attacks would need to be adopted to distinguish it from

[110] *Id.* More recently, President Putin has claimed that Russia in 2015 reached out to the U.S. to discuss a cyber treaty, but that the Obama Administration never gave a response. Max de Haldevang, *Putin Claims Russia Proposed a Cyber War Treaty in 2015 but the Obama Administration Ignored Them,* QUARTZ (June 16, 2017), https://qz.com/1007996/oliver-stone-putin-interview-vladimir-putin-says-russia-proposed-a-cyber-war-treaty-in-2015-but-obamas-administration-ignored-them/.

permissible espionage. It is unlikely, though, that states would be able to come to agreement on a uniform definition given the disparity of interests.[111]

If each state is also given the freedom to determine its own standard, it is inconceivable why any state would not adopt the strict liability approach where all cyber attacks are considered an armed attack.[112] While this could help develop a system of cyber deterrence, in that states would not risk committing cyber attacks that justify a response in self-defense, the treaty would continue to be undercut by the attribution issue. Even if a state adopts a strict liability approach, it would still have to prove that a state committed the attack or was responsible for the attack. The treaty would therefore also have to determine a standard for proving attribution, which would again be difficult due to differing interests.[113] Lastly, a cyber treaty would most likely due nothing to deter the actions of cyber terrorists and other independent non-state actors, whose goal of causing nuclear detonations is arguably deadlier than state cyber attacks.

V. Conclusion.

Nuclear weapons and their supporting systems clearly face a variety of cyber threats, including information theft, warhead or nuclear material theft, spoofed attacks, communications disruption or manipulation, and hijacked launches or detonation. Yet despite such threats, little comfort can be taken in the use of international law as a deterrent. International law, and particularly the *jus ad bellum,* has struggled to harmonize with rapidly emerging cyber weapons.

The current state of the laws on self-defense, attribution, and espionage, for example, all retain ambiguities when applied to cyberspace. A treaty could be helpful in establishing clear standards regarding cyberspace, and could also possibly prohibit attacks against nuclear systems.

---

[111] States that are frequent victims of cyber espionage, for example, would probably want a broader definition of cyber attacks that incorporated some aspects of espionage.
[112] *See supra* Part III.A.2.
[113] States who lack advanced attribution capabilities, for example, would probably want less stringent attribution standards than states who are more able to carry out clandestine cyber attacks.

However, it will be difficult to establish a treaty that all countries involved, whether they own nuclear weapons or have cyber capabilities, will approve. Even if this is achieved, enforcement difficulties will remain so long as states lack the ability to accurately attribute the use of cyber weapons back to a state or non-state actor.

Attribution, then, may well be the key in resolving the issues presented above. As attribution technology improves, treaties on cyber warfare may be more easily enforced. More accurate attribution technology may also result in reduced advantages for cyber attacks, as states and non-state actors will be unwilling to carry out attacks that can be accurately traced back to them. Thus, as attribution technology improves, cyber weapons may find themselves becoming more similar to traditional weaponry, and thus more tightly controlled by the dictates of international law.

The question remains, though, of what to do now regarding these cyber threats. If the law is too ambiguous to regulate cyber attacks, and a treaty is not feasible, the solution to reducing cyber threats to nuclear weapons may be the adoption of non-legal policies. A possible policy for threat reduction could be to reduce the dependency of nuclear weapons on cyberspace. Attribution technology and cyber defenses are getting stronger as time goes on, and as stated this can reduce the threat of cyber attack and make such attacks more easily governed by law or treaty. But it is also important to note that cyber weapons are not sitting by idly; they are constantly being improved and evolved to beat attribution mechanisms and discover new vulnerabilities in the defenses.

The only complete way to prevent cyber attacks, then, is to deny cyber weapons the environment in which they operate. Nuclear weapons and C3 systems that are not connected to a network, or operate on low-tech systems, face a much lower threat of being affected by a cyber

attack.[114] A total disconnection of nuclear systems, though, is unlikely given that there are still some benefits to connectivity, as well as a negative image associated with relying on outdated technology.[115] Stuxnet has also demonstrated that even disconnected networks can be penetrated through the manual insertion of malware via USB drives. It is thus also essential that nuclear weapons continue to be monitored by human personnel, and that such personnel are properly trained to act as a fail-safe in the event that a system is attacked and breaks down.[116] Paradoxically, then, low technology and human intuition may currently be the best way to reduce cyber threats in an increasingly connected and computerized world.

[114] In the United States, missile silos around the country continue to use outdated IBM computers that rely on floppy disks to relay commands and share intelligence. Several military commanders have recognized the advantages of such low technology in reducing cyber threats. When asked about this on "60 Minutes," Major General Jack Weinstein said that "those older systems provide us some – I will say huge safety when it comes to some cyber issues that we currently have in the world." Brian Fung, *The Real Reason America Controls its Nukes With Ancient Floppy Disks,* WASHINGTON POST (May 26, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/05/26/the-real-reason-america-controls-its-nukes-with-ancient-floppy-disks/?utm_term=.2c6fc94193ed. Many nuclear power plants also run on analog technology and are not connected to the Internet. James Conca, *Is Hacking Nuclear Power Plants Something We Should Be Afraid Of?,* FORBES (July 7, 2017), https://www.forbes.com/sites/jamesconca/2017/07/07/is-hacking-nuclear-power-plants-something-we-should-be-afraid-of/#3496bbbadde8.

[115] Despite the recognition that low technology may reduce the risk of cyber attack, the U.S. military has nonetheless begun to modernize the technology controlling nuclear weapons. Under the current plan, the Department of Defense intends to devote $60 million towards a full-system replacement by 2020. As an initial step, the Department is currently in the process of replacing the floppy disks with secure digital cards. *See* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS 60-61 (2016).

[116] It has been reported that the Department of Defense may be working with IBM to develop neurosynaptic computer chips that will be used to control and coordinate the nuclear arsenal. *See* Adam Toobin, *IBM Brain-Inspired Computer Will Look After Our Nuclear Weapons,* INVERSE (Mar. 30, 2016), https://www.inverse.com/article/13514-ibm-brain-inspired-computer-will-look-after-our-nuclear-weapons. While the prospect of control through a centralized computer system may seem efficient and prevent human error, the consequences would be catastrophic if cyber weapons were developed that could gain control over this "supercomputer."