I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

# Cyber Attack Treaty Verification

GRANT HODGSON*

Abstract: A successful cyber treaty would require an effective way for each party to verify that the other parties were living up to their obligations. Despite the differences between cyber weapons and traditional weapons, verification methods used in treaties that limit nuclear weapons have several parallels that would be useful in a cyber treaty. Intrusion detection and network monitoring of the networks that a state controls parallels with national technical means. Cyber investigations using session reconstruction, log inspection, and traffic analysis would be a useful parallel to on-site inspections. In addition, data exchanges containing details about the most destructive cyber weapons would reduce the risk of attacks on critical infrastructure but still enable states to use intelligence gathering capabilities of cyber weapons.

## I. INTRODUCTION

A new cyber espionage group was discovered in 2014. It is suspected to be part of the Chinese government and has been named Axiom.[1] The group has been operating for at least six years,[2] and it has

* J.D., J. Reuben Clark Law School, 2016. MS Computer Science Candidate, Brigham Young University, 2017. The author would like to thank Eric Talbot Jensen for his excellent guidance.

[1] Ellen Nakashima & Ashkan Soltani, *FBI Warns Industry of Chinese Cyber Campaign*, WASH. POST (Oct. 15, 2014), http://www.washingtonpost.com/world/national-security/fbi-warns-industry-of-chinese-cyber-campaign/2014/10/15/0349a00a-54b0-11e4-ba4b-f6333e2c0453_story.html.

[2] Kaila Brosey, Cyber Security Coalition Releases Full Report on Large-Scale Interdiction of Chinese State Sponsored Espionage Effort, Novetta (Oct. 24, 2014), https://www.novetta.com/2014/10/cyber-security-coalition-releases-full-report-on-large-scale-interdiction-of-chinese-state-sponsored-espionage-effort/.

infiltrated over 43,000 computers, including computers in corporations and those owned by governments around the world.[3] Axiom has focused on economic targets including technology companies and other political targets that might threaten the stability of the Chinese government.[4]

Attacks similar to those performed by Axiom have led to an increased focus on cybersecurity by the United States[5] and other countries. One complicating factor in combating cyber attacks is the problem of attribution.[6] When a state discovers that a cyber attack has occurred, it is difficult to obtain conclusive proof that another state sponsored the attack. For example, conclusive proof may include specific text embedded in the code or the use of coding techniques known to be used by specific countries or groups. Similar to the attack on Sony, proof may also be obtained by placing malware on the networks used by attackers.[7] States are often able to deny involvement with any cyber attack. For example, China consistently denies U.S. accusations of cyber attacks and in return makes its own accusations of cyber attacks coming from the United States.[8] In regard to

---

[3] Franz-Stefan Gady, *The Axiom Report: Cybersecurity and Its Impact on China-U.S. Relations*, HUFFINGTON POST (Jan 5, 2014), http://www.huffingtonpost.com/franzstefan-gady/the-axiom-report-cybersec_b_6101206.html.

[4] Brosey, *supra* note 2.

[5] Damian Paletta, *White House Aims to Harden Cyberattack Defense*, THE WALL STREET JOURNAL (Jan. 11, 2015), http://www.wsj.com/articles/white-house-aims-to-harden-cyberattack-defense-1421023121.

[6] *See* Major Erik Mudrinich, Cyber 3.0: *The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F. L. REV. 167 (2012); Susan W. Brenner, "*At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINALITY 379, 409-29 (2007) (explaining the difficulty of attributing cyber attacks to a particular attacker); Duncan Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373 (2011).

[7] David Sanger & Martin Fackler, *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*, N.Y. TIMES (Jan. 15, 2015), http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

[8] Ellen Nakashima & Ashkan Soltani, *FBI Warns Industry of Chinese Cyber Campaign*, WASH. POST (Oct. 15, 2014), http://www.washingtonpost.com/world/national-security/fbi-warns-industry-of-chinese-cyber-campaign/2014/10/15/0349a00a-54b0-11e4-ba4b-f6333e2c0453_story.html; Simon Denyer, *China calls U.S. hacking accusations '**irresponsible and unscientific**'*, WASH. POST (June 5, 2015), https://www.washingtonpost.com/world/asia_pacific/china-calls-us-hacking-

accusations about Axiom, the Chinese Embassy stated that, "judging from past experience, these kinds of reports or allegations are usually fictitious."[9]

Many authors have suggested that a cyber treaty would be helpful to limit cyber attacks like the ones made by Axiom and others.[10] A cyber treaty could reduce the recent increase in cyber attacks,[11] and could help to limit the motivations for a devastating attack on U.S. critical infrastructure.[12] If a cyber treaty were to be successful, however, it would need an effective way for each party to verify that the other parties were living up to their obligations. According to one U.N. General Assembly resolution, "effective verification is an essential element of all arms limitation and disarmament agreements."[13] The purpose of verification is to "build confidence among states and ensure that agreements are being observed by all parties."[14] For example, on-site inspections and information exchanges were used to verify Syria's compliance with international

---

accusations-irresponsible-and-unscientific/2015/06/05/7989cad3-583f-417e-a0b7-34be46eb16ff_story.html.

[9] Franz-Stefan Gady, *The Axiom Report: Cybersecurity and Its Impact on China-U.S. Relations*, HUFFINGTON POST (Jan 5, 2014), http://www.huffingtonpost.com/franzstefan-gady/the-axiom-report-cybersec_b_6101206.html.

[10] *See* Rex Hughes, A Treaty for Cyberspace, 86(2) INT'L AFF. 523, 541 (2010); *Comment*, Stephen Moore, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C.J. INT'L L. & COM. REG. 223 (2013); J. Stein Schjolberg, Recommendation for Potential New Global Legal Mechanisms Against Global Cyberattacks and Other Global Cybercrimes: An International Criminal Tribunal for Cyberspace (ICTC) Cybercrimelaw (Feb. 22, 2013, 1:45 AM), http://www.cybercrimelaw.net/documents/ICTC.pdf; David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 MINN. J. INT'L L. 347 (Summer 2013); Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 Geo. J. Int'l L. 971, 993 (Summer 2011) ("Despite the support for this approach, both the details for how such a [cyber] treaty would function and whether there is sufficient political will to make it a reality remain uncertain.").

[11] David Sanger & Martin Fackler, *supra* note 7.

[12] Particia Zengerle, *NSA chief warns Chinese cyber attacks could shut U.S. infrastructure*, REUTERS (Nov. 21, 2014), http://www.reuters.com/article/2014/11/21/us-usa-security-nsa-idUSKCN0J420Q20141121.

[13] 1988 UN Assembly Res: A/RES/43/81.

[14] *Id.*

agreements to destroy its chemical weapons.[15] Syria was required to submit information describing the chemical weapons Syria possessed.[16] Syria was also subject to on-site inspections of facilities used for production and research of chemical weapons.[17]

However, given current technology, the fundamental differences between cyber weapons and traditional military weapons present challenges to verification techniques used in the past. This paper will discuss the challenges in constructing, implementing, and verifying a cyber attack treaty. Part II will discuss the nature of cyber attacks and what makes them difficult for verification purposes. Part III will describe techniques that have previously been used to verify other treaties. Each technique is evaluated for its potential efficacy when applied to cyber attacks.

## II. CYBER ATTACK FUNDAMENTALS

It is important to have a basic understanding of cyber attacks to understand why traditional verification techniques would be ineffective when applied to a cyber treaty.[18] There are many known forms of cyber attacks including Distributed Denial of Service (DDoS) attacks, IP spoofing attacks, Man-in-the-Middle attacks, DNS re-directs, and—perhaps the most common—social engineering attacks. In this section I will discuss the basics of malware and advanced persistent threats (APTs) because they are the kind of sophisticated attack a state would employ.

### A. *Malware Basics*

Cyber attacks typically rely on software vulnerabilities and malware (short for malicious software) to carry out the attacker's desired effect.[19] Malware often incorporates backdoors[20] and various

---

[15] Decision Destruction of Syrian Chemical Weapons, OPCW Executive Council, http://www.opcw.org/fileadmin/OPCW/EC/M-33/ecm33dec01_e_.pdf.

[16] *Id.* at 3.

[17] *Id.* at 4.

[18] For a good description of the hacking cycle and common forms of attack *see* PATRICK ENGEBRETSON, THE BASICS OF HACKING AND PENETRATION TESTING (2013).

[19] There are many different kinds of malware. There are overwriting viruses that overwrite the host files with their own malware code. CHRISTOPHER ELISAN, MALWARE, ROOTKITS & BOTNETS: A BEGINNER'S GUIDE 11 (2013). Some are known as parasitic infectors because

other features such as the ability to evade detection[21] and send sensitive information back to its controller. Attackers will often use social engineering to trick an unsuspecting user into installing the malware.[22] This occurs when a user clicks on a link embedded in an email or downloads an infected file from a compromised website. In addition, malware often has a rootkit[23] component that allows the intruder to gain control over the computer and perform any type of command from a remote location.[24]

### B. *Advanced Persistent Threats*

One type of advanced attack that would likely be used by a well-funded state actor is an advanced persistent threat (APT). The goal of

---

they "attach themselves to the host file during infection" then "take control of the host file's first instruction to point to the virus code. After the virus execution concludes, control is passed to the host program." *Id.* at 14. There are also boot-sector viruses that infects the boot sector of a disk to get control of the computer system's execution flow even before the operating system." *Id.* at 15. Network Worms are "Malware that replicates itself to multiple systems in the network with little or no user intervention using widely used network services such as browsing, e-mail, and chat." *Id.* at 22. A trojan horse is malware in disguise because "it passes itself as a harmless, legitimate program such as a game or a tool, easily convincing the user to execute it." *Id.* at 25.

[20] Backdoors "enable an attacker to gain access to a compromised system, bypassing any form of safeguards and authentication, usually through the use of undocumented OS and network functions." *Id.* They can be embedded in software that might otherwise serve a legitimate purpose. Remote access tools (RAT) are related to backdoors. They have additional features such as user interfaces and client components that allow the user to issue commands to the compromised computer. *Id.*

[21] *Evasive Malware Goes Mainstream*, HELPNETSECURITY (April 22, 2015), http://www.net-security.org/malware_news.php?id=3022.

[22] ELISAN, *supra* note 19. Malware will also have a regeneration component that rebuilds malware. *Id.* at 96. The regeneration component checks periodically if the malware still exists. If it does not, then it rebuilds the malware from an "encrypted backup source found in the compromised system or downloads it directly from a malware-serving domain." *Id.*

[23] A "Rootkit is an application (or set of applications), that hides its presence or presence of another application (virus, spyware, etc.) on the computer, using some of the lower layers of the operating system (API function redirection, using of undocumented OS functions, etc.), which makes them almost undetectable by common anti-malware software." *What is a Rootkit*, AVG HOME SUPPORT (2016), https://support.avg.com/SupportArticleView?l=en_US&urlName=What-is-rootkit.

[24] Root is the most privileged user on a computer. ELISAN, *supra* note 19 at 40. A "[r]ootkit is a set of tools that enables root level access on a computer system." *Id.*

an APT is to be persistent; gain access to a computer system and maintain a presence on the system for "long-term control and data collection."[25] With a successful APT, an attacker will complete a number of stages including reconnaissance, scanning, exploitation, maintaining access, and removing evidence.[26]

During the reconnaissance stage, attackers gather information on the target through publicly available sources. This may include public websites of a company or the social media profiles of employees.[27] For example, an attacker may look at technical job postings on the target's website because they often give clues about what kind of hardware and software the target is using.[28] If the attacker knows the target's hardware and software the attacker might figure out what type of techniques would be effective in an attack. By the end of the reconnaissance stage the attacker has gathered a large number of IP addresses that belong to the target network.[29]

In the scanning stage, an attacker identifies the specific ports[30] and services that the target network is running.[31] The attacker also performs vulnerability scanning during this stage.[32] Through vulnerability scanning the attacker can discover "known weaknesses in the services and software running on a target machine."[33]

---

[25] Colin Tankard, *Advanced Persistent Threats and How to Monitor and Deter Them*, NETWORK SECURITY JOURNAL 16 (2011).

[26] ENGEBRETSON, *supra* note 18, at 14.

[27] Tony Sager, *Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention* (SANS Inst., July 2014), https://www.sans.org/reading-room/whitepapers/analyst/killing-advanced-threats-tracks-intelligent-approach-attack-prevention-35302.

[28] ENGEBRETSON, *supra* note 18, at 25.

[29] *Id.* at 53.

[30] *Port*, TECHTARGET, http://searchnetworking.techtarget.com/definition/port (last visited May 5, 2016) ("In programming, a port (noun) is a "logical connection place" and specifically, using the Internet's protocol, TCP/IP, the way a client program specifies a particular server program on a computer in a network.").

[31] ENGEBRETSON, *supra* note 18, at 53. The attacker will often use a scanning tool such as Nmap during this stage.

[32] *Id.*

[33] *Id.*

In the exploitation stage, the attacker typically makes an initial compromise where it gains access to the target network.[34] The attacker might take advantage of a software vulnerability or use social engineering including phishing and spear phishing.[35]

In the maintaining access stage, attackers establish a foothold, ensuring that they can "access and control one or more computers within the victim organization" from outside the organization's network.[36] To maintain presence, attackers might install new backdoors and different malware on multiple computers.[37] Attackers then try to gain access to more resources within the target organization's network by escalating privileges.[38] One way this can be done is by obtaining usernames and passwords from people with greater privileges such as network administrators.[39] Attackers perform internal reconnaissance using operating system commands to obtain information about the target organization's network including "computers, trust relationships, users, and groups."[40] The attacker issues a command (such as the "net" command if the computer is using windows) on the victim system to see if any other computers are connected to the same system.[41] If the victim system is part of a network (e.g. connected to a company network), the attacker will then begin scanning ports from the victim system.[42] The scan allows the attacker to identify services running on other systems, and learn

---

[34] *Exposing One of China's Cyber Espionage Units*, MANDIANT (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf at 63.

[35] Tankard, *supra* note 25, at 16-17.; Kim Zetter, *Hacker Lexicon: What Are Phishing and Spear Phishing*, WIRED (Apr. 7, 2011), http://www.wired.com/2015/04/hacker-lexicon-spear-phishing/.

[36] *Exposing One of China's Cyber Espionage Units, supra* note 34, at 63.

[37] *Id.* at 64.

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] Tankard, *supra* note 25, at 17.

[42] Binde, McRee & O'Connor, *Assessing Outbound Traffic to Uncover Advanced Persistent Threat*, SANS 3, *available at* http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf.

valuable information about the network.[43] Essentially, the scan lets the attacker create a map of the network. Once the attacker has the network mapped out, the attacker may move to targeting high priority victims that have access to valuable data.[44]

Often attackers will have to move laterally (to other computers) within the target organizations network because the initially compromised systems do not contain the information that the attackers are after.[45] Once entry is gained onto a computer in a system, attackers use a technique known as pivoting. Pivoting involves exploiting "the systems they have compromised to attack other systems on the same network and avoid restriction such as those set by firewalls."[46] Pivoting allows them to explore the company's network, look for intellectual property and other data, and then send the data to the command and control servers.[47]

Finally, during the remove evidence stage, attackers make efforts to cover their tracks. This may include clearing event logs and erasing command history.[48] Log files[49] record events such as successful or unsuccessful logins and security events.[50] Thus, log files are one way that the target can discover what has taken place on their network. In Linux systems, previous commands issued on the computer will be

---

[43] Tankard, *supra* note 25, at 17.

[44] Binde, McRee & O'Connor, *supra* note 42.

[45] *Exposing One of China's Cyber Espionage Units, supra* note 34, at 64.

[46] Tankard, *supra* note 25, at 17.

[47] *Command and Control Server*, TECHTARGET, http://whatis.techtarget.com/definition/command-and-control-server-CC-server (last visited on Apr. 11, 2015) ("A command and control server (C&C server) is the centralized computer that issues commands to a botnet (zombie army) and receives reports back from the coopted computers.").

[48] *Hack Like a Pro: How to Cover Your Tracks & Leave No Trace Behind on the Target System*, WONDERHOWTO (2014), http://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-leave-no-trace-behind-target-system-0148123/.

[49] "A file that lists actions that have occurred. For example, Web servers maintain log files listing every request made to the server. With log file analysis tools, it's possible to get a good idea of where visitors are coming from, how often they return, and how they navigate through a site." Vangie Beal, *Log File*, WEBOPEDIA (2016) http://www.webopedia.com/TERM/L/log_file.html.

[50] *Hack Like a Pro, supra* note 48.

recorded in command history.[51] This also gives the target clues as to what has occurred recently, giving the attacker reason to erase it.

APTs are deemed advanced because once entry is gained, the attackers are able to avoid detection.[52] They use multiple techniques in combination, such as coupling zero-day exploits with social engineering.[53] Malware used in APTs is often able to recompile its code and use encryption to prevent detection from virus scanners. [54] The malware used in APTs is also stealthy.[55] APTs "aim to appear as close as possible to legitimate network traffic."[56] Victims are "often unaware of an attack until after the organization has been compromised."[57] One example of an APT is Operation Aurora. It was discovered by Google in 2010, and began with emails that were sent to carefully targeted Google employees.[58] The emails contained links to websites that "hosted malicious code used to exploit a zero-day vulnerability[59] in the Internet Explorer browser."[60] The attack used around twelve pieces of malware with "several layers of encryption to obfuscate the attack and avoid common detection methods."[61] The attackers also used "backdoors to communicate with remote [c]ommand and [c]ontrol [] centers via TCP port 443, which is usually

---

[51] Narad Shrestha, *The Power of Linux "History Command" in Bash Shell*, TECMINT (June 14, 2013), http://www.tecmint.com/history-command-examples/.

[52] Tankard, *supra* note 25, at 16.

[53] Advanced Persistent Threats and Other Advanced Attacks, WEBSENSE 4 (2011), available at https://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf.

[54] Tankard, *supra* note 25, at 16.

[55] Advanced Persistent Threats and Other Advanced Attacks, *supra* note 53.

[56] Tankard, *supra* note 25, at 16.

[57] Gordon Thomson, *APTs: A Poorly Understood Challenge*, NETWORK SEC. J. 11 (2011).

[58] Tankard, *supra* note 25, at 17.

[59] *What is a Zero-Day Vulnerability?*, PCTOOLS, http://www.pctools.com/security-news/zero-day-vulnerability/ (last visited on Apr. 11, 2015).

[60] Tankard, *supra* note 25, at 17.

[61] *Id.*

associated with encrypted traffic and which is therefore difficult to inspect."[62]

As can be seen from the above explanation, APTs and other cyber attacks are very different from traditional military weapons. While traditional military weapons such as tanks and missiles tend to be state monopolized, cyber weapons can be created and used by anyone.[63] In addition, cyber weapons are much more multipurposed than traditional military weapons. The cyber weapon that provides access to a computer can also be used in the destruction of the computer. While traditional military weapons are used mainly for destruction purposes, cyber weapons can be used for gathering information as well as destruction.[64] Cyber attacks are also much more difficult to detect when compared to traditional attacks such as bombings. These fundamental differences are the reason why verification techniques used for controlling nuclear weapons would have some challenges if used in a cyber treaty. The next section will discuss techniques used in verifying compliance with nuclear arms treaties and explain potential cyber parallels and the efficacy of those parallels if used in a cyber treaty.

## III. VERIFICATION

Verification methods are the techniques that treaty signatories use to determine whether other signatories are in compliance with their treaty obligations. Verification is an essential element of any arms control treaty because without it, signatories have no reason to trust the other parties to the treaty.[65] Verification must be strong enough to enable the involved parties to trust each other but not too intrusive that it becomes impractical. The minimum intrusion required has been described as "a level of verification intrusiveness sufficient to convince treaty signatories that other signatories cannot cheat in a militarily significant manner without such non-compliance being detected in sufficient time to negate any advantage gained by the

---

[62] *Id.*

[63] Anyone can download tools, such as Kali Linux, that facilitate hacking. *See* https://www.kali.org/.

[64] Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014), http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[65] *See* Zengerle, supra, note 12.

violator."[66] The goal of verification is to "provide clear and convincing evidence of compliance or non-compliance and [allow] parties to maintain confidence in each other as they [seek] to limit [weapons]."[67]

After World War II, several verification approaches have been used in treaties that limit nuclear weapons.[68] The techniques used in the treaties fall into the following categories: 1) National technical means (NTM)(e.g., the use of satellites to look at missile silos); 2) On-site inspections (OSI) (e.g., physical inspections of military bases); 3) Data exchanges (e.g., exchanging data about the technical details and capabilities of weapons); and 4) The use of committees to clarify and negotiate ambiguities found in treaties.

This section will focus on the above-mentioned techniques that were used in treaties that limited nuclear weapons between the United States and the USSR. It will describe each technique in more detail and discuss how the technique would apply to cyber verification. The techniques come from the Strategic Arms Limitation Treaties (SALT),[69] the Intermediate-Range Nuclear Forces (INF)[70] treaty, the Strategic Arms Reduction treaties (START I and START II),[71] the Test Ban treaties[72], and the Non-proliferation treaty (NPT).[73] These treaties

---

[66] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 11 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html).

[67] *See* 1988 UN Assembly Res., *supra* note 13.

[68] *See, e.g.*, Treaty on Measures for the Further Reduction and Limitation of Strategic Offensive Arms, U.S.-Russ., Apr. 8, 2010, S. TREATY DOC. No. 111-5 (2010); Treaty on the Limitation of Anti-Ballistic Missile Systems, U.S.-USSR, May 26, 1972, 23 U.S.T. 3435 [hereinafter ABMT].

[69] Interim Agreement on Certain Measures with Respect to the Limitation of Strategic Offensive Arms, U.S.-USSR, May 26, 1972, 23 U.S.T. 3462 [hereinafter SALT I Interim Agreement].

[70] Treaty on the Elimination of Intermediate-Range and Shorter-Range Missiles, U.S.-USSR, Dec. 8, 1987, 100 U.S.T. 1 [hereinafter INF Treaty].

[71] Treaty on the Reduction and Limitation of Strategic Offensive Arms, U.S.-USSR, July, 31, 1991, S. TREATY DOC. No. 102-20 (1992) [hereinafter START I]; Treaty on Further Reduction and Limitation of Strategic Offensive Arms, U.S.-Russ., Jan. 3, 1993, S. TREATY DOC. No. 103-01 (1993) [hereinafter START II].

[72] Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, Aug. 5, 1963, 480 U.N.T.S. 43.

served to limit escalations in the development of nuclear weapons.[74] Many of the treaties limited nuclear weapons by reducing the number of each party's missile launchers and warheads.[75] Some of the treaties focused on launchers because they are large, difficult to hide, and are required for a nuclear strike.[76] Following a description of each technique, I will discuss how effective the technique would be in a cyber treaty.

### A. *National Technical Means*

National Technical Means (NTM) include a nation's "technological capabilities, collection systems, and other intelligence and analytical resources" that can be used to gather information about the activities of actors around the world.[77] It is one of the most widely used verification methods because it is easy for one state to use even without an agreement from another state. NTM includes satellite, radar, radioactive air sampling, and other signals intelligence. Other specific examples of NTM methods include image and signal collecting satellites, seismic detectors, nuclear radiation detectors, radar, and infrared light detectors.[78] Most NTM technologies allow a state to gather information without entering another state's territory.[79] To make the NTM techniques more effective, NTM is often accompanied by treaty requirements that force cooperation between parties.

---

[73] Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161 [hereinafter NPT].

[74] *Strategic Arms Limitations Talks/Treaty (SALT) I and II*, U.S DEPARTMENT OF STATE https://history.state.gov/milestones/1969-1976/salt (last visited Apr. 10, 2015).

[75] Treaty between the United States of America and the Union of Soviet Socialist Republics on Strategic Offensive Reductions (START I), NUCLEAR THREAT INITIATIVE, http://www.nti.org/treaties-and-regimes/treaties-between-united-states-america-and-union-soviet-socialist-republics-strategic-offensive-reductions-start-i-start-ii/ (last visited Apr 10, 2015).

[76] Kifleyesus-Matschie, *supra* note 66, at 36.

[77] RICHARD SCRIBNER ET AL., THE VERIFICATION CHALLENGE 47 (1985).

[78] Kifleyesus-Matschie, *supra* note 66, at 24.

[79] Clarence Smith, *CIA's Analysis of Soviet Science and Technology*, CENTRAL INTELLIGENCE AGENCY, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/article04.html (last visited Apr. 10, 2015).

Satellites have been especially helpful to verify compliance with nuclear arms treaties. Satellites allow a state to see things all over the world, and allow a state to focus on a particular area if needed.[80] Further, the typical ways satellites are used are not considered violations of sovereignty.[81] Thus, states do not need to obtain permission from other states to use satellites. In addition, sites that are being monitored do not know exactly how and when they are being monitored.

The SALT regime used NTM and contained agreed upon rules that increased the verification abilities of NTM. For example, the parties established methods for tabulating the number of missiles held by a party.[82] The parties also used assumptions as long as they were not proven wrong "to compensate for dependence on a limited number of monitoring methods."[83] For example a silo observed by a NTM satellite was considered to contain the maximum number of missiles it could hold.[84] In addition, parties were required to notify each other of ICBM launches.[85] Further, items that were banned but looked like an uncontrolled item were required to have distinguishing features added to them.[86]

The Strategic Arms Reduction Treaty (START) also relied heavily on NTM. It had cooperative measures allowing NTM to be more effective than it otherwise would be.[87] The treaty defined what the

---

[80] Kifleyesus-Matschie, *supra* note 66, at 28.

[81] *See* Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928); Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 6, 43 (Apr. 9, 1949) (individual opinion of Judge Alvarez).

[82] Kifleyesus-Matschie, *supra* note 66, at 35.

[83] *Id.*

[84] *Id.*

[85] Agreement Between the United States of America and the Union of Soviet Socialist Republics on Notifications of Launches of Intercontinental Ballistic Missiles and Submarine-Launched Ballistic Missiles, U.S.-U.S.S.R., May 31, 1988, 27 I.L.M. 1200 (available at: http://www.state.gov/t/avc/trty/187150.htm).

[86] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 35 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html).

[87] Amy Woolf, *Monitoring and Verification in Arms Control* 23 (2011) available at http://www.fas.org/sgp/crs/nuke/R41201.pdf.

limited strategic nuclear delivery vehicles were and how warheads were to be counted.[88] In INF, NTM was also coupled with cooperative agreements. For example, the USSR periodically had to open sliding roofs of SS-25 missile shelters to be examined by satellites (because the SS-20 missile was similar to SS-25 and only the SS-20 was prohibited).[89]

The Nuclear Test Ban (NTB) treaties prohibited testing nuclear bombs that carried a payload greater than 150 kilotons.[90] They contained some cooperative measures that improved the capability of seismic monitoring.[91] Although a 150 kiloton test explosion could be detected using seismic monitoring anywhere in the world, due to margin of error problems any detection could have been as small as 75 kilotons or as large as 300 kilotons.[92] Thus, it needed cooperative measures to reduce the margin of error. To overcome the margin of error problem, the parties exchanged information regarding test sites and the surrounding geological environment.[93] Parties also verified

---

[88] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 45 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html).

[89] *Id.* at 38.

[90] *1963-77: Limits on Nuclear Testing*, COMPREHENSIVE TEST BAN TREATY, http://www.ctbto.org/the-treaty/history-1945-1993/1963-77-limits-on-nuclear-testing/ (last visited Apr 10, 2015).

[91] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 54 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html); *see also Comprehensive Test Ban Treaty*, ATOMIC ARCHIVE, http://www.atomicarchive.com/Treaties/Treaty19.shtml (last visited on Apr 11, 2015).

[92] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 40 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html); Vink & Pine, *The Politics of Verification: Limiting the Testing of Nuclear*, 3 SCIENCE AND GLOBAL SECURITY 267 (1993).

[93] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 54 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html).

each other by using satellites to "observe excavation and other evidence of nuclear testing."[94]

## B. *Cyber Applications of National Technical Means*

Despite the differences between cyber weapons and nuclear weapons,[95] some parallels exist between traditional NTM and NTM with cyber weapons. One possible cyber comparison to traditional NTM techniques such as the use of satellites, might be the use of network scanners[96] and intrusion detection systems.[97] For example, the Department of Homeland Security (DHS) describes a program known as Continuous Diagnostics and Mitigation (CDM) that quickly identifies and prioritizes cybersecurity risks.[98] States can gain some information about attackers by scanning and monitoring their own networks. Network monitoring can show what kind of traffic is occurring between networks within two different states.[99] For

---

[94] *See* Leith & Simpson, *Monitoring Underground Nuclear Tests*, in M. KREPON, P.D. ZIMMERMAN, L.S. SPECTOR, AND M. UMBERGER (eds.), COMMERCIAL OBSERVATION SATELLITES AND INTERNATIONAL SECURITY (1990).

[95] *See supra* II. Cyber Attack Fundamentals.

[96] Margaret Rouse, "Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment." *Network Scanning*, TECHTARGET, http://searchmidmarketsecurity.techtarget.com/definition/network-scanning (last visited Apr 10, 2015). Network scanners such as NMAP allow a user to "determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics." *Nmap Introduction*, Nmap, http://nmap.org/ (last visited Apr 10, 2015).

[97] Intrusion detection systems serve to "identify unauthorized, illicit, and anomalous behavior based solely on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting." *Intrusion Detection FAQ: What is Intrusion Detection?*, SANS, http://www.sans.org/security-resources/idfaq/what_is_id.php (last visited Apr 10, 2015).

[98] *See Continuous Diagnostics and Mitigation,* U.S. DEPT. OF HOMELAND SECURITY, (Nov. 6, 2015), http://www.dhs.gov/cdm.

[99] Dave Shackleford, *Optimized Network Monitoring for Real-World Threats*, SANS INSTITUTE (July 1, 2011), https://www.sans.org/reading-room/whitepapers/analyst/optimized-network-monitoring-real-world-threats-35040.

example, states can monitor and analyze all traffic on particular TCP or UDP ports.[100] Network monitoring will attempt to "match patterns of usage and behavior to detect malicious activity."[101] It can reveal what kinds of attacks are occurring on a network. However, fairly analogous to traditional NTM monitoring capabilities, cyber NTM also has its limitations.[102] Due to the high volume of traffic, it can be difficult to catch malicious activity occurring within a network.[103]

Another parallel to traditional NTM would be to gain access (by launching a cyber attack or with permission) to another state's computers, or routers that forward the other state's internet traffic on to its intended destination.[104] However, with that access a state could read other files on the computer or perform other malicious acts. The key to satellite and other NTM use is that it is not a violation of international law. In contrast, hacking into a computer to monitor activity might be viewed as a violation of international law.[105] At the very least, needing to launch a cyber attack to verify that another state is not launching cyber attacks seems to defeat the purpose of having a cyber treaty.[106] Thus, without a monitoring agreement between states, network monitoring would need to be limited to states monitoring their own networks.

---

[100] *Id.* at 7.

[101] *Id.* at 2.

[102] Companies and governments already use network scanners and intrusion detection systems. Although they are helpful, states still do not seem to have much trouble launching successful cyber attacks. *See* Paul Rubens, *Cybersecurity: Defending 'Unpreventable' Cyber Attacks*, BBC NEWS (Feb, 3 2015), http://www.bbc.com/news/business-31048811.

[103] Shackleford, *supra* note 99.

[104] JAMES F. KUROSE & KEITH W. ROSS, COMPUTER NETWORKING A TOP DOWN APPROACH 394 (5th ed. 2010).

[105] INT'L GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 24 (Michael N. Schmitt ed., 2013) ("The International Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty."). "Although there are provisions of international law that allow the violation of another state's sovereignty and territorial integrity to stop a harmful action that the originating state has not adequately addressed or does not have the means to address."

[106] *Id.* at 36 ("A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State"); *Id.* at 54 ("A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense.").

Another difficulty with NTM is that malware used in a cyber attack can be easily hidden in nearly any program or file. While it might not be too difficult to hide a nuclear missile launch pad, it is even easier for a state to hide a cyber attack.[107] This is partially because attacks can be launched from a computer nearly anywhere in the world even if the state does not own the computer. With nuclear missiles there are specific areas, like military bases, for satellites to focus on. In contrast, cyber weapons can be hidden in any computer, mobile device and sometimes even refrigerators.[108] For example, malware can be hidden in any Microsoft Office document.[109] With the advent of the internet of things (IoT), there will be a proliferation of attack vectors because more devices will be connected to the internet.[110] Thus, there will be even more places to hide malware as more devices become connected. According to the U.N. General Assembly, "[t]o be adequate and effective, a verification regime for an agreement must cover all relevant weapons, facilities, locations, installations and activities."[111] However, with cyber weapons, every piece of code is relevant because malware can be hidden anywhere. This makes it difficult to cover all relevant facilities, locations, installations and activities.

---

[107] *See supra* II.B.

[108] Ryan Grenoble, *Refrigerator Busted Sending Spam Emails in Massive Cyberattack,* HUFFINGTON POST (Jan. 24, 2014), http://www.huffingtonpost.com/2014/01/23/refrigerator-spam-email-internet-of-things-attack_n_4654566.html.

[109] Kevin Casey, *Retro Macro Viruses: They're Baaack*, INFORMATION WEEK (July 9, 2014), http://www.informationweek.com/vulns-threats/vulnerability-management/retro-macro-viruses-theyre-baaack/d/d-id/1279215; *Macros Explained: Why Microsoft Office Files Can Be Dangerous*, HOW-TO GEEK, http://www.howtogeek.com/171993/macros-explained-why-microsoft-office-files-can-be-dangerous/ (last visited Apr. 10, 2015). Macro viruses are created using Microsoft Office's application-specific programming language. *See* CHRISTOPHER ELISAN, MALWARE, ROOTKITS & BOTNETS: A BEGINNER'S GUIDE 19 (2013). Microsoft Office uses Visual Basic for Applications (VBA) as its programming language. *Id.* These kinds of viruses are operating system independent because they depend only on the application and not the underlying operating system. *Id.* at 21.

[110] *The Internet of Things is Far Bigger than Anyone Realizes*, WIRED, http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/ ("The Internet of Things revolves around increased machine-to-machine communication; it's built on cloud computing and networks of data-gathering sensors; it's mobile, virtual, and instantaneous connection; and they say it's going to make everything in our lives from streetlights to seaports 'smart'").

[111] G.A. Res. 43/81, U.N. DOC. A/RES/43/81 (Dec. 7, 1988).

### C. *On-Site Inspections*

On-site inspections (OSI) involve direct access to another state's military sites. OSI greatly improved verification abilities with respect to nuclear weapons. In reference to OSI, defense secretary Caspar Weinberger stated that it is "absolutely essential that we have something better in the way of verification than we have ever had before … the ability to go on each other's soil and …look in factories and look at gun sites. You have to have the ability to do what bank examiners do, if we want to be sure."[112]

One example of OSI was the suspect site inspections (also known as challenge inspections). They allowed a party to inspect any site that it suspected might be violating the treaty.[113] However, this type of inspection was not as strong as it might seem. With the exception of three designated sites in each country, a state could always refuse a challenge inspection.[114] Further, parties were allowed to answer the challenger's concerns by other means, if possible, and thus were able to avoid inspections entirely.[115] Another type of inspection was known as continuous inspection or portal monitoring. It gave a party the right "to measure all vehicles existing in the facility and inspect the interior of those large enough to contain a banned missile."[116]

---

[112] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 40 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html); J. Mendelsohn, *INF Verification: A Guide for the Perplexed*, ARMS CONTROL TODAY, 25-6 (1987) ("Caspar Weinberger on Meet the Press in September of 1986"); *see also* J. Dean, *The INF Treaty Negotiations*, SIPRI YEARBOOK, 375-94 (1988); Garthoff, *The Soviet SS-20 Decision*, 25:3 SURVIVAL, (1983); JONATHAN HASLAM, THE SOVIET UNION AND THE POLITICS OF NUCLEAR WEAPONS IN EUROPE 1969-87 (1990).

[113] *START I: Protocol on Inspection and Continuous Monitoring Activities*, ACQWEB, http://www.acq.osd.mil/tc/treaties/start1/protocols/insp_7-12.htm (last visited Apr. 11, 2015).

[114] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 48 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html).

[115] *Id.*

[116] *Id.* at 42. For information on portal monitoring see S.I. Griffiths, *The Implementation of the INF Treaty*, SIPRI YEARBOOK 1990: WORLD ARMAMENTS AND DISARMAMENT, OXFORD 447 (1990).

The Nuclear Test Ban treaty (NTB) allowed scientists to collect geological data and rock samples from the nuclear test site. This allowed a state to compare seismometer readings with on-site measurements and was "a real key to improving NTM." [117] For example, inspectors took soils samples and made geological measurements to make sure that an illegal explosion could not be concealed.[118]

### D. *On-Site Inspections Cyber Applications*

One potential cyber parallel to on-site inspections (OSI) would be cyber investigations or the use of cyber forensics. After discovering a cyber attack a state may find a likely source of the attack, perhaps a number of servers located in another state. Assuming that there is a cyber treaty between the two states, it would be useful for the treaty to contain a provision that allowed the victim state access to the suspect state's networks for a cyber investigation. Similar to the forced cooperation in nuclear arms treaties, a cyber treaty could force states to cooperate by placing network taps[119] that store network traffic for each other to examine when they suspect a cyber attack has occurred. Instead of using OSI's physical presence, facility sampling, and personnel interviews, a cyber investigation could use session reconstruction, log inspection, and traffic analysis to verify the suspect state's compliance with the treaty. In session reconstruction, captured packets are correlated with each other to determine what information

---

[117] C. Paul Robinson, *Verifying Testing Treaties – Old and New*, ARMS CONTROL TODAY, 3 (1990); *Dep't of Def. Authorization for Appropriations for Fiscal Year 1997 and the Future Years Def. Program: Hearing on S. 1745 Before the Committee on Armed Services United States Senate*, 104th Cong. (1996) (statement of Dr. C. Paul Robinson, President, Sandia National Laboratories); Kathleen C. Bailey & C. Paul Robinson, *To Zero or Not to Zero: A US Perspective on Nuclear Disarmament*, 28:2 SECURITY DIALOGUE 149, 149-58 (1997).

[118] *Comprehensive Test Ban Treaty (1996)*, ATOMIC ARCHIVE, http://www.atomicarchive.com/Treaties/Treaty19.shtml (last visited on Apr 11, 2015); Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 57 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html).

[119] *Network Tap Definition*, TECHTARGET, http://searchnetworking.techtarget.com/definition/Network-tap ("A network tap is an external monitoring device that mirrors the traffic that passes between two network nodes. A tap (test access point) is a hardware device inserted at a specific point in the network to monitor data").

was sent between two computers.[120] When the packets from the raw network data are reassembled, the data can be analyzed efficiently.[121] For example, session reconstruction would make it easy to search for keywords such as "bomb" in network data.[122] The network packets can also be correlated with information contained in logs to provide a more comprehensive picture of what events have occurred.[123]

Traffic analysis can also be used as a defensive technique to identify anomalies in traffic patterns. It can be used to "baseline the traffic to and from hosts on the network over time, in a graphical format (line charts or other graphs)."[124] The data can show how the network typically performs, "including packet quantity, packet sizes, bandwidth utilization, connections per hour, etc."[125] After learning what typical activity looks like, network administrators can detect "anomalies in connections between hosts and networks such as port-scans, DoS attacks, significant increases in bandwidth utilization, and other factors that might indicate hosts that are under attack or have become compromised."[126]

However, OSI that involves either a cyber investigation or physical presence at a facility would have several challenges. One key principle about verification arrangements is that they should be implemented without discrimination, and, in accomplishing their purpose, avoid unduly interfering with the internal affairs of State's parties or other States, or jeopardizing their economic, technological and social development.[127] One potential problem for OSI is that it may be difficult to establish without unduly interfering with the internal

---

[120] *TCP Session Reconstruction*, REDSPLICE (2016), https://www.redsplice.com/tcp-session-reconstruction/.

[121] CyberForensics: Understanding Information Security Investigations 86 (Jennifer Bayuk ed. 2010).

[122] *Id.*

[123] Dave Shackleford, *When Breaches Happen: Top Five Questions to Prepare for*, SANS INSTITUTE, https://www.sans.org/reading-room/whitepapers/analyst/breaches-happen-top-questions-prepare-35220.

[124] Stephen Northcutt, *Traffic Analysis*, SANS TECHNOLOGY INSTITUTE, http://www.sans.edu/research/security-laboratory/article/traffic-analysis.

[125] *Id.*

[126] *Id.*

[127] G.A. Res. 43/81, U.N. DOC. A/RES/43/81 (Dec. 7, 1988).

affairs of states. The problem stems from a lack of separation between cyber weapons and other harmless computer activities. Although inspecting another state's cyber infrastructure could help one state to verify that it was not used to launch a cyber attack, the inspecting state could also gain access to a treasure trove of information. A state's cyber infrastructure would likely hold very sensitive information, and by allowing another state to inspect the cyber infrastructure the state would run a risk of handing over the information to the inspecting state. Some of the data the inspecting state might look at, such as diplomatic communications, would be protected under international law from being accessed by other states.[128] According to the Tallinn Manual,[129] "[d]iplomatic archives and communications are protected at all times from cyber operations" regardless of whether the state is part of an armed conflict or not.[130]

However, this problem might be solved if the sensitive information were encrypted. Even if the network is tapped, the victim state will not be able to read encrypted network traffic. The victim state will be able to read the metadata (e.g. where the data was sent and the route it took to reach its final destination) and still gather useful clues relating to cyber attacks.[131] In addition, states could obfuscate network infrastructure that contains sensitive data to prevent an investigating state from accessing it.[132] States can create a subnet within a network to prevent inspection of the sensitive parts of the network.[133] If

---

[128] *See* Vienna Convention on Consular Relations arts. 33, 35, 24 April 1963, 596 U.N.T.S. 261.

[129] A manual on the "law governing cyber warfare" that was created by a group of international experts. INT'L GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 1, (Michael N. Schmitt ed., 2013).

[130] INT'L GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 233, Rule 84, (Michael N. Schmitt ed., 2013); Vienna Convention on Consular Relations arts. 33, 35, 24 April 1963, 596 U.N.T.S. 261; see also Tehran Hostages case, paras. 61-62, 77, 86; Vienna Convention on Consular Relations arts. 33, 35, 24 April 1963, 596 U.N.T.S. 261.

[131] Paul Assadoorian, *Analyzing Network Metadata*, TENABLE NETWORK SECURITY (Oct. 1, 2009), https://www.tenable.com/blog/analyzing-network-metadata.

[132] Network Infrastructure Obfuscation, U.S. Patent No. 14/058,034 (Filed Oct. 18 2013), *available at* http://www.google.com/patents/US20140115706.

[133] Bradley Mitchell, *IP Tutorial Subnets,* ABOUT.COM, http://compnetworking.about.com/od/workingwithipaddresses/a/subnetmask.htm.

encryption and obfuscated networks are overused, however, the investigating state will have not have enough power to adequately verify treaty compliance. Thus, a treaty would need to find the proper balance between protecting sensitive data and allowing a victim state to investigate treaty compliance.

A recent example helps illustrate how OSI in the form of a cyber investigation could be useful for verification. The U.S. suspects that Unit 61398 of China's People's Liberation Army (PLA) is using cyber attacks to steal intellectual property.[134] Mandiant, a cybersecurity firm released a report that reflects years of research on a hacker group named APT1.[135] The Mandiant report concluded that APT1's activities primarily occur in China and that the Chinese government is aware of the activities.[136] The Mandiant report further concluded that APT1 is likely PLA unit 61398.[137] The conclusions were based in part on evidence tracing APT1's activity to four large networks in Shanghai, two of which serve the building where Unit 61398 is located.[138] APT1's remote desktop sessions used the Chinese (simplified) U.S. keyboard[139] and 98% of the IP addresses used to log into APT1-controlled systems were located in China.[140] Mandiant was able to observe activity accessing hop points[141] from 832 IP addresses over a two year period.[142] The hop points were accessed through Remote

---

[134] Schmidt & Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES (May 19, 2014), http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0.

[135] *Exposing One of China's Cyber Espionage Units*, MANDIANT APT1, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (last visited Apr. 10, 2015).

[136] *Id.*

[137] *Id.*

[138] *Id.*

[139] Microsoft's Remote Desktop Client configures the keyboard based on the client's language setting. *Id.* at 4.

[140] *Id.*

[141] In this example, hop point refers to the computer that the hackers sent the attack from. Hackers will often send attacks from compromised computers that they do not own to avoid attribution.

[142] *Exposing One of China's Cyber Espionage Units*, MANDIANT APT1, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (last visited Apr. 10, 2015).

Desktop[143] and File Transfer Protocol (FTP).[144] Of the 832 IP addresses observed, 817 resolved to locations within Shanghai, China.[145] If the U.S. had network taps on networks in Shanghai, the U.S. might obtain even more evidence of cyber attacks or at least reduce the cost of cyber investigations. This might solve problems with attribution and make states less willing to perform cyber attacks if they know that the attacks can easily be traced back to them.

Another difficulty is that with cyber weapons, there are many locations to inspect. Malware can be hidden anywhere on any computer or server. Obvious locations to inspect would include computers on military bases and intelligence agency headquarters but it would be easy for a state to erase evidence, move evidence of cyber attacks to another location (if it knew its computers might be inspected), or use remote computers to launch the cyber attacks.

### E. *Data Exchanges*

Data exchanges are another key component of verification. According to the U.N. General Assembly, "[r]equests for inspections or information in accordance with the provisions of an arms limitation and disarmament agreement should be considered as a normal component of the verification process. Such requests should be used only for the purposes of the determination of compliance, care being taken to avoid abuses."[146] Several arms control treaties implemented ways for parties to exchange data about nuclear weapons. The INF treaty provided for Nuclear Risk Reduction Centers that managed "exchanges of baseline information and continuous data exchanges on the technical details of missiles."[147] Having an additional source of

---

[143] Connect to Another Computer Using Remote Desktop, *Connect to another computer using Remote Desktop Connection*, MICROSOFT, http://windows.microsoft.com/en-us/windows/connect-using-remote-desktop-connection#connect-using-remote-desktop-connection=windows-7.

[144] *Exposing One of China's Cyber Espionage Units*, MANDIANT APT1, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (last visited Apr. 10, 2015).

[145] *Id.*

[146] G.A. Res. 43/81, U.N. DOC. A/RES/43/81 (Dec. 7, 1988).

[147] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 40 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html).

information was useful because it allowed politicians more "leeway to publicize compliance judgments."[148] State leaders needed several methods to obtain information because it is more difficult for an opposing state to thwart multiple methods of collecting information.[149]

In the START verification regime, each party was required to provide the other full access to telemetric information from missile flight tests.[150] The information access requirement "[a]pplied to nearly all [intercontinental ballistic missile] flight tests, not just those that might be considered a violation of the Treaty."[151] The parties agreed to exchange information on treaty-limited items and to notify each other of any future developments or changes to the treaty-limited items.[152] The parties also maintained a common database that contained "detailed records on the location and technical characteristics of all [t]reaty-related equipment."[153]

---

[148] *Id.* at 43; US Arms Control and Disarmament Agency, Annual Report to Congress 1988, p. 63 – cited in A.F. Woolf, On-site Inspection in Arms Control: Verifying Compliance with INF and START, Congressional Research Service 10, The Library of Congress, November 1, 1989; *See also* J.K. DAVIS ET AL., THE INF CONTROVERSY: LESSONS FOR NATO MODERNIZATION AND TRANSATLANTIC RELATIONS (1989).

[149] US Arms Control and Disarmament Agency, Annual Report to Congress 1988, p. 63 – cited in A.F. Woolf, On-site Inspection in Arms Control: Verifying Compliance with INF and START 10, Congressional Research Service, The Library of Congress, November 1, 1989.

[150] Treaty on the Reduction and Limitation of Strategic Offensive Arms, U.S.-USSR, art. X, July 31, 1991, No. 102-20 [hereinafter START I]; Amy Woolf, *Monitoring and Verification in Arms Control* 13 (2011) available at http://www.fas.org/sgp/crs/nuke/R41201.pdf.

[151] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 47 (2006) (unpublished Ph.D. dissertation, University of Erfurt) (on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html).

[152] Amy Woolf, *Monitoring and Verification in Arms Control* 2 (2011) *available at* http://www.fas.org/sgp/crs/nuke/R41201.pdf.

[153] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 48 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html); Treaty on the Reduction and Limitation of Strategic Offensive Arms, U.S.-USSR, art. VIII, July 31, 1991, No. 102-20.

F. *Data Exchanges: Cyber Applications*

If performed in a limited manner, data exchanges could be an effective and practical method for verification in cyber weapon treaties because it could be used to prevent the most destructive types of attacks. Exchanging data about cyber weapons would need to be limited because exchanging data about how the weapon works would likely render a cyber weapon ineffective. While states may be interested in preventing destructive attacks, they would likely not be willing to give up the intelligence gathering capabilities that cyber weapons offer. To understand why this is true, it is helpful to understand how malware remains effective and avoids detection.

Successful malware must be able to prevent anti-virus products from detecting its presence and it must also prevent anti-virus researchers from obtaining the malware source code.[154] Once the malware source code is obtained, the researchers can update the anti-virus products to recognize the malware and delete it immediately upon infection of a computer system.[155] In malware analysis, researchers find a copy of malware and then try to determine the functions, capabilities, and code that the malware is using.[156] Once the code is obtained the researchers can create "an effective signature to detect and eradicate the malware."[157] Thus, one instance of malware is typically not enough because if it is detected, a solution can be quickly made for all infected computers.[158]

Malware writers use a variety of anti-reversing and anti-analysis defenses to prevent researchers from successfully obtaining and analyzing the malware code.[159] Some of the techniques include code

---

[154] CHRISTOPHER ELISAN, MALWARE, ROOTKITS & BOTNETS: A BEGINNER'S GUIDE 102 (2013).

[155] Mandiant has reported that Iran-based malware remains on systems for an average of 28 days while China-based malware remains on systems for an average of 243 days. *Beyond the Breach,* MANDIANT, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

[156] Dennis Distler, *Malware Analysis: An Introduction*, SANS INST., *available at* http://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103.

[157] ELISAN, *supra* note 154, at 115.

[158] *Id.* It should be noted that signature based anti-virus techniques are becoming ineffective.

[159] *Id.* at 140.

obfuscation,[160] entry point obscuring,[161] malware encryption[162], and metamorphism.[163] Hackers often use many malware samples, enabling the hackers to remain in control of a system even if one or two malware samples are caught by anti-virus researchers.[164] This is partly why security researchers were finding 54,000 unique samples of malware per day in 2010.[165] In addition, malware typically has an installer component that "installs the malware and all its components in a target system."[166] The installer often deletes itself after installing the malware to prevent anti-virus researchers from gaining possession.[167]

Thus, because malware depends so heavily on keeping its code secret, if a cyber treaty were to include verification methods that

---

[160] "In software development, obfuscation is the deliberate act of creating obfuscated code, i.e. source or machine code that is difficult for humans to understand. Like obfuscation in natural language, it may use needlessly roundabout expressions to compose statements." *Obfuscation (software)*, WIKIPEDIA, https://en.wikipedia.org/wiki/Obfuscation_(software) (last visited May 12, 2016).

[161] Piotr Bania, *Fighting EPO Viruses*, SYMANTEC (Jun 28, 2005), http://www.symantec.com/connect/articles/fighting-epo-viruses ("An entry- point obscuring virus is a virus that doesn't get control from the host program directly. Typically, the virus patches the host program with a jump/call routine, and receives control that way.").

[162] Attackers will encrypt malware to make it difficult for anti-virus researchers to understand what the malware is doing. *See Encrypted malware and code reusability*, SANS ISC INFOSEC FORUMS, https://isc.sans.edu/forums/diary/Encrypted+malware+and+code+reusability/2223/.

[163] ELISAN, *supra* note 159, at 134-35 (stating that in metamorphism the malware uses a mutation engine that changes the code of the malware without changing its functionality making every infection different and harder to detect).

[164] *Id.* at 115.

[165] *Id.* at 153.

[166] *Id.* at 88.

[167] *Id.* The malware waits for an internet connection and then downloads necessary components allowing it to be small and hard to detect. *Id.* at 90-91. The malware installer can use a URL and a server. The Server can be one that is used for a legitimate looking website. Some examples include "online dropboxes, free web hosting sites, free cloud drives." *Id.* at 92. This allows malware to escape a URL blacklist making it hard to detect. *Id.* In addition, it provides cover because the "only way to find out the exact location of the malware being hosted in the legitimate site is through analysis of a captured malware sample." *Id.*

require parties to exchange details about the cyber weapons they use, the cyber weapons would become ineffective. Any data that reveals the functions and capabilities of malware would greatly assist anti-virus researchers in creating a solution that defeats the malware. States would likely be reluctant to share data about their cyber weapons if it rendered them useless and thus would not want to enter into a cyber treaty that contained data exchange provisions for cyber weapons.

However, states may find it practical to exchange limited amounts of data specific to only the most destructive types of attacks. For example, states could exchange data about cyber weapons that target industrial control systems or any weapons that target critical infrastructure such as financial services, nuclear reactors, dams, and chemical facilities.[168] The disclosures could be limited to operating systems, protocols, and software that these systems use. This is especially true if cyber attacks become more damaging and occur more frequently. For example, the U.S. and China may enter into this type of exchange to prevent massive power outages.[169]

### G. *Committees and Other Treaty Provisions*

Several treaties also included committees and other treaty provisions to create a more robust verification regime. For example, the SALT regime created the Standing Consultative Committee (SCC). The SCC was a Joint body made of delegates from each party that met at least twice a year.[170] Although the group had no legal or jurisdictional authority, it would obtain results by seeking to establish consensus between the parties.[171] The purpose of the committee was to clear up ambiguities that were discovered as the treaty's verification provisions were implemented.[172] The group's business was done in

---

[168] For a complete listing of critical infrastructure, see *Critical Infrastructure Sectors*, HOMELAND SECURITY, http://www.dhs.gov/critical-infrastructure-sectors.

[169] *See* Steve Reilly, *Bracing for a Big Power Grid Attack: One is too Many*, USA TODAY (Mar. 24, 2015), http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/.

[170] Mitslal Kifleyesus-Matschie, The Role of Verification in International Relations: 1945-1993, 37 (2006) (unpublished Ph.D. dissertation, University of Erfurt, on file with author and available at http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-10690/html/front.html).

[171] *Id.*

[172] *Id.*

private and was classified.[173] Privacy allowed "serious negotiation and the resolution of disputes by allowing sensitive issues and ideas to be realized in the absence of public pressures."[174] In addition, the SCC was responsible for the agreed database that contained exchanged data on nuclear missiles.[175]

Further, the Nuclear Test Ban treaty contained at least one provision that might prove useful in a cyber verification regime. It contained a "whoops" clause allowing "for one or two slight unintentional breaches per year, which when noted by the other party would be termed a 'cause for concern' but not serious enough to warrant withdrawing from the treaty."[176]

### H. *Cyber Applications of Committees and Other Treaty Provisions*

A committee would be a useful mechanism to clarify requirements of a cyber treaty. It could, for example, clear up ambiguities on treaty provisions regarding cyber investigations such as network taps and network obfuscation. Just as the SCC's activities were classified and private, a cyber verification committee's business should also be classified to reduce public pressures.

A Whoops clause would be particularly useful with cyber weapons because they tend to proliferate and accidentally end up on systems they were not intended for. One example of this is the Stuxnet virus, which was used to disrupt Iran's uranium enrichment program.[177] Although the virus was never meant to be used outside of Iran's uranium enrichment facilities, it replicated itself and began spreading

---

[173] *Id.*

[174] J. Boulde, *Bilateral Nuclear Agreements: The Standing Consultative Commission and the Special Verification Commission*, in E. Morris (ed.), INT'L VERIFICATION ORG., CTR. FOR INT'L AND STRATEGIC STUDIES 205 (1991).

[175] Kifleyesus-Matschie, *supra* note 170, at 36.

[176] *Id.* at 56.

[177] David Sanger, *Obama Order Sped Up Wave of 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?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all (the virus "accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet.").

throughout the internet due to a bug[178] in the code.[179] The proliferation of Stuxnet may not have caused a great deal of damage to ordinary computer users, but it is possible that the proliferation of another virus could cause significant damage. It is possible that a future cyber attack launched by a state A against a state B would accidentally infect cyber infrastructure in a state C. If state A and state C had a cyber treaty with a verification regime then it would be useful for it to include a whoops clause excusing state A's buggy cyber attack. Such a whoops clause could prevent state C from withdrawing from the treaty.

## IV. CONCLUSION

Despite the differences between cyber weapons and traditional weapons, verification methods used in treaties that limit nuclear weapons have several parallels that would be useful in a cyber treaty. Intrusion detection and network monitoring of the networks that a state controls parallels with NTM. Although there are some difficulties, cyber investigations would make a useful parallel to on-site inspections. Data exchanges containing limited details about the most destructive cyber weapons would reduce the risk of attacks on critical infrastructure but still enable states to use intelligence gathering capabilities of cyber weapons. A committee that is able to clear up ambiguities in private would also be helpful with cyber treaty verification. A combination of these techniques could provide an effective verification regime for a cyber treaty.

Without verification it may be difficult to create an effective treaty to limit cyber attacks. Fortunately, cyber attacks are not as devastating as nuclear missiles (at least for now).[180] Additionally, nuclear arms treaties have not eliminated nuclear weapons entirely. One major disincentive for a nuclear attack is the threat of a reciprocal attack. The same may be true for cyber weapons. For example, China would not want to launch a cyber attack to turn off the United States' power

---

[178] *Software Bug*, TECHOPEDIA, http://www.techopedia.com/definition/24864/software-bug- (last visited Apr. 10, 2015) (stating that a software bug is an "an error, mistake, defect or fault, which may cause failure or deviation from expected results").

[179] Sanger, *supra* note 177.

[180] No one has died from a cyber attack. Kelsey Atherton, *Cyber Attacks Are America's Top Security Threat. That's Better News Than It Sounds*, POPSCI (Mar. 14, 2013), http://www.popsci.com/technology/article/2013-03/cyber-attacks-were-named-top-security-threat-%E2%80%99s-better-news-it-sounds.

grid because then the United States would do the same to China.[181] The threat of a reciprocal attack is one of the greatest deterrents available.

[181] Robert Lenzner, *Chinese Cyber Attack Could Shut Down U.S. Electric Power Grid*, FORBES (Nov. 28, 2014) http://www.forbes.com/sites/robertlenzner/2014/11/28/chinese-cyber-attack-could-shut-down-u-s-electric-power-grid/.