2012

The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict

Landon J. Wedermyer

The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict

by

Landon J. Wedermyer

Submitted in partial fulfillment of the requirements of the
King Scholar Program
Michigan State University College of Law
under the direction of
Professor Adam Candeub
Spring, 2012

Introduction

Once in a generation, the rules of warfare change. In the early 20th Century, the revolution in flight opened up the vast expanse of the skies to military exploitation.[1] In the middle of the century, the dawn of the atomic age brought about the means for warfare to reach previously unimaginable levels of destruction.[2] The electronic age has spawned its own paradigm-shifting development in human conflict: Warfare in and through cyberspace. The extraordinarily rapid development of cyber networks and electronic capabilities during the beginning of the 21st Century has given states the ability to strike their adversaries out of, quite literally, thin air.

In the past, international treaties, conventions, and legal principles, particularly the United Nations and its Charter, constructed a framework of rules to govern and restrict the conduct of warfare between states.[3] While international organizations such as the U.N. lack for themselves the coercive ability to police these rules and punish offending states, the existence of international fora allows for a unified application of political, economic, and military pressure on states that flout the laws of war.[4]

---

[1] For an introductory discussion of how air power changed the early-20th Century paradigm of war, *see* SMITHSONIAN INSTITUTE PRESS, THE GREAT WAR IN THE AIR: MILITARY AVIATION FROM 1909 TO 1921 (1993).

[2] CHUCK HANSEN, THE SWORDS OF ARMAGEDDON: U.S. NUCLEAR WEAPONS DEVELOPMENT SINCE 1945 (1995).

[3] U.N. CHARTER art. 1, para. 1

The Purposes of the United Nations are:

1. To maintain international peace and security, to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.

[4] For a discussion of U.N. peacekeeping and "peacebuilding", *see,* MICHAEL W. DOYLE & NICHOLAR SAMBANIS, MAKING WAR AND BUILDING PEACE: UNITED NATIONS PEACE OPERATIONS (2006).

The advent of the age of cyber warfare threatens to obliterate the credibility and political-moral force behind the U.N. Charter and the ability of the law of war to effectively govern interstate conflict. The Charter's provisions were drafted for an era of warfare in which massive bodies of soldiers, aircraft, and naval forces crossed clearly demarcated borders and left little doubt as to when an act of war had occurred.[5] In 1945, when the United Nations came into existence, there was little need for the international community to agonize over the definitions of terms such as "use of force[6]" and "armed attack[7]"; the charred remains of Europe and East Asia were all the definition that was needed. Unfortunately, cracks and gray areas in the vague definitions and prohibitions in the Charter began to appear during the proxy wars of the Cold War. In the present day, the dizzying expansion of cyber capabilities has opened up a myriad of new, asymmetric strategic options for states to project military power in ways never contemplated by the drafters of the U.N. Charter.

With the deployment of the Stuxnet virus against the Iranian nuclear program, cyber weapons have taken their place alongside traditional, kinetic weapon systems in a state's warfighting arsenal. While the Charter gives states the right to respond in self-defense when they are the victims of an armed attack,[8] it provides no guidance for states attempting to form an appropriate response or a forward-thinking strategic policy for cyber warfare.

Using the Stuxnet attack as a basis, this paper demonstrates how two interpretations of the U.N. Charter, the traditional "effects-based" approach and a proposed "definitional"

---

[5] The U.N. Charter refers directly to World Wars I and II in its Preamble:

> "We the peoples of the United Nations determined: to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind…"

[6] U.N. CHARTER art. 2 para. 4

[7] U.N. CHARTER art. 51

[8] *Id.*

approach, both fail to account for the asymmetrical nature of cyber warfare. The effects-based test has long been the standard for states to determine if an armed attack or use of force has occurred.[9] However, it leaves too much room for states to wage simmering, shadow wars in cyberspace, which could easily erupt into a more traditional shooting war, enhanced by an escalation in cyber attacks. The varied means by which a cyber attack may take place, such as the length of time between the infiltration of a state's computer networks and any subsequent "trigger", issues of neutrality when electronic signals pass through neutral states, and problems inherent in attributing cyber attacks to specific state actors, have encouraged states to create their own cyber strategies unilaterally, with no international oversight.

On the other hand, the proposed definitional approach takes a much harder line in holding states accountable for cyber attacks originating in their territory. Unfortunately, such an approach swings the interpretive pendulum too far to the side of draconian strict liability in cyberspace. An international adherence to the definitional approach risks unneeded and undue escalation of a cyber conflict as neutral or truly innocent nations may be held accountable for an anonymous signal routed through their servers or originating within their borders. Only an international solution, forged by the U.N. or the international community at large, can update the obsolete Articles 2(4) and 51 of the U.N. Charter, thus providing guidance for the conduct of warfare in the Cyber Age.

I. The Story of Stuxnet

A. Cyber Attack in Iran

[9] Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999)

In Januray 2010, the centrifuges at Iran's Natanz nuclear facility went haywire. Investigators from the International Atomic Energy Agency observed that researchers were replacing centrifuges at "an incredible rate.[10]" In nuclear enrichment processes, centrifuges are used to separate Uranium-235[11] from the far more common Uranium-238 isotope.[12] Because the process involves spinning the centrifuge at rapid velocities in order to separate the uranium isotopes, wear and tear is expected and centrifuges are commonly replaced.[13] This time, however, the IAEA inspectors noticed that the Iranian technicians were replacing their centrifuges at more than double the normal rate.[14] In May 2010, the IAEA stated the Natanz facility contained 3,900 operational centrifuges, a 20% reduction from the number of working centrifuges the facility housed one year prior.[15] In addition, thousands of installed centrifuges were simply idle.[16]

The frantic replacement of centrifuges and subsequent impairment of operations at the Natanz facility led many outside observers to believe "there has been a concerted intelligence operation which is able to debilitate and set back the Iranian program.[17]" The Iranian government acknowledged later in 2010 that its nuclear program had indeed been the victim of

---

[10] For the most comprehensive and exhilarating telling of the Stuxnet saga, *see* Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED, July 11, 2011, available at http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 (last accessed March 27, 2012).

[11] Uranium 235 comprises only 0.78% of naturally-occurring uranium. As the only fissile uranium isotope, only Uranium 235 can sustain the fission reaction necessary for nuclear weapons of power processes. *See, e.g.,* G.W.C. KAYE, T.H. LABY ET AL., TABLES OF PHYSICAL AND CHEMICAL CONSTANTS, Ch. 4, Sec. 7

[12] *Id.*

[13] Ivan Oelrich and Ivanka Barzashka, *How a Centrifuge Works,* FEDERATION OF AMERICAN SCIENTISTS, Available at http://www.fas.org/programs/ssp/nukes/fuelcycle/centrifuges/centrifuge.html (last accessed March 27, 2012)

[14] *See* Zetter, *supra* Note 9 at 1

[15] James Blitz, Daniel Dombey & Roula Khalaf, *Signs of Sabotage in Tehran's Nuclear Programme*, FINANCIAL TIMES, July 24, 2010, available at http://gulfnews.com/news/region/iran/signs-of-sabotage-in-tehran-s-nuclear-programme-1.658481 (last accessed March 27, 2012)

[16] *Id.*

[17] *Id.* "A large number of Iranian centrifuges have crashed and up to half have had to be replaced in recent times. This success didn't happen entirely accidentally."

an electronic attack.[18] Iran has understandably downplayed the impact the attack left on the country's nuclear program, making any damage assessment difficult. Some Iranian officials initially claimed that the attack did not reach any nuclear components or critical systems,[19] but President Mahmoud Ahmadinejad admitted, in November 2010, that the attack had "creat[ed] problems for a limited number of our centrifuges.[20]" President Ahmadinejad went on to claim that any problems had been corrected and the Natanz facility was fully operational.[21] International observers are skeptical of this claim, noting multiple instances of disruption in the Natanz facility throughout 2010 and into 2011.[22]

B. Stuxnet – The World's First Cyber Weapon

The perpetrator of the mayhem unleashed on the Iranian nuclear program was an exquisitely crafted computer virus that has come to be known as Stuxnet. Stuxnet was identified in June 2010 by VirusBlokAda, a small online security firm in Belarus. VirusBlokAda received a complaint from a client in Iran whose computer was trapped in a reboot loop.[23] A reboot loop is a clear sign of a computer virus, and the Belorussian technicians were not surprised to find that just such a malware program had infected their client's computer.[24]

---

[18] Atul Aneja, *Under Cyber-Attack, Says Iran*, THE HINDU, September 26, 2010, available at http://www.thehindu.com/news/international/article797363.ece (last accessed March 27, 2012)
[19] *Stuxnet Worm Hits Iran Nuclear Plant Staff* Computers, BBC NEWS, September 26, 2010, available at http://www.bbc.co.uk/news/world-middle-east-11414483 (last accessed March 27, 2012)
[20] Mark Clayton: *Stuxnet: Ahmadinejad Admits Cyberweapon Hit Iran Nuclear* Problem, CHRISTIAN SCIENCE MONITOR, November 30, 2010, available at http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program (last accessed March 27, 2012)
[21] *Id.*
[22] *Id.*
[23] *See* Zetter, *Supra* Note 10
[24] *Id.*

When they cracked into the virus, however, the team at VirusBlokAda immediately realized Stuxnet was far more than just a simple prankster or hacker's virus.[25] First, the size of the file was huge. Whereas almost all malware programs or files come in at about 50 kilobytes, Stuxnet was huge: almost half a megabyte in size.[26] Additionally, the virus' files were more complex, camouflaged, and multi-layered than any malware program on record.[27] VirusBlokAda shared their initial findings with the private, interconnected cybersecurity community, sparking a months-long investigation of Stuxnet by the top private firms and researchers in the world.[28]

The combined efforts of the global cybersecurity community revealed the following about the Stuxnet virus: Stuxnet originally spread to the infected networks by way of infected USB devices, enabling it to reach computer networks not connected to the wider Internet.[29] Once planted onto a victim computer, Stuxnet was designed to seek out and attack a single component of software designed by Siemens AG[30] for use in controlling manufacturing processes.[31] Once in place on a single computer, Stuxnet "searched" for the specific Siemens software. If the Siemens software was not present, the virus would simply go inert, burying itself undetected in the computer system.[32] If Stuxnet detected the Siemens software, it used peer-to-peer methods to spread to other computers on the same private network as the original

[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] Siemens is a large German technology conglomerate based in Munich.
[31] Information on Siemens industrial control software can be found at http://www.automation.siemens.com/mcms/topics/en/simatic/Pages/Default.aspx
[32] *See* Zetter, *Supra* Note 10

infected system.[33] Nearly 60% of all Stuxnet-infected computers worldwide were located in Iran, a staggering concentration for a computer virus.[34]

Stuxnet's actions once it infiltrated the Siemens-equipped computers reveal its intended target. When cybersecurity experts cracked into the inner workings of Stuxnet's code, they discovered that the virus had one specific kind of action to perform:

> Once [Stuxnet] infects a system, it searches for the presence of two kinds of frequency converters made by the Iranian firm Fararo Paya and the Finnish company Vacon, making it clear that the code has a precise target in its sights. Once it finds itself on the targeted system, depending on how many frequency converters from each company are present on that system, Stuxnet undertakes two courses of action to alter the speed of rotors being controlled by the converters. In one of these courses of action, Stuxnet begins with a nominal frequency of 1,064 Hz — which matches the known nominal frequency at Natanz but is above the 1,007 Hz at which Natanz is said to operate — then reduces the frequency for a short while before returning it back to 1,064 Hz.
>
> In another attack sequence, Stuxnet instructs the speed to increase to 1,410 Hz, which is "very close to the maximum speed the spinning aluminum IR-1 rotor can withstand mechanically," according to the ISIS report, which was written by ISIS president David Albright and colleagues. The stresses from the excessive, then slower, speeds cause the aluminum centrifugal tubes to expand, often forcing parts of the centrifuges into sufficient contact with each other to destroy the machine.[35]

In short, Stuxnet was designed to induce malfunctions in the centrifuges within Iran's nuclear enrichment facilities. It searched out systems running one specialized kind of industrial-control software, cracked into specific components of that software – the frequency controls for centrifuges – and subtly manipulated them into a sustained breakdown.[36] The sheer size and complexity of the virus, its exclusive distribution inside Iran, and its specific target profile,[37] led the cybersecurity community to nearly unanimously conclude that Stuxnet was designed solely

[33] *Id.*
[34] *Id.*
[35] DAVID ALBRIGHT, PAUL BRANNAN, & CHRISTINA WALROND, INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY, DID STUXNET TAKE OUT 1,000 CENTRIFUGES AT THE NATANZ ENRICHMENT PLANT? at 11, December 22, 2012.
[36] *Id.* at 13
[37] *See* Zetter, *Supra* Note 10

to attack the Iranian nuclear program.[38] One observer, in a telling analogy, compared the Stuxnet cyber attack to "a commando raid in the heart of Iran."[39]

Symantec, one of the world's best-known online security companies, estimates that the creation of a malware code like Stuxnet would have taken dozens of designers months, if not over a year.[40] Some have gone on to conclude that Stuxnet's development was "the largest and costliest development effort in malware history."[41] The code was so complex, so wrapped in layers upon layers of encryption, misdirection, and stealth protocol, that most believe only a state actor could have possessed the technical know-how, funding , and (most importantly), motive to create such a virus.[42]

The universal perception of Stuxnet is fascinating to observe. Virtually every observer to comment on Stuxnet, from government bodies on down to individual technology bloggers, has either used military analogies (such as the commando raid description above) or outright declared the Stuxnet event to be the equivalent of a military attack. As one commenter put it, Stuxnet "it saved the Iranians a good old-fashioned bombing.[43]" Inartfulness aside, this commenter points out an emerging reality of warfare: Cyber attacks have now taken their place among airstrikes or ground assaults in the strategic arsenal of the world's nation-states. In a December 2010 report, the Congressional Research Service classified Stuxnet as a "harbinger of

---

[38] Gregg Keizer, *New Stuxnet Clues Suggest Sabotage of Iran's Nuclear Enrichment Program*, ComputerWorld, November 15, 2010, available at http://www.computerworld.com/s/article/9196458/New_Stuxnet_clues_suggest_sabotage_of_Iran_s_uranium_enrichment_program (last accessed March 27, 2012)

[39] Gregg Keizer, *Is Stuxnet the 'Best' Malware Ever?* COMPUTERWORLD, September 16, 2010, available at http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_? (last accessed March 27, 2012)

[40] *See* Zetter, *Supra* Note 10

[41] *Id.*

[42] *Id.*

[43] Marcus J. Ranum, *Cyberwar*: *About Stuxnet, the next generation of warfare?*, FABIUS MAXIMUS, 29 September 2011, http://fabiusmaximus.wordpress.com/2011/09/29/29291/ (last accessed March 27, 2012)

an emerging warfare capability.[44]" The explosive growth of cyberwarfare capabilities and doctrines across the world which culminated in the release of Stuxnet will be examined in the next section.

II. A New Era of Warfare

A. Cyber War in the United States

The United States has been slowly integrating cybersecurity and cyber warfare capabilities into its national security apparatus since the 1990's.[45] The pace of cyber integration surged in the mid-2000's, as the capabilities of the Internet exploded and fears of outside penetration of sensitive networks and computer systems came to pass.[46] In 2008, the Department of Defense brought cyberspace under the umbrella of military conflict, assigning the realm of cyberspace to the United States Air Force. The Air Force changed its official mission to include the domination of cyberspace, alongside the traditional domains of "air" and "space.[47]"

[44] CONGRESSIONAL RESEARCH SERVICE, THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY, December 9, 2010.

[45] Bruce D. Berkowitz, *War Logs On: Girding America for Computer Combat,* FOREIGN AFFAIRS, May/June 2000 ("In Kosovo, America stumbled into the age of computer warfare. Now Washington must think hard about how to attack its foes' electronic networks and defend its own.")

[46] In 2007, a "spearphishing" attack struck the Department of Defense. The attacker(s) sent spoofed e-mails containing recognizable names were OSD employees. When they opened the messages, user IDs and passwords that unlocked the entire network were stolen; as a result, sensitive data housed on Defense systems was accessed, copied and sent back to the intruder. *See*, SANS INSTITUTE, PHISHING: ANALYSIS OF A GROWING PROBLEM, December 2007, available at http://www.sans.org/reading_room/whitepapers/threats/phishing-analysis-growing-problem_1417 (last accessed March 27, 2012)

[47] "About the Air Force: Our Mission", www.airforce.com/learn-about/our-mission/ (last accessed March 27, 2012)

In 2006, the Air Force announced its intentions to develop Air Force Cyber Command (AFCYBER), which would be commanded by a 3-Star General and operate as a Major Command (MAJCOM), the broadest sub-division of the Air Force.[48] Those plans were scrapped in 2008, as the DOD decided on an even broader role for cyber military forces. Instead of placing the responsibility for cyber warfare completely under the Air Force's purview, the DOD created United States Cyber Command (USCYBERCOM).[49] The proposed Air Force Cyber Command was rolled into USCYBERCOM as the 24th Air Force.[50] Because USCYBERCOM operates as an entity of the DOD, rather than a specific military branch, it is able to synergize operations among the cyber arms of the Air Force, Army, and Navy.[51]

The mission of USCYBERCOM is as follows:

> USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries.[52]

The United States government has instituted a sweeping program to defend civilian computer networks as well as to project military power through cyberspace. Under the USA PATRIOT Act and subsequent legislation, the job of protecting nonmilitary government and

---

[48] As a MAJCOM, Air Force Cyber command would have operated alongside units such as Air Combat Command, Strategic Command, and Air Force Material Command. Each MAJCOM is in charge of a distinct, crucial portion of the Air Force's mission. The fact that a Cyber Command would have risen to the MAJCOM level is a key indicator of the importance of cyber warfare to the future military.

[49] Jeremy Hsu, *U.S. Cyber Command Now Online, and Seeking a Few Good Geeks*, POPULAR SCIENCE, October 5, 2009

[50] GEN. C. ROBERT KEHLER, 24TH AIR FORCE ACTIVATION, August 19, 2009, http://www.24af.af.mil/news/story.asp?id=123163965

[51] USCYBERCOM includes U.S. Army Cyber Command (Second Army), U.S. Navy Fleet Cyber Command, and the U.S. Marine Corps Cyberspace Command.

[52] "U.S. Cyber Command Factsheet", http://www.stratcom.mil/factsheets/Cyber_Command/

civilian networks has fallen to the Department of Homeland Security (DHS).[53] DHS is in the process of introducing a standardized information security system that will cover every unclassified, civilian computer network in the federal government.[54] Known as EINSTEIN, this security protocol is designed to make mirror copies of all data packets transferred through government networks and screen those packets for malicious code or other threats.[55]

How DHS and USCYBERCOM would work together in together in the event of a massive cyber attack is unclear at the present time. If Stuxnet were to strike computer networks in the United States, how would the overlapping agencies respond and what would be their respective operating fields? A few statements from key members of the new cyber warfare apparatus are illuminating. In July 2011, Deputy Defense Secretary William Lynn stated,

> [USCYBERCOM fields] a full spectrum of capabilities, but the thrust of the strategy is defensive. The strategy rests on five pillars…(T)reat cyber as a domain; employ more active defenses; support the Department of Homeland Security in protecting critical infrastructure networks; practice collective defense with allies and international partners; and reduce the advantages attackers have on the Internet.[56]

Secretary Lynn's remarks mirror the DOD Cyberwarfare Strategy, released in July of 2011.[57]

General Keith Alexander, commander of USCYBERCOM, stated "If [a cyber strike is] determined to be an organized attack, I would primarily want to go and take down the source of those attacks.[58]"

---

[53] Stephen G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*: *Keynote Address, 2011 Harvard National Security Journal Symposium*, 2 HARV. NAT'L SEC. J. 366, 369 (2011).
[54] *Id.*
[55] *Id.*
[56] Karen Parrish, *Lynn: Cyber Security's Thrust is Defensive*, AMERICAN FORCES PRESS SERVICE, JULY 14, 2011, available at http://www.defense.gov/news/newsarticle.aspx?id=64682 (last accessed March 28, 2012)
[57] UNITED STATES DEPARTMENT OF DEFENSE, DOD STRATEGY FOR OPERATING IN CYBERSPACE, July 2011 http://www.defense.gov/news/d20110714cyber.pdf

Based on these strategic positions and doctrines, it appears the civilian cyber security apparatus would be responsible for "combatting" any cyber attack that pierced any non-military infrastructure (with DOD support and resources if necessary).[59] What is certainly clear is that the United States government is racing to fit cyber warfare capability into its strategic and legal arsenal. The next sections will detail how other nations are also driving headlong into the unknown, based on their own legal principles and historical circumstances.

B. Cyber Militarization in Russia

Since the early 2000's, Russian military leaders have enthusiastically embraced the adoption of cyber weapons.[60] Used in a conventional military capacity, Russia envisions its cyber weapons as a "force multiplier.[61]" In military strategy, a force multiplier is a component of a military force that increases the effectiveness or fighting efficiency of a unit or group.[62] Like all offensive cyber strategies, Russia's includes the capability to disrupt the information infrastructure of their enemies and includes strategies that would attack financial markets and military and civilian communications capabilities as well as other parts of an enemy's critical infrastructure prior to the initiation of traditional military operations.[63] Additionally, rumors have swirled for years that the Russian government maintains close ties with various

---

[58] Ryan Singel, *Cyberwar Commander Survives Senate Hearing*, WIRED, April 15, 2010, available at http://www.wired.com/threatlevel/2010/04/cyberwar-commander/
[59] Bradbury, *Supra* Note 53 at 371.
[60] KEIR GIELS, "INFORMATION TROOPS" – A RUSSIAN CYBER COMMAND? At 5, *3rd International Conference on Cyber Conflict* (C. Czosseck, E. Tyugu, T. Wingfield, Eds.) 2011.
[61] Maj. Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law,* 64 A.F. L. Rev. 121, 133 (2009).
[62] *Id.*
[63] *Id.*

"underworld" organizations within Russia, providing them with tools and tacit support to launch cyber vandalism, espionage, and other activities.[64]

The world may have already received several previews of what a Russian cyber war action would entail. In 2007, the Estonian government announced plans to relocate the Bronze Soldier of Talinn, a Soviet-era statute commemorating Russian soldiers who died liberating Estonia from Germany during World War II, from the city's central square.[65] The removal sparked a brief but intense diplomatic dispute with Russia.[66] On April 27, 2007, a wave of cyberattacks swamped Estonian government, banking, and political party sites.[67] The attacks were almost entirely Distributed Denial of Service (DDoS)[68] strikes. While the DDoS attacks themselves were not very sophisticated,[69] the breadth and coordination of the cyber attack led many observers to conclude that the attacks could not have been carried out without the blessing of the Russian authorities and that the hackers apparently acted under "recommendations" from parties in the Russian Government.[70] While the DDoS attacks were traced back to sources in Russia and Eastern Europe, they could not be connected to the Russian government.[71]

In 2008, Russia and Georgia went to war over the breakaway Georgian provinces of South Ossetia and Abkhazia.[72] As Russian troops crossed the border into Georgia, "a multi-faceted cyber attack" began against the Georgian communication infrastructure and key government web

---

[64] ENEKEN TIKK, ANNA-MARIA TALIHARM ET AL., CYBER ATTACKS AGAINST GEORGIA: LEGAL LESSONS LEARNED, Cooperative Cyber Defense Center (2008) at 5.
[65] BBC News, *Estonia to Remove Soviet Memorial*, January 12, 2007, available at http://news.bbc.co.uk/2/hi/europe/6255051.stm (last accessed March 28, 2012)
[66] *Id.*
[67] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe,* WIRED, August 21, 2007.
[68] In a DDoS strike, the cyber attacker uses a network of linked computers (known as "bots") to flood the targeted server with information requests, causing the server to shut down under the strain.
[69] *Supra* Note 62.
[70] RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010) at 72.
[71] *Id.* at 75.
[72] Schap, *Supra* Note 61 at 134.

sites.[73] Georgian government websites were defaced or brought offline by DDoS attacks, along with Georgian internet and phone service providers.[74] Once again, the Russian government denied launching the cyber attacks.[75] Much like the Estonian cyber attacks, however, outside experts, analyzing the coordination and complexity of the attacks (the first strikes occurred almost exactly as Russian troops made their first moves over the border), concluded that, while non-governmental "hacktivists" were the likely culprits, they did so with under-the-table support or encouragement from Moscow.[76]

The Russian example, particularly the use of cyber attacks during the 2008 war with Georgia, reveals how a small-scale cyber war could be conducted. The attacks fit the Russian government's "force multiplier" views of cyber warfare; the attacks were intended to diminish Georgian morale and undermine government operations, a classic support strategy. However, the decentralized nature of the Internet means that the cyber attacks could not be attributed to the Kremlin. As this paper will show, problems with attribution of cyber attacks are one of the key factors that hamper the application of existing international legal regimes to cyber warfare. Russia seems to have figured this out.

C. Chinese Cyber Warriors

When most American politicians speak of cyber security threats, the first country they mention is almost always China. China currently possesses a significant cyber weapons and intelligence infrastructure, and their cyber warfare doctrine is designed to achieve global

[73] *Id.*
[74] *Id.*
[75] *Id.* at 136.
[76] Tikk, et al., *Supra* Note 64 at 7.

"electronic dominance" by 2050. This includes the capability of disrupting the information infrastructure of their enemies.[77] In 1999, the PLA Daily, the official media outlet for the People's Liberation Army (PLA), stated, "Internet warfare is of equal significance to land, sea, and air power and requires its own military branch."[78] According to military and intelligence sources, Chinese cyber forces have developed detailed plans for cyber attacks against the United States and others.[79] A 2007 Department of Defense report indicated the PLA had established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks.[80] A Congressional Research Service Report noted that China was pursuing the concept of a Net Force, which would consist of a strong reserve force of computer experts trained at a number of universities and training centers.[81] In 2005, the PLA began to incorporate offensive computer network operations into its exercises, primarily in first strikes against enemy networks.[82]

Chinese sources were the likely culprits in some of the most complex and extensive intrusions into U.S. government computer networks on record.[83] Unlike the dramatic attacks on Estonia and Georgia (particularly the Georgian attack, which coincided with a military operation) carried out by Russian actors, cyber attacks originating from China have largely been in the realm of espionage.[84] In 2003, for example, a group of Chinese hackers code named

---

[77] Kevin Coleman, *China's Cyber Forces*, DEFENSETECH, May 8, 2008, available at http://defensetech.org/2008/05/08/chinas-cyber-forces (last accessed March 28, 2012).
[78] Kevin B. Alexander, *Warfighting in Cyberspace*, JOINT FORCES Q., July 31, 2007, at 58, available at http://www.miltary.com/forums/0,15240,143898,00.html
[79] *Id.*
[80] U.S. DEP'T OF DEF. ANN. REP. TO CONG.: MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 21(2007), available at http://defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf.
[81] STEVEN A. HILDRETH, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS NO. RL30735, CYBERWARFARE 11 (June 19, 2001)
[82] *Supra* Note 80 at 24.
[83] *Supra* Note 81 at 6.
[84] *Id.*

"Titan Rain" stole military research information and broke into the computer systems of government agencies.[85] The Chinese military sponsors regular computer hacking tournaments in order to discover and cultivate talented young computer warriors.[86]

The world's major powers have spent the last decade integrating cyber capabilities into their arsenals. From espionage, as in the case of China, to the smaller-scale attacks that supported Russia's invasion of Georgia, to the precision strike of Stuxnet, states now have the ability to fight their wars in cyberspace. From this point, the question focuses on how cyber warfare capabilities can be utilized in accordance with international treaties, agreements, and conventions. The following section will outline the United Nations prohibition on "use of force" between member states, the corresponding rights of states to defend themselves against "armed attack", and the intractable problems cyber weapons such as Stuxnet pose when a government is trying to figure out if it has been the victim of a use of force or armed attack.

III. The Law of Cyber War

A. Article 2(4) and Article 51

Article 2(4) of the U.N. Charter establishes the blanket prohibition on the use of force between U.N. Member States. "All members shall refrain…from the threat or use of force against the territorial integrity or political independence of any state…."[87] As a corollary, Article 51 of the Charter guarantees "the inherent right of individual or collective self-defense if

[85] Nathan Thornburgh, *The Invasion of the Chinese Cyberspies,* TIME, August 29, 2005, available at http://www.time.com/time/magazine/article/0,9171,1098961,00.html
[86] Cha Si, *The Threat of China's Patriotic Hacker* Army, EPOCH TIMES, August 23, 2011, available at http://www.theepochtimes.com/n2/opinion/the-threat-of-chinas-patriotic-hacker-army-60695.html
[87] U.N. CHARTER, art. 2, para. 4

an armed attack occurs against a Member.[88]" Because neither "use of force" nor "armed attack" are defined in the Charter, the two Articles often overlap. Interpretation by international powers, long experience, and academic consensus has established that Articles 2(4) and 51 apply to "military attacks or armed violence" only.[89] As the primary risk of cyber warfare lies in potentially uninhibited escalation in an international legal vacuum, the key question is, in terms of Article 51, can a cyber attack trigger a state's right to use military force to defend itself? In the age of Stuxnet, can a cyber attack rise to the level of an "armed attack?"

As mentioned previously, the U.N. Charter does not define what constitutes an "armed attack." Fortunately, a look at other U.N. documents helps form a definition of the term. As to what constitutes an armed attack, U.N. Resolution 3314 contains a definition of the term "aggression" for use in the military context. "Aggression" is defined as "use of force against the sovereignty, territorial integrity, or political independence of another state.[90]" Examples given in the Resolution include:

> Invasion, attack, or military occupation; bombardment or the use of any weapons against a State**;** blockade; an attack on the land, sea, or air forces or the marine and air fleets of a State; and the sending of armed bands, groups, irregulars or mercenaries to complete any of the previous acts.[91]

Resolution 3314 qualifies the right to self-defense against aggression by instituting a principle of proportionality governing the responses available to victims of military aggression. Additionally, the Resolution states that a state action meeting the criteria above that an act must be of "sufficient gravity" in order to be classified as aggression. Combining the elements of

[88] U.N. CHARTER, art. 51
[89] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 429 (2011).
[90] Definition of Aggression, G.A. RES. 3314 (XXIX), art. 1 (December 14, 1974).
[91] *Id.,* art. 3

"aggression" and "armed attack," scholars have largely agreed that the right of a state to self-defense is triggered only in the case of clear and defined invasion of national sovereignty through military action.[92]

B. When Does the Use of a Cyber Weapon Constitute an Armed Attack?

1. Effects-Based Tests

The traditional legal framework for analyzing when an aggressive action by a state rises to the level of an armed attack places the key analysis on the effects of the action on the victim state.[93] There are two common effects-based tests that have achieved common use among international legal scholars who have ventured into the issue of cyber war. These approaches attempt to fuse pre-existing canons of interpretation for the U.N. Charter with the difficulties presented by cyber warfare. Unfortunately, each traditional test falls short.

i. Equivalent Effects Test

The Equivalent Effects test is the simplest of the formulas used to postulate whether a cyber attack meets the "Armed Attack" threshold. The Equivalent Effects test "requires that [a cyber attack] must result in the same consequences as kinetic attack and physical invasion by

[92] *See* Waxman, *Supra* Note 89 at 430.

[93] *See* Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT. L. ONLINE, 2011, available at http://www.yjil.org/docs/pub/o-37-hinkle-countermeasures-in-the-cyber-context.pdf

traditional military forces.[94]" This was the first position adopted by the United States Department of Defense regarding the legal framework governing DOD's use of cyberspace.[95]

The Equivalent Effects Test is an attempt to graft cyber weapons directly onto the current U.N. Charter legal regime. Under this test, the 2007 and 2008 Russian cyber attacks in Estonia and Georgia would not rise to the level of an armed attack. The defacement of government and commercial websites, while a valuable component of a full-spectrum assault, is not the effect that any kinetic, traditional military assault would have on the Georgian and Estonian cyber networks. A missile might destroy a server, and thus deny access to its users, but a purely electronic attack that overloads the server does no physical damage. The effects of the cyber attacks in Georgia and Estonia were on a different level than the results of any of Russia's military operations.[96]

An analysis of Stuxnet under the Equivalent Effects Test is much more difficult, and ultimately reveals the inability of the Equivalent Effects Test to properly classify the use of today's modern cyber weapons. Unlike the simple DDoS attacks and website-alteration used in Estonia and Georgia, Stuxnet sought out and physically damaged Iran's nuclear research infrastructure.[97] Comparisons to the effect of a cruise missile or a commando raid quickly spring to mind.

While these analogies are valid, Stuxnet created effects that were far more limited than an airstrike or commando operation. An airstrike would have created considerable collateral

---

[94] Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 997 (2011).

[95] *See, e.g.,* OFFICE OF GEN. COUNSEL, U.S. DEP'T OF DEF., AN ASSESSMENT OF INTERATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (2d ed. 1999).

[96] However, Shackelford and Andres note that "while not an armed attack, cyber attacks can be precursors, warning that a more serious attack is about to begin." 42 Geo J. Int'l L. at 999. Indeed, the cyber attacks against Georgia heralded the imminent military incursion and seemed intended to augment the Russian advance.

[97] *Supra* Note 37.

damage to the Natanz facility, destroying far more than the targeted centrifuges. The effects of a commando raid to destroy Natanz' centrifuges are difficult to predict, but the process of inserting and retrieving the attacking forces is far more likely to result in the destruction of property and lives outside of the narrow objective. The Equivalent Effects Test fails because it treats cyber attacks as something outside of "traditional" military actions. As this paper has demonstrated, cyber weapons have been integrated into the military arms of the significant world powers. This integration renders the search for an "equivalent effect" obsolete. Cyber attacks should not be compared to older methods of military action as if they operate in some other reality. They are their own weapons, capable of achieving unique military objectives.

ii. Schmitt Test

Professor Michael Schmitt developed a framework for analyzing cyber attacks as potential armed attacks falling under Article 51.[98] His test attempts to combine the recognition of the military applications of cyber weapons with the reality that not all cyber attacks will meet the armed attack threshold.[99] Schmitt's analysis focuses on seven factors on a case-by-case basis.

1. *Severity* – How many people were killed, and how much damage was inflicted?
2. *Immediacy* – How fast and unexpected was the military action?
3. *Directness* – Is there a clear cause and effect relationship?
4. *Invasiveness* – Are militaries crossing borders, causing substantial effects?
5. *Measurability* – How accurately can the effects be calculated?
6. *Presumptive Legitimacy* – Is the cyber attack an action that presumably takes a country to accomplish, indicating a high level of coordination?

[98] For Prof. Schmitt's full analysis, *see* Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).
[99] *Id. at 889*.

7. *Responsibility* – Which nation's military forces were responsible?[100]

Professor Schmitt's test creates a spectrum upon which an individual cyber attack can be measured and compared. For example, Schimtt finds that a cyber attack that shuts down air traffic control systems, causing airplane crashes and significant casualties, would constitute an armed attack under Article 51.[101] On the other end of the spectrum, Schmitt cites the scenario of a malware code used to crash a university computer system in order to delay government research as not sufficient to constitute an armed attack.[102]

Where does Stuxnet fall under the Schmitt analysis? The Stuxnet virus wreaked havoc on a critical Iranian computer system, causing extensive and expensive damage. The sensitive, precise nature of the Stuxnet strike combined with the importance of the target computer system points in the direction of Schmitt's air traffic control scenario. However, the attack did not cause any casualties and did not cause collateral damage outside of the Natanz facility. Additionally, Stuxnet struck a research project, the kind of target Schmitt did not believe was important enough to trigger self-defense rights under Article 51.[103] The balance of the factors, however, favors treating Stuxnet as an armed attack under the Schmitt Test. Stuxnet caused physical damage to the Iranian nuclear infrastructure, was highly invasive, its damage was quantifiable,[104] and it was almost certainly created under the auspices of a national government.

---

[100] James B. Michael, et al., *Presentation at the 27th Annual IEEE Int'l Computer Software and Applications Conference, Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System* (Nov. 5, 2003).

[101] COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 24 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2010)

[102] *Id.*

[103] *Supra* Note 98 at 900.

[104] Estimates of the actual damage wrought by Stuxnet range wildly, primarily because the Iranian government has, understandably, not been forthcoming with the information. *See* Jeffrey Goldberg, *Could Iran Be Using Stuxnet to Confuse the West?* THE ATLANTIC, March 4, 2011.

While Schmitt's analysis provides a modicum of the flexibility and close analysis that states need when evaluating whether an attack against their cyber networks has triggered their Article 51 right to self-defense, the real-world example of Stuxnet reveals that even the in-depth Schmitt Test is unworkable in the event of a modern cyber conflict. Like the equivalent effects test, the Schmitt Test is an academic exercise that, while "quite helpful academically, is not easily applicable in an operational setting.[105]" When a military crisis occurs, time is of the essence. A state government needs a fast, streamlined analysis of its legal and military options, particularly in the case of a cyber attack, which may be the prelude to kinetic military strikes.[106] Likewise, the intent, origin, and effects of a cyber attack might not be known for months or years after the initial manifestation of the attack. For example, Stuxnet was probably introduced into Iran six months to a year before its activation.[107] Finally, the effects of the Stuxnet attack took months to reveal themselves, and are still not fully known. Older tests meant to apply Articles 2(4) and 51 to traditional military actions do not translate well to the cyber realm.[108]

2. Fundamental Flaws of Effects-Based Tests

For all the practical encumbrances that weaken the application of effects-based tests in determining if a cyber attack is an armed attack according to Article 51, the greatest flaw in the traditional tests rests upon the seemingly simple issues of attribution and identification of any

---

http://www.theatlantic.com/international/archive/2011/03/could-iran-be-using-stuxnet-to-confuse-the-west/72040/

[105] Shackelford & Andres, *Supra* Note 86 at 998.

[106] *Supra* Note 88.

[107] Kim Zetter, *Stuxnet Timeline Shows Correlation Among Events*, WIRED, July 11, 2011, available at http://www.wired.com/threatlevel/2011/07/stuxnet-timeline/

[108] *See* Hinkle, *Supra* Note 93. "Because these lesser uses of cyber-force can still have disruptive and threatening effects, states will want to react to them quickly and effectively."

attackers. The infrastructure of the internet allows attackers to route their attacks through multiple systems in multiple countries far from the true source. This is exactly what the makers of Stuxnet did.[109] As the previous analysis of Stuxnet and the Georgian-Estonian cyber attacks reveals, even the most advanced forensic technology will have a difficult, if not impossible, time attempting to link cyber attacks or intrusions to a specific source.[110]

Even if investigators are able to follow an electronic attack through a complicated tunnel of servers across the world, they may find themselves "stymied by a collision between fundamental principles of physics and those of international law.[111]" The electrons which comprise cyber transmissions flow largely unimpeded across borders, but the jurisdiction of national investigative agencies largely ends at their own geographic boundaries. Even if a state can use the old tests to determine it is the victim of an armed attack in cyberspace, the U.N. charter offers no guidance for preventing the spillover of a cyber conflict into neutral, innocent states as the victim state seeks to assert its Article 51 rights. Should states have carte blanche to hold neutral nations responsible for an armed cyber attack simply because the electronic signal passed through their servers? The old tests do not apply to the science and methods of cyber warfare. The twin problems of identification of cyber attackers and attribution of identification threaten to obliterate any force behind Articles 2(4) and 51.

Such problems connecting armed attacks to a single perpetrating state are not new. During the Cold War, decades of small-scale proxy conflicts undermined Articles 2(4) and 51,

---

[109] *Id.*

[110] UNTANGLING ATTRIBUTION: MOVING TO ACCOUNTABILITY IN CYBERSPACE, PLANNING FOR THE FUTURE OF CYBER ATTACK: HEARING BEFORE THE H. SUBCOMM. ON TECH. AND INNOVATION OF THE H. COMM. ON SCI. AND TECH., 111TH CONG. (July 15, 2010) (Statement of Robert F. Knake, Int'l Aff. Fellow in Residence, Council on Foreign Relations)

[111] James A. Lewis, *Multilateral Agreements to Constrain Cyberconflict*, ARMS CONTROL TODAY, June 2010 at 16 (arguing states should develop mutual understandings on "what actions can be considered a violation of sovereignty, on what constitutes an act of war, and what actions are seen as escalatory.")

which were written with the massive movements of armies seen during World War II in mind.[112] During conventional wars, "the scale, formations, and strategy…[made] the identification of aggression relatively easy.[113]" As the superpower belligerents of the cold war squared off through "proxy conflicts" in the Middle East, South America, and East Asia, "the small-scale and diffuse new wars of insurgency, by their nature, made clear-cut distinctions between aggression and self-defense, which are better adapted to conventional military warfare, exceedingly difficult.[114]" The International Court of Justice was able to use effects-based tests in order to find that the United States did not committ an "armed attack" on Nicaragua by supplying and supporting the Contra guerrillas,[115] but that decision was hotly contested by international scholars.[116] The advent of cyber warfare has driven a further gulf between the world envisioned by the U.N. Charter and modern international relations.

3. Definitional Test – An Incomplete Solution

Some theorists have begun to propose alternative tests to guide states in determining when they may resort to the use of force in self-defense in response to a cyber attack. Of these proposed reinterpretations of the Charter, U.S. Air Force Major Graham Todd's is the most creative. In his proposal, Major Todd recognizes the problems inherent in holding states accountable under the Charter for armed attacks in cyberspace, as well as problems of neutrality and attribution for the states from which a cyber attack might have originated or passed

[112] The U.N. Charter was incorporated in 1948
[113] Thomas M. Franck, *Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States*, 64 AM. J. INT'L L. 809 (1970); *see also* Michael J. Glennon, *How International Rules Die*, 93 GEO. L.J. 939 (2005)
[114] *Id*. at 820
[115] *Military and Paramilitary activities in and against Nicaragua* (Nicar. V. U.S.), 1986 I.C.J. 14 (June 27).
[116] *See* John Norton Moore, *The Nicaragua Case and the Deterioration of World Order*, 81 AM. J. INT'L L. 151 (1987)

through.[117] Maj Todd looks at principles of criminal law to find a test that provide both clear lines of responsibility for states which may use cyberspace to deliver an attack against an enemy and a clear standard for a victimized state to employ when deciding if an armed attack has occurred and, if so, how and whom to strike back.[118]

Major Todd's test is twofold. He analyzes 1) The intent of the party conducting the attack, and 2) Knowledge and approval/acquiescence of the state which exercises legal control of the actor.[119] Combining the two relevant factors, he creates the following test for am armed attack in cyberspace: "A cyberspace attack occurs when a state knowingly uses or knowingly acquiesces to an entity under its legal control or within its territory using a cyberspace weapon against the people or property of another state.[120]"

Major Todd's goal is "to develop a framework that inspires states to cooperate to eliminate the harmful use of cyberspace-to create deterrence.[121]" To that end, he succeeds in tying the acts of private actors within the borders of a state to that state's government as long as the government "knowingly acquiesces" to the private actor's cyberspace attack on another state.[122] Major Todd's test, therefore, solves the problem of attribution and neutrality inherent in the traditional Effects-Based Tests. While the effects-based tests do not offer victims of a cyber attack a way to determine whether their right to self-defense has been triggered by a cyber attack that did not originate directly from the host state or was assisted by the networks of a third-party state, Major Todd's test applies a clear *mens rea* standard of culpability.[123]

---

[117] Maj. Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 66-7 (2009).
[118] *Id.*
[119] *Id.* at 86.
[120] *Id.* at 87.
[121] *Id.* at 89.
[122] *Id.*
[123] Maj Todd discusses a range of available defenses, all of them based on standard criminal law doctrine, such as impossibility. *Id.*

Does the Definitional Test solve the twin problems of attribution and identification that threaten to lead to unpredictable escalations of cyber conflict? Application of the Stuxnet attack Major Todd's test reveals that, not only does the Definitional Test fail to solve the technological and legal barriers to identifying belligerents in cyberspace, it may exacerbate the ultimate danger of the current state of U.N. Charter interpretation: An unregulated, rapid expansion of a cyber war in both the electronic and physical realms.

If Iran had been using Major Todd's test when the Stuxnet virus revealed itself, they would have determined the virus to be an armed attack under the U.N. Charter, thereby triggering their right to self-defense. As described in this paper, Stuxnet was clearly a "cyberspace weapon," designed to seek out and corrupt the software program running the Natanz centrifuges, destroying the affected machinery.[124] With that question out of the way, Iran would have looked for any state that "knowingly use[d] or knowingly acquiesce[d] to an entity under its legal control or within its territory.[125]" At this point, the Definitional Test begins to fail.

If Stuxnet was indeed created by a state actor, as all the evidence suggests, which state did it? How many states let their own intelligence arms cooperate with the primary culprit in designing the virus? Given the political situation, the primary suspects would be the United States and Israel, two strategic allies with fully-developed cyber intelligence capabilities.[126] However, the evidence linking the American and Isreali governments to Stuxnet is circumstantial at best.[127] There is no "Made in Washington/Tel Aviv" stamp in the Stuxnet Code.[128] What

[124] While the question of how to define a cyberspace weapon is still open, Maj Todd's definition will suffice. "Any capability, device, or combination of capabilities and devices, which if used for its intended purpose, is likely to impair the integrity or availability of data, a program, or information located in a computer or information processing system." *Id*. at 83.
[125] *Id.* at 87.
[126] *See* Zetter, *Supra* Note 10 at 6.
[127] *Id.*
[128] *Id.*

about Denmark and Taiwan, where Stuxnet's launching pad servers were located?[129] Iran would have to investigate whether those two governments acquiesced to the placement of Stuxnet on their servers. While unlikely, such a possibility would be extremely difficult to prove or disprove.

In this scenario, Iran finds itself in a situation similar to one which would have transpired if it were trying to apply one of the Effects-Based Tests: It knows it has been attacked by a cyber weapon, but it does not have a clear trail of liability. However, the Definitional test expands liability so far that a victimized nation could plausibly claim Article 51 self-defense against any number of ostensibly neutral countries. The Definitional Test grants a suitably belligerent victim the ability to expand a cyber conflict zone, turning a simmering online war into one which may embroil many other governments.[130] The Definitional Test, as an academic exercise, is superior to its Effects-Based predecessors, but it still leaves the management of time-sensitive crises up to individual states, which may have developed their own independent cyber warfare doctrines or even wish to respond to a cyber attack with kinetic military force.[131]

Is the hazy regime of state responsibility envisioned by the Definitional Test an effective way to prop up the U.N. Charter in the new age of warfare? If a "hacktivist" group such as Anonymous launched a massive cyber attack against a rival of the United States during a time of acute tension, a state following the Definitional Test for an armed attack would be strongly

---

[129] *Id.*

[130] *See* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty To Prevent*, 201 MIL. L. REV. 1, 6, 37 (2009)

[131] *See* Eric Talbot Jensen, *Computer Network Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 229-31 (2002) (noting that states should be able to defend against computer network attacks, whether or not classified as uses of force, and reviewing both active and passive defense options).

inclined to respond before the "true" culprits could ever be identified.[132] Under the Definitional Test, the chances of a cyber conflict devolving into a widespread, unregulated war are still too high.

IV. Regulating the New Era of Cyber War

The development of cyberspace has connected the world in ways that were confined to science fiction just two decades ago. A marked exception to this trend of cooperation and interconnectivity is the application of military force through cyberspace. The interpretive holes in the U.N. Charter's regulations on use of force and self-defense right that developed during the Cold War have been blown wide open by the militarization of cyberspace. State governments are currently content to operate within their own interpretations of the laws of war and in consideration of their individual strengths and interests.

The willingness of powerful states to skirt the prohibitions on use of force and armed attack in the U.N. Charter is nothing new. Local conflicts between neighboring belligerents (and even conflicts within one country) often became shadow wars, in which the United States and Soviet Union funneled money, materiel, and ideology into the conflict.[133] As the *Nicaragua* case revealed, the U.N. was unable to stretch the interpretation of Article 2(4) and 51 to cover proxy conflicts, even when the entire world knew the driving forces behind the conflict.[134] The failure

---

[133] Scott L. Bills: *The World Deployed : US and Soviet Military Intervention and Proxy Wars in the Third World Since 1945*. From: Robert W. Clawson (Ed.): EAST-WEST RIVALRY IN THE THIRD WORLD, 77-101 (1986).
[134] *Supra* Notes 113-116.

of the U.N. Charter to effectively regulate asymmetric warfare led any scholars to propose that any previous inhibitive force exercised by the Charter on belligerent nations had died out.[135]

The international community has a narrow window of opportunity to define the parameters for military engagement in cyberspace, thereby saving the U.N. Charter from obsolescence and irrelevance. After the Russo-Georgian War, the Estonia incident, and Stuxnet, the issues surrounding the application of the established laws of war have crystallized. The ability to strike an enemy using servers placed around the world or civilian operatives with only a tenuous link to any state government continues the progression toward anonymity in use of force that developed during the Cold War.

With individual nations hoarding their cyber weapons, content to operate in a legal and strategic gray area, the U.N. is the most logical place to lay out the rules of war in cyberspace before they are established through costly (and potentially bloody) experience. If a future cyber war, or the escalation of a cyber war into a kinetic shooting war, is the event that defines the parameters of international cyber conflict, the U.N. will have lost the ability to make a proactive mark on the way war is fought in the 21st Century.

The most effective scenario is an international agreement adopting a standard of responsibility for armed attack in cyberspace that fuses the tough standards of liability for armed attack found in Maj Todd's Definitional Test with a means for victimized nations to quickly pinpoint and confront the "true" attacker without waiting for an armed invasion or drawing neutral nations into a wider conflict. In time, technological developments in tracking internet signals may make Major Todd's original approach workable. In the interim, however, an international consensus must be found to prevent shadow wars waged from the electronic

[135] *See* Moore, *Supra* Note 116 at 154.

darkness of the Internet or, conversely, overreactions from states that find themselves under attack from cyberspace.

Conclusion

Stuxnet put the world on notice to the maturation of cyber warfare. With the absence of an effective interpretation of Article 51, states are reserving for themselves the right to decide when to initiate a cyber war or, if victimized through cyberspace, how to react. Such a state of affairs is untenable and unacceptable. The persuasive and political force of the U.N. Charter, already called into question by its failure to regulate the proxy conflicts of the Cold War, will be relegated to obsolescence if the international community cannot act to find an international framework for the conduct of war in cyberspace. In this vacuum, individual states will continue to accord in according to their own interpretations of the Charter, which in many cases will be little more than articulations of a state's national interests. Eventually, different interpretations will clash, especially if more states begin adopting stricter self-defense doctrines such as the Definitional Appproach without an international forum for resolution or effective methods for identification of attackers.

Cyber attacks will play an increasingly central role in the conduct of warfare long into the future. The international community has a rare chance to establish the rules of warfare in a world without borders. In the past, experience with new weapons of war was enough to establish their place in the international legal order. Today, however, geographic borders are giving way to interconnected electronic passageways. Only an international solution can effectively regulate a war which can touch any nation in the world at any time. The time for the U.N. to reassert

itself is now. It must act before wealth, knowledge, and lives are needlessly lost in a conflict between states that still play by the old rules.