Roger Williams University
DOCS@RWU

Law Faculty Scholarship | Law Faculty Scholarship

2018

Nation-States and Their Operations in Planting of Malware in Other Countries: Is It Legal Under International Law

John J. Chung
Roger Williams University School of Law, jchung@rwu.edu

Follow this and additional works at: https://docs.rwu.edu/law_fac_fs

Part of the International Law Commons

Recommended Citation
John J. Chung, Nation-States and Their Operations in Planting of Malware in Other Countries: Is It Legal Under International Law, 80 U. Pitt. L. Rev. 33, 68 (2018)

This Article is brought to you for free and open access by the Law Faculty Scholarship at DOCS@RWU. It has been accepted for inclusion in Law Faculty Scholarship by an authorized administrator of DOCS@RWU. For more information, please contact mwu@rwu.edu.

HEINONLINE

Citation:
John J. Chung, Nation-States and Their Operations in Planting of Malware in Other Countries: Is It Legal Under International Law, 80 U. Pitt. L. Rev. 33 (2018)
Provided by:
Roger Williams University School of Law Library

Content downloaded/printed from HeinOnline

Fri Feb 8 15:14:37 2019

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at https://heinonline.org/HOL/License

-- The search text of this PDF is generated from uncorrected OCR text.

-- To obtain permission to use this article beyond the scope of your HeinOnline license, please use:

Copyright Information

Use QR Code reader to send PDF to your smartphone or tablet device

NATION-STATES AND THEIR CYBER OPERATIONS IN PLANTING OF MALWARE IN OTHER COUNTRIES: IS IT LEGAL UNDER INTERNATIONAL LAW?

John J. Chung*

About 56 minutes into the eponymous film, the fictionalized character of Edward Snowden recounts his work as an intelligence analyst while posted to an assignment in Japan. He says the United States planted malware in Japan's power grid and other critical infrastructure systems.[1] This malware (according to the film) provides the United States with the capability to shut down the systems if there ever comes a day when Japan turns from an ally into an enemy.[2] I had never heard anything like this before, and three questions came to mind: (1) Does the United States have the technological capability to accomplish this (the undetected planting of the malware and the ability to trigger the destructive effects)? (2) Did the United States actually do this? (3) Is this legal? Since that time, my work has led me to the following conclusions. The answer to Question 1 is "yes". The answer to Question 2 ranges from "probably" to "certainly." This article deals with Question 3. If the United States did plant malware in Japan's critical infrastructure, is it legal under international law?[3]

---

* Professor, Roger Williams University School of Law; B.A., Washington University (St. Louis); J.D., Harvard Law School.

[1] SNOWDEN (Endgame Entertainment et al. 2016).

[2] *Id.*

[3] In the movie, Snowden also says that the United States planted similar types of malware with similar intent in other countries, including (but not limited to) Mexico and Austria. *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

With regard to Question 1, the United States, other nation-states, and non-state actors have the ability to cripple or shut down critical infrastructure.[4] For example, in December 2015, a cyber attack shut down the electrical power grid in western Ukraine.[5] More than 230,000 people lost power in the dead of winter.[6] This was the first confirmed cyber attack that shut down a power grid.[7] Although the identity of the cyber attackers is uncertain, Ukraine blamed Russia for the attack.[8]

It appears that the attack on the Ukrainian power grid was not intended to result in permanent damage. It may have been conducted to send a message. If that was the case, Ukraine was fortunate:

> A cyber attack on the power grid would be truly catastrophic. The industrial control, or SCADA, systems used by power plants and other utilities are increasingly connected to the Internet. Hackers could exploit this connectivity to

---

[4] The Critical Infrastructures Protection Act of 2001 defines critical infrastructure ("CI") as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195(e) (2018). The Department of Homeland Security ("DHS") adopts this definition as well. DHS has identified 16 critical infrastructure sectors. They are the (1) chemical sector, (2) commercial facilities sector, (3) communications sector, (4) critical manufacturing sector, (5) dams sector, (6) defense industrial base sector, (7) emergency services sector, (8) energy sector, (9) financial services sector, (10) food and agriculture sector, (11) government facilities sector, (12) healthcare and public health sector, (13) information technology sector, (14) nuclear reactors, materials and waste sector, (15) transportation systems sector, and (16) water and wastewater systems sector. *Critical Infrastructure Sectors*, U.S. DEP'T OF HOMELAND SEC. (July 11, 2017), https://www.dhs.gov/critical-infrastructure-sectors.

[5] Kim Zetter, *Inside the Cunning, Unprecedented Attack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[6] *Id.*

[7] *Id.* Since the attack in Ukraine, cybersecurity experts report that the ability of hackers to shut down a power grid has grown much more dangerous, and "found that the hackers obtained what they call operational access: control of the interfaces power company engineers use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses." Andy Greenberg, *Hackers Gain Direct Access to US Power Grid Controls*, WIRED (Sept. 6, 2017, 6:00 AM), https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems.

[8] *See* Zetter, *supra* note 5. Russia is also suspected of conducting a cyber attack on Estonia's critical infrastructure in 2007. The attack shut down Estonia's banking system, telephone and television networks. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1504 (2013).

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

> disrupt power generation and leave tens of millions of people in the dark for months. They could even destroy key system components like turbines.[9]

The attack on the Ukrainian power grid may have been exceptional only insofar as its effectiveness. There are reports that electric utilities are probed thousands of times each month by hackers, and that nation-states have designed plans for attacking the power grids of other countries.[10]

Perhaps the most famous cyber attack was the use of the Stuxnet virus, which damaged Iran's nuclear program.[11] In June 2009, someone introduced a destructive digital worm into the computer network controlling Iran's nuclear enrichment program.[12] Stuxnet was the "world's first real cyber weapon."[13] Unlike other worms or viruses, Stuxnet did not simply hijack targeted computers or steal information; it physically destroyed equipment controlled by the computers.[14] Stuxnet directly caused the physical destruction of hundreds of centrifuges, which are necessary

---

[9] Sales, *supra* note 8, at 1514. A report from the Congressional Research Service states:

> Attacks on *industrial control systems* can result in the destruction or disruption of the equipment they control, such as generators, pumps, and centrifuges. Most cyber attacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy and safety of individual citizens.

Eric A. Fischer, *Cybersecurity Issues and Challenges: In Brief*, CONG. RESEARCH SERV. 2 (Aug. 12, 2016), https://fas.org/sgp/crs/misc/R43831.pdf.

[10] *See* Scott J. Shackelford, Timothy L. Fort & Danuvasin Charoen, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995, 2005–06 (2016). The *New York Times* reported that North Korea wants the capability to launch a cyber attack on the U.S. power grid. *See* David E. Sanger & William J. Broad, *Trump Inherits a Secret Cyberwar Against North Korean Missiles*, N.Y. TIMES, Mar. 4, 2017, at A1.

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

[12] *Id.*

[13] *Id.*

[14] *See* Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

pieces of equipment to make weapons-grade uranium.[15] It is widely assumed that Stuxnet was developed by the United States and Israel, although that has never been publicly confirmed.[16]

With regard to Question 2, it seems highly probable that the United States, China, and Russia (and undoubtedly others) are preparing for possible war and preparing the cyber battlefield with the use of "logic bombs" and "trapdoors"—in effect, "placing virtual explosives in other countries in peacetime."[17] They have already hacked into each other's systems to plant such malware for future use, if necessary.[18] One senior national security expert believes China has planted logic bombs in the U.S. power grid, and assumes the United States has done likewise.[19] So, what can cyber war accomplish? The successful triggering of malware can control and crash networks and systems.[20] Such attacks can steal money, cause oil spills, blow up generators, derail trains, crash airplanes, detonate missiles, and on and on.[21] "If cyber warriors crash networks, wipe out data, and turn computers into doorstops, then a financial system could collapse, a supply chain could halt, a satellite could spin out of orbit into space, an airline could be grounded. These are not hypotheticals. Things like this have already happened . . . ."[22] There appears to

---

[15] *Id.* ("Centrifuges are large cylindrical tubes—connected by pipes in a configuration known as a 'cascade'—that spin at supersonic speed to separate isotopes in uranium gas for use in nuclear power plants and weapons.").

[16] *See* William J. Broad, John Markoff & David E. Sangerjan, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 16, 2011, at A1.

[17] *See* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 11 (2010). A "logic bomb" is "a software application or series of instructions that cause a system or network to shut down and/or to erase all data or software on the network." *Id.* at 287. A "trapdoor" is software maliciously added to a program to allow unauthorized entry into a network or software program at a later time without the network operator's knowledge. *Id.* at 289–90 (also sometimes referred to as a "Trojan horse"). Logic bombs and trapdoors are just two examples of what is generally known as "malware," which is malicious software that causes computers or networks to do things against the wishes of their owners. *Id.* at 287.

[18] *Id.* at 31.

[19] *Id.* at 245. In 2009, U.S. intelligence sources informed the media that Chinese hackers had penetrated the U.S. power grid and planted malware that could be used to shut down the grid. *Id.* at 59.

[20] *Id.* at 70.

[21] *Id.*

[22] *Id.* "Military and intelligence officials have repeatedly warned that malicious hackers could disrupt critical infrastructure with the click of a mouse, causing severe economic loss, persistent blackouts or even

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

be no doubt that states possess the ability to cause serious, even catastrophic, physical damage through cyber attacks.

So, it seems reasonable to conclude that states have planted malware in other countries (even allied states in addition to states recognized as threats, as claimed in the Snowden movie) in preparation for a day when it may be deemed necessary to activate the malware to cause destruction. As mentioned, experts report that China, Russia, and other countries have been planting malware in the U.S. electric grid since at least 2009.[23] The United States has reportedly engaged in similar activities.[24] The purpose of planting such malware is to "prepare the battlefield" in the event it becomes necessary for the countries to engage in war or armed conflict.[25] Every state also operates under, and feels the pressure of, structural and systemic incentives to engage in such conduct in peacetime, even without knowing if the need to activate the malware will ever arise.[26] Malware planted today takes advantage of weaknesses and vulnerabilities that may not be known to the affected party.[27] The ability to plant the malware exists because the other side is unaware of the flaws in its systems and is therefore unaware of the need to address them.[28] States seeking to capitalize on a flaw must act quickly, because once a vulnerability is discovered, the other side may fix it before it can be exploited. Thus, there is strong incentive to take advantage of the vulnerability today before it is discovered and addressed:[29]

> The shelf life of vulnerabilities thus puts pressure on countries to exploit them at present; if they wait until an outbreak of hostilities, the vulnerability might have been closed by then. This has led to a situation in which countries are actively infiltrating other countries' systems, planting logic bombs that execute malicious

---

mass casualties." Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825, 827 (2012).

[23] *See* Caroline Baylon, *Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare*, *in* ETHICS AND POLICIES FOR CYBER OPERATIONS: A NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE INITIATIVE 218 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017).

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

> functions when certain conditions are met or trapdoors that grant access to a system later.[30]

This state of facts leads to Question 3: Is it legal for nation-states to engage in this activity? Here, the answer is elusive, and the analytical framework to examine this question is undeveloped. The crux of the matter comes down to this: Is it a violation of the target state's sovereignty if another state plants malware in the target state? A follow-up and related question on this issue then arises: "Does the insertion of malware that could potentially harm critical infrastructure (and thus cause 'intangible' destruction almost equal to powerful, kinetic effects) rise to the level of an 'armed attack' or an 'act of war?'"[31] The legality or illegality of the actions described in the Snowden movie go to the heart of two foundational principles of the public international legal system: sovereignty, and the prevention of armed conflict and war.

The advances in technological capability have given rise to new challenges for international lawyers. One school of thought views the issues raised by cyber operations as a set of issues that may be integrated and incorporated into the existing systems of rules and structures of international law, while others view cyber issues as so fundamentally new and different that a whole new set of rules and structures is required.[32] This thorny issue was summarized by an observation that "the principle of sovereignty appears to be incompatible with cyberspace."[33] This is because sovereignty is "an inherently territorial concept," while cyberspace is not bound by the limits of physical geography or borders.[34] However, the two phenomena have been forced "to exist in parallel since the emergence of cyber capabilities," without an adequate reconciliation in a coherent legal framework.[35] In short, can laws and

---

[30] *Id.*

[31] CYNTHIA E. AYERS, U.S. ARMY WAR COLL., RETHINKING SOVEREIGNTY IN THE CONTEXT OF CYBERSPACE: THE CYBER SOVEREIGNTY WORKSHOP SERIES 16 (2016).

[32] Matthew Hoisington, *Regulating Cyber Operations Through International Law: In, Out or Against the Box?*, *in* ETHICS AND POLICIES FOR CYBER OPERATIONS: A NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE INITIATIVE 89 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017).

[33] Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 AJIL UNBOUND 213, 218 (2017).

[34] *Id.*

[35] *Id. See also* Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207 (2017) ("The technological structure and global interconnectedness of cyberspace offers both state and nonstate actors a medium through which to operate against a broad array of targets, free from the physical constraints of geography and territorial boundaries.").

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

legal frameworks developed for a physical world be adapted and effectively applied to address issues arising in a non-physical, cyber world?

Part I begins by presenting definitions of key words and phrases. Words like "cyberspace" and "cyber attack" are commonly used to address the kinds of issues presented in this article. However, there are no commonly accepted definitions for words or phrases like these. Commentators may have a general, shared understanding of their meaning, but each must present his or her own definitions. Even more traditional terms such as "use of force" do not enjoy a universally accepted definition. So, Part I addresses the definitional issues. Part II turns to the nature of critical infrastructure, its importance in maintaining ordered and functional societies, and its vulnerability to cyber attacks. The cyber threats to critical infrastructure are the reason why the stakes are so high in discussing the legality of these issues. Damage or destruction of critical infrastructure has the potential to be catastrophic, so if the law is to have any relevance in preserving peace and order, it is here that it must be most effective.

Part III examines the legal issue of the relationship between cyber operations and sovereignty in a general manner, and whether the planting of malware in another state violates sovereignty. The issue of sovereignty is crucial (according to one important commentator) because it defines "the normative architecture of cyberspace."[36] "Perhaps the most operationally relevant, and hence politically delicate, legal issue with respect to the cyber environment is the identification of criteria for determining when cyber operations directed against a state violate its sovereignty."[37] So, if State A plants malware (that is currently dormant and inactive) within systems located inside the territory of State B, and if that malware is capable of being activated in the near or distant future to destroy State B's critical infrastructure, has State A violated State B's sovereignty? The discussion in Part III will show that international law is unclear and undeveloped when it comes to the issue of whether the planting the malware in another state is a violation of sovereignty.

Because the prism of sovereignty does not provide a clear answer, Part IV will examine the issue of legality through the prism of Article 2(4) of the Charter of the United Nations, which provides: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of

---

[36] Schmitt & Vihul, *supra* note 33, at 213.

[37] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

the United Nations."[38] Does the planting of malware violate Article 2(4)? This can be broken down into three specific and related questions: (1) Does the planting of malware in another nation constitute a "use of force"? (2) Does it constitute a "threat" of use of force? (3) Is it an act against the "territorial integrity" of another state? The concept of "territorial integrity" is practically synonymous with the concept of "sovereignty." To that extent, there may be no material distinction between asking whether the planting of malware is a violation of sovereignty or of territorial integrity. However, because a general discussion of cyber operations and sovereignty does not yield a clear answer, the purpose of examining the issue through the use of the phrase "territorial integrity" in Article 2(4) is to conduct a more complete analysis to determine whether that approach illuminates the matter (insofar as it relates to the discussion of Article 2(4)). Not surprisingly, a particular focus on "territorial integrity" does not seem to clarify the topic or supplement a general focus on "sovereignty." It seems the most that can be said is that the legality of planting dormant malware is an unsettled issue. For this reason, Part V concludes by looking to rough analogues in other areas of international law, such as espionage, to view this issue.

I. DEFINITIONS OF KEY WORDS AND PHRASES

At this point, a summary of loose, working definitions is necessary. Many of the definitions used in this article are adopted from the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (The *Tallinn Manual 2.0*).[39] The

[38] U.N. Charter art. 2, ¶ 4. As one commentator put it, "one must look to the U.N. Charters prohibition against the use of force, or the customary international law principle of non-intervention, to assess the legality of states' actions in cyberspace." AYERS, *supra* note 31, at 84.

[39] *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0]. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia ("NATO CCD COE") gathered a group of international legal experts to produce a manual on the international law governing cyber warfare. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael Schmitt ed. 2013) [hereinafter TALLINN MANUAL]. This began a three-year project by twenty renowned international law scholars and practitioners to identify the international law applicable to cyber warfare, and their work resulted in the formulation of ninety-five "black-letter rules" governing such conflicts. *Id.* at 1. The focus of the *Tallinn Manual* was on cyber operations involving the use of force and/or occurring during armed conflict. *See* TALLINN MANUAL 2.0, *supra*, at 1. However, the NATO CCD COE recognized the need to address cyber issues that do not rise to the level of use of force. *Id.* Hence, in the same year that the *Tallinn Manual* was published, the NATO CCD COE began a follow-on initiative to expand the scope of the *Tallinn Manual* to include issues involving cyber operations in peacetime. *Id.* It convened a new group of international experts, and this group produced the TALLINN MANUAL 2.0. *Id.* The TALLINN MANUAL 2.0 supersedes

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

Tallinn Manual 2.0 defines "cyber" to "connote[ ] a relationship with information technology."[40] It defines "cyber activity" as "any activity that involves the use of cyber infrastructure or employs cyber means to affect the operation of such infrastructure. Such activities include, but are not limited to, cyber operations."[41] The manual then defines "cyber operation" as "the employment of cyber capabilities to achieve objectives in or through cyberspace."[42]

The *Tallinn Manual 2.0* also defines "cyberspace" as "the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks."[43] The Office of the U.S. President defined "cyberspace" to mean "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[44] These definitions of "cyberspace" may actually be too technical to be useful. Richard Clarke, a former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States, provides a more useful definition of "cyberspace:"

> Cyberspace is all of the computer networks in the world and everything they connect and control. It's not just the Internet. Let's be clear about the difference. The Internet is an open network of networks. From any network on the Internet, you should be able to communicate with any computer connected to any of the Internet's networks. Cyberspace includes the Internet *plus* lots of other networks of computers that are not supposed to be accessible from the Internet. Some of these private networks look just like the Internet, but they are, theoretically at least, separate. Other parts of the cyberspace are transactional networks that do things like send data about money flows, stock market trades, and credit card transactions. Some networks are control systems that just allow machines to speak to other machines, like control panels talking to pumps, elevators, and generators.
>
> What makes these networks a place where militaries can fight? In the broadest terms, cyber warriors can get into these networks and control or crash them. If

---

the *Tallinn Manual*. *Id.* at 1–2. The scholars and practitioners involved in the manuals are referred to as "the Experts" in the manuals.

[40] TALLINN MANUAL 2.0, *supra* note 39, at 564.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] Department of Homeland Security, Directive HSPD-23, Cybersecurity Policy (U.S.D.A. 2008).

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

> they take over a network, cyber warriors could steal all of its information or send out instructions that move money, spill oil, vent gas, blow up generators, derail trains, crash airplanes, send a platoon into an ambush, or cause a missile to detonate in the wrong place. If cyber warriors crash networks, wipe out data, and turn computers into doorstops, then a financial system could collapse, a supply could halt, a satellite could spin out of orbit into space, an airline could be grounded. These are not hypotheticals. Things like this have already happened, sometimes experimentally, sometimes by mistake, and sometimes as a result of cyber crime or cyber war.[45]

This description of what cyberspace actually is presents a more accessible account of what is at stake.

"Cybersecurity" will be used generally to mean (1) a "set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software and the information they contain and communicate, including software and data, as well as other elements of cyberspace"; (2) "[t]he state or quality of being protected from threats"; and (3) "[t]he broad field of endeavor aimed at implementing and improving those activities and quality."[46] This article also adopts the definition of "cyber attack" used by the U.S. military:

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems

---

[45] CLARKE & KNAKE, *supra* note 17, at 70. In terms of the distinction between "cyberspace" and the "Internet," the *Tallinn Manual 2.0* defines "Internet" as "[a] global system of interconnected computer networks that use the Internet Protocol suite and a clearly defined routing policy." TALLINN MANUAL 2.0, *supra* note 39, at 565. Internet Protocol ("IP") is defined as "[a] protocol for addressing hosts and routing datagrams (i.e., packets) from a source host to the destination host across one or more IP networks." *Id.* at 566.

[46] Fischer, *supra* note 9, at 1. There is no agreed upon meaning of the term "cybersecurity"; it serves more as a loose reference. *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U.L. REV. 287, 291 (2014). A similar working definition of cybersecurity is "the policy field concerned with managing cyber threats, including unauthorized access, disruption, and modification of electronically stored information, software, hardware, services, and networks." Scott J. Shackelford, Andrew A. Proia, Brenton Martell & Amanda N. Craig, *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 311–12 (2015).

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

> which are intended to degrade or destroy infrastructure . . . . A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from delivery.[47]

The Cybersecurity Information Sharing Act of 2015 ("CISA") also sets forth important definitions.[48] It defines "cybersecurity purpose" to mean "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[49] It also defines "cybersecurity threat" to mean:

> [A]n action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.[50]

Turning away from the cyber world, this article also addresses whether certain cyber operations constitute a "use of force." The prohibition against the "use of force" is the foundation of Article 2(4); however, the U.N. Charter does not define "use of force."[51] Rule 69 of the *Tallinn Manual 2.0* describes the "use of force" in this way: "A cyber operation constitutes a use of force when its scale and efforts are

---

[47] Memorandum from James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, Department of Defense, for the Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates (2010). So what may a cyber operation accomplish? The possibilities (which may or may not result in violent effects) include: (1) The exploitation of information available on a network. Examples would include monitoring communications, exfiltration of confidential data, stealing of passwords; (2) Passive observation of a network's topology and traffic, which may enable the exploiter to determine the important routes of traffic, the organization structure of the network, and the relative importance of those with access to the network; (3) Conducting industrial espionage; (4) Destroying data on a network or system; (5) Generating bogus or fake traffic and communications on a network, such as issuing a fake order from a superior officer to a subordinate; (6) Altering data in a database; (7) Degrading or denying service on a network. *See* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 68–70 (2010).

[48] Cybersecurity Information Sharing Act, 6 U.S.C. §§ 1501–1510 (2018).

[49] *Id.* § 1501(4).

[50] *Id.* § 1501(5)(A).

[51] TALLINN MANUAL 2.0, *supra* note 39, at 331.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

comparable to non-cyber operations rising to the level of a use of force."[52] Rule 69 will be discussed in more detail in Part IV. However, Rule 69 incorporates the phrase "use of force" while expressly acknowledging there is no "authoritative definition" of the phrase.[53] The definition of "use of force" is further complicated by the yet unsettled question of whether there is a difference between an "armed attack" and the "use of force;" the *Tallinn Manual 2.0* distinguished between the two in its discussion of the Nicaraguan Military and Paramilitary Case.[54] In the *Nicaragua* case, the court made this observation: "As regards certain particular aspects of the principle in question, it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[55] Thus, the literal meaning of this statement is that there are different forms of "use of force" ranging from "the most grave" to forms that are perhaps merely annoying or inconvenient.

It is necessary to explore the difference between use of force and armed attack because it has direct relevance (as will be discussed below) whether the planting of malware is an unlawful use of force. The *Tallinn Manual 2.0* provides a definition of "cyber attack": "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[56] The drafters adopted the widely accepted understanding

---

[52] *Id.* at 330.

[53] *Id.* at 331.

[54] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14 (June 27). There is a view held by some countries that any difference in definition is immaterial. *See* TALLINN MANUAL 2.0, *supra* note 39, at 333. However, the *Tallinn Manual 2.0* offers a substantive distinction.

> Finally, it must be understood that 'use of force' and 'armed attack' (Rule 71) are standards that serve different normative purposes. The 'use of force' standard is employed to determine whether a State has violated Article 2(4) of the UN Charter and its related customary international law prohibition. By contrast, the notion of 'armed attack' has to do with whether the target State may respond to an act with a use of force without itself violating the prohibition of using force. This distinction is critical in that the mere fact that a use of force has occurred does not alone justify a use of force in response.

Id. at 337.

[55] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 191 (June 27).

[56] TALLINN MANUAL 2.0, *supra* note 39, at 415.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

of "attack" to focus on the causation and/or existence of violence.[57] In doing so, the drafters emphasize that what constitutes an attack is determined by its consequences and effects:

> The crux of the notion lies in the effects that are caused. Restated, the consequences of an operation, not its nature, are what generally determine the scope of the term 'attack'; 'violence' must be considered in the sense of violent consequences and is not limited to violent acts. For instance, a cyber operation that alters the running of a SCADA system controlling an electrical grid and results in a fire qualifies. Since the consequences are destructive, the operation is an attack.[58]

Even with these attempts toward a workable definition, some commentators are of the view that the discussion of these issues remains complicated by the fact that terms such as "attack," "defense," "aggression," and "conflict" are not defined and are used somewhat loosely by experts in the area.[59] According to this view, it is particularly troublesome that the term "harm" is not effectively defined.[60] It raises the question as to what is meant by harm originating in or related to cyberspace, and how is it measured:[61]

> Without some understanding of the nature and scale of harm which could result from cyber conflict it cannot be possible to answer the most basic of ethical

---

[57] *Id.* ("[I]t is the use of violence against a target that distinguishes attacks from other military operations.").

[58] *Id.* at 415–16. However, not all commentators define "attack" through the criterion of consequences. Critics of this approach, at times, refer to it as an "instrumentalist" definition of attack. "Instrumentalist views are often committed to the idea that only harms to material human interests—death, injury, and serious economic damage—count as the morally relevant cyberharms." Patrick Taylor Smith, *Towards a Richer Account of Cyberharm: The Value of Self-Determination in the Context of Cyberwarfare*, *in* ETHICS AND POLICIES FOR CYBER OPERATIONS: A NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE INITIATIVE 50 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017). Smith offers a competing view, which he calls the "intrinsic" view of cyberharm. "Conversely, the intrinsic view is that the intentional disruption of computer systems, making them operate in ways contrary to their design, is intrinsically harmful to those systems regardless of those effects on human beings." *Id.* at 51.

[59] *See* Paul Cornish, *Deterrence and the Ethics of Cyber Conflict*, *in* ETHICS AND POLICIES FOR CYBER OPERATIONS: A NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE INITIATIVE 5 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017).

[60] *Id.* at 6.

[61] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

> questions to do with conflict and coercion; where is the threshold at which the harm resulting from a cyber action of some sort moves from the tolerable (e.g. inconvenience, discomfort, disruption) to the unacceptable (e.g. multiple deaths, irreversible physical damage, or even social collapse).[62]

Although there may be uncertainty in defining the precise limits of terms like "attack," "harm," and "violence," at a minimum, these concepts permit the creation of a spectrum along which cyber operations may be categorized. At one extreme, a cyber operation that results in a catastrophic malfunction at a nuclear power plant would be universally viewed as a violent attack because of the resulting harm. At the other extreme, a cyber operation that results in a temporary denial of access to entertainment websites would probably not.[63]

---

[62] *Id.*

[63] The possibility of cyber attack and cyberwar has generated its own set of issues and observations for some commentators. Such observations include:

> Cyber has its own rules / Cyberwar is only possible because systems have flaws / Operational cyberwar is unlikely to be decisive / Cyber deterrence may not work as well as nuclear deterrence / Cyber deterrence raises difficult questions: / Will we know who did it? / Can retaliators hold assets at risk? / Can they do so repeatedly? / Can cyber attacks disarm cyber attackers? / Will third parties stay out of the way? / Might retaliation send the wrong message? / Can states set thresholds for response? / Can escalation be avoided?

Paul K. Davis, *Deterrence, Influence, Cyber Attack and Cyberwar*, 47 N.Y.U. J. INT'L L. & POL. 327, 335 (2015).

An understanding of additional terms is helpful in understanding these issues. One such term is "vulnerability."

> For a computer or network, a vulnerability is an aspect of the system that can be used to compromise that system. . . . 'Compromise' is used here as a verb to mean to attack or exploit. Weaknesses may be introduced accidentally through design or implementation flaws. A defect or 'bug' may open the door for opportunistic use of that vulnerability by an adversary. Many vulnerabilities are widely publicized after discovery and may be used by anyone with moderate technical skills until a patch can be disseminated and installed. Adversaries with the time and resources may also discover unintentional defects that they protect as valuable secrets, also known as zero-day exploits. As long as those defects go unaddressed, the vulnerabilities they create may be used by adversaries. Vulnerabilities may also be introduced intentionally. Of course, vulnerabilities are of no use to an adversary unless the adversary knows they are present on the system or on the network being compromised. But an adversary may have some special way of finding vulnerabilities, and nation states in particular often have special advantages in

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

II. CRITICAL INFRASTRUCTURE AND ITS VULNERABILITY TO CYBER ATTACK

Given that cyber operations directed at critical infrastructure systems pose a threat of catastrophic damage, and given that such systems around the world may have already been infiltrated by malware, it is important to more fully understand the nature of the potential danger. Electric power grids, communications networks, air traffic control systems, maritime navigation systems, and bank payment systems are just a few examples of Critical Infrastructure ("CI"). What is overlooked, and frightening, is that most CI systems are owned by the private sector, and not protected by the government. Because everyone depends on these systems for daily activity, personal safety, health, and welfare, one would expect the government to be in charge of protecting such systemically crucial systems. For example, people do not expect the private sector to provide CI for the army or navy. But when it comes to most CI, it is provided by private entities, which are also responsible for protecting their systems:

> Most cyber attacks have limited impacts, but a successful attack on some components of [CI]—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Thus, a rare successful attack with high impact can pose a larger risk than a common successful attack with low impact.[64]

> doing so. For example, although proprietary software producers jealously protect their source codes as intellectual property upon which their businesses are dependent, some such producers are known to provide source code access to governments under certain conditions. Availability of source code for inspection increases the likelihood that the inspecting party will be able to identify vulnerabilities not known to the general public. Furthermore, through covert and nonpublic channels, nation states may even be able to persuade vendors or willing employees of those vendors to insert vulnerabilities—secret 'back doors'—into commercially available products (or require such insertion as a condition of export approval), by appealing to their patriotism or ideology, by bribing, blackmailing, or extorting them, or by applying political pressure.

Lin, *supra* note 47, at 65–66. The term "payload" is the thing or effect that can be done once a vulnerability has been exploited. *Id.* at 67. The payload is what interferes with, disrupts, or destroys the exploited system.

[64] Fischer, *supra* note 9, at 3. For example, the air traffic control system relies on Internet Protocol ("IP") networking to communicate. The operation of an aircraft depends upon systems connected to multiple networks. *See* TALLINN MANUAL 2.0, *supra* note 39, at 259. A passenger jet is vulnerable to interference with its flight control systems, and its on-board navigation and communications systems. *Id.* The potential

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

A basic challenge in cybersecurity is the fact that approximately 85% of America's CI is owned by the private sector.[65] The CI systems are owned and operated by thousands of businesses, which in turn may have thousands more private entities who either supply, service, or access the CI systems. The national cybersecurity framework relies on private actors to invest in a sufficient amount of cybersecurity measures to avoid catastrophic damage to CI. However, few private entities are required by law to implement any particular level of cybersecurity.[66] Thus, it is not surprising that many describe the state of cybersecurity defenses for CI as "inadequate."[67] The legal framework essentially leaves it to the private sector entities to set their own practices and policies for protecting their computer systems, with the government refraining from imposing security requirements.[68] Yet, the Department of Homeland Security makes clear that protection of CI from cyber attacks is a matter of national security.[69] President Obama described cybersecurity as "one of the most serious economic and national security challenges we face as a nation."[70] The reason is self-evident due to the increasingly important role of the Internet for personal, business, and government use. The Internet is inseparable from numerous CI systems, and is in itself CI.[71] In sum, "the effects of a well-coordinated,

---

exists to endanger a single aircraft or perhaps even the air traffic control system through a cyber-breach. *Id.*

[65] Sales, *supra* note 8, at 1506.

[66] One important exception applies to private firms that contract with the Department of Defense ("DoD") in certain situations. For example, the DoD has published an interim final rule, which requires contractors to comply with certain cybersecurity requirements specified by the National Institute for Standards and Technology. *See Interim Rule, Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*, U.S. SMALL BUS. ADMIN. (Feb. 29, 2016), https://www.sba.gov/advocacy/2-29-16-interim-rule-defense-federal-acquisition-supplement-network-penetration-reporting (the National Institute for Standards and Technology and its role in cybersecurity is discussed in Part II). This particular requirement has the goal of safeguarding access to the Cloud by contractors. Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services, 80 Fed. Reg. 51,739 (Aug. 26, 2015).

[67] *See* Sales, *supra* note 8, at 1506.

[68] *Id.*

[69] *Cyber Security*, DEPT. OF HOMELAND SECURITY, https://www.dhs.gov/topic/cybersecurity (last visited June 5, 2018).

[70] Remarks on Signing an Executive Order on Promoting Private Sector Cybersecurity Information Sharing, 2015 DAILY COMP. PRES. DOC. 3 (Feb. 13, 2015).

[71] *See* Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 920 (2005).

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

state-sponsored cyber attack against our financial, transportation, communications, and energy systems would be catastrophic."[72] So, is it legal for a state to plant malware in another state's CI systems, with the intent of perhaps activating it at some future point?

III. A BRIEF INTRODUCTION TO THE LEGAL RELATIONSHIPS BETWEEN CYBER OPERATIONS AND SOVEREIGNTY

When it comes to the issue of sovereignty and cyber operations, two prominent and opposing views of the issue were presented at a 2017 symposium organized by the American Society of International Law. One view is that sovereignty is a primary rule of international law; the other is that sovereignty is not a primary rule, but a fundamental principle that is part of the constitutional framework governing the law of nations. The proponents of the latter view stated:

> However, law and state practice instead indicate that sovereignty serves as a principle of international law that guides state interactions, but is not itself a binding rule that dictates results under international law. While this principle of sovereignty, including territorial sovereignty, should factor into the conduct of every cyber operation, it does not establish an absolute bar against individual or collective state cyber operations that affect cyberinfrastructure within another state, provided that the effects do not rise to the level of an unlawful use of force or an unlawful intervention.[73]

> The Internet meets all three demand-side criteria for infrastructure. The Internet infrastructure is a partially (non)rival good; it is consumed both nonrivalrously and rivalrously, depending on available capacity. The benefits of the Internet are realized at the ends. Like a road system, a lake, and basic research, the Internet is socially valuable primarily because of the productive activity it facilitates downstream. That is, end-users hooked up to the Internet infrastructure generate value and realize benefits through the applications run on their computers and through the consumption of content delivered over the Internet . . . . The Internet currently is a mixed commercial, public, and social infrastructure.

Id. at 1006.

[72] Admiral Michael G. Mullen, Chairman, Joint Chiefs of Staff, Posture Statement Before the House Comm. on Armed Serv., 112th Cong. 17 (Feb. 17, 2011).

[73] Corn & Taylor, *supra* note 35, at 208–09.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

More succinctly, Corn and Taylor state: "In short, sovereignty is a principle, not a rule, and its legal consequences are not fully formed in this area."[74] They add that international law does not prohibit states from engaging in activities "that might infringe upon or operate to the prejudice of the territorial state's internal sovereignty."[75] They frame the issue of cyber operations and sovereignty as "a question that must be resolved through the practice and *opinio juris* of states, developed over time and in response to the need of states to effectively defend themselves and provide security for their citizens."[76] This more amorphous view would, of course, allow for more legal flexibility in determining whether the planting of malware is a violation of sovereignty. Indeed, the adoption of this view seems necessary to establish and justify the legality of such practices.

The opposing view was expressed by the general editor of both the first *Tallinn Manual* and the *Tallinn Manual 2.0*. Michael Schmitt strongly asserts the view that sovereignty is a primary rule of international law, and adds, "[i]n our view, sovereignty operates to safeguard territorial integrity and inviolability; disregard for another state's territorial integrity and inviolability constitutes an internationally wrongful act."[77] In a related article, Schmitt adds, ". . . overwhelming evidence of State practice and *opinio juris*—the foundational elements of customary international law—supports the assertion that a primary rule not to violate the territorial sovereignty of other States exists."[78] Thus, Schmitt objects to attempts to introduce ambiguity into an issue governed by a primary rule. He then points to the work of nearly 40 scholars on the two *Tallinn Manuals* to support this point.[79]

The starting point on this issue in the *Tallinn Manual 2.0* is Rule 4, which provides: "A State must not conduct cyber operations that violate the sovereignty of another State."[80] This raises the question: What kind of operations "violate"

---

[74] *Id.* at 211.

[75] *Id.* at 209.

[76] *Id.* at 210–11.

[77] Schmitt & Vihul, *supra* note 33, at 214.

[78] Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639, 1650 (2017).

[79] *Id.*

[80] TALLINN MANUAL 2.0, *supra* note 39, at 17. Note 5 to Rule 4 makes clear that the principle of sovereignty includes and protects cyber infrastructure within a state's territory whether it is government infrastructure or privately owned. *Id.* at 18.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

sovereignty? To address this question, Rule 4 focuses on two factors: "(1) the degree of infringement upon the target State's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions."[81]

With regard to the first factor, Rule 4 breaks it down into three subsets: "(1) physical damage; (2) loss of functionality; and (3) infringement upon territorial integrity falling below the threshold of loss of functionality."[82] Rule 4 takes the position that cyber operations resulting in physical damage or injury violate sovereignty; similarly, causation of physical consequences by remote means also constitutes a violation of sovereignty.[83] It also takes the position that remote causation of loss of functionality in another state may constitute a violation of sovereignty, although there is no consensus as to the threshold that must be crossed to constitute a violation.[84] With regard to the second factor, Rule 4 encompasses the view that a violation of sovereignty occurs when "one State's cyber operation interferes with or usurps the inherently governmental functions of another State."[85]

For purposes of this article, however, the most important note in Rule 4 is Note 14, which confirms that a consensus does not exist on the issue addressed in this article. Note 14 states: "Third, no consensus could be achieved as to whether, and if so, when, a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty."[86] This means that the leading

---

[81] *Id.* at 20 ("The first is based on the premise that a State controls access to it sovereign territory, as described above, and the second on the sovereign right of a State to exercise within its territory, 'to the exclusion of any other State, the functions of a State.'").

[82] *Id.*

[83] *Id.*

[84] *Id.* at 20–21. However, there is "full agreement that a cyber operation necessitating repair or replacement of physical components of cyber infrastructure amounts to a violation because such consequences are akin to physical damage or injury." *Id.* at 21.

[85] *Id.* at 21.

[86] *Id.* It should be noted that Note 6 of Rule 4 of the *Tallinn Manual 2.0* states:

> In the cyber context, therefore, it is a violation of territorial sovereignty for an organ of a State, or others whose conduct may be attributed to the State, to conduct cyber operations while physically present on another State's territory against that State or entities or persons located there. For example, if an agent of one State uses a USB flash drive to introduce malware into cyber infrastructure located in another State, a violation of sovereignty has taken place.

Id. at 19. However, cyber technology does not require a physical presence or actor in the target state to introduce malware into the target state's systems. It may be accomplished remotely with no physical

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

source of guidance on cyber operations and international law appears to be silent, and unable to arrive at a view, as to whether the planting of malware (by itself, and which is dormant) violates sovereignty. Because a violation of sovereignty is conditioned on the criteria of objectively manifested consequences in the form of physical damage or loss of functionality, the question remains: What is the legality of planting malware within another state if the malware is dormant and manifests no physical consequences?

IV. DOES THE PLANTING OF MALWARE VIOLATE ARTICLE 2(4)?

Because a general discussion of sovereignty does not provide a clear answer regarding the legality of planting malware in another state, the next logical step in the analysis is to determine if it violates some other rule or principle of international law. If such practices do not constitute a violation of sovereignty, are they violations of the prohibition of the use of force given that the intent and purpose is to establish the capability, and create the potential, to cause violent, catastrophic effects? This leads to a discussion of Article 2(4) of the U.N. Charter.

A. Does the Planting of Malware Constitute a Prohibited Use of Force Under Article 2(4)?

The U.N. Charter does not set forth any criteria to illustrate what constitutes "use of force," or offer any "authoritative definition."[87] Because the Charter was drafted before the invention of the Internet, it obviously offers no guidance to the even more complicated question of what constitutes "use of force" in cyberspace. The drafters of the *Tallinn Manual 2.0* addressed the use of force in Rule 69, which provides: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[88] The drafters of the Rule placed deliberate weight on the phrase "scale and effects," which was borrowed from the opinion of the *Nicaragua*[89] judgement. Note 1 to Rule 69 provides:

---

violation of territory, and it appears to be an open question in the *Tallinn Manual 2.0* whether such conduct would constitute a violation of sovereignty.

[87] *Id.* at 330–31.

[88] *Id.* at 330.

[89] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

> In other words, 'scale and effects' is a shorthand term that captures the quantitative and qualitative factors to be analysed in determining whether a cyber operation amounts to a use of force. The Experts agreed that there is no basis for excluding cyber operations from within the scope of actions that may constitute a use of force if the scale and effects of the operation in question are comparable to those of non-cyber operations that would qualify as such.[90]

In an attempt to provide some guidance as to the meaning and nature of use of force as it pertains to cyberspace, the *Tallinn Manual 2.0* looks to parallels in the non-cyberspace world, and treats use of force in the same way use of force may occur through kinetic or non-kinetic actions in the physical world.[91] As part of this analysis, Rule 69 identifies eight non-exhaustive criteria: (a) Severity; (b) Immediacy; (c) Directness; (d) Invasiveness; (e) Measurability of effects; (f) Military character; (g) State involvement; and (h) Presumptive legality.[92]

Severity: Under the severity criterion, Rule 69 provides that at one extreme, where use of force is unquestionably present, cyber operations resulting in physical harm to individuals or property constitute a use of force, subject to a *de minimis* rule.[93] An obvious example would be a cyber attack that results in the explosive destruction of an offshore oil drilling rig or destruction of a nuclear reactor (think, for example, if Deepwater Horizon or the Fukushima nuclear reactor meltdown had been the result of cyber attack). At the other extreme, cyber operations resulting in mere inconvenience or irritation, such as a temporary shutdown of an entertainment network like Netflix, would not be sufficiently severe to qualify as "use of force." Other factors that would affect severity would include whether critical national interests were involved (such as critical infrastructure), and the scope, duration, and intensity of the consequences.[94]

---

[90] *Id.* at 331. Not surprisingly, the *Tallinn Manual 2.0* is able to provide only a broad range of possibilities that may or may not constitute "use of force" in cyberspace. Note 8 to Rule 69 provides that "some cyber actions are undeniably not uses of force, uses of force need not involve a State's direct use of armed force, and all armed attacks are uses of force. This leaves unresolved the question as to what actions short of an armed attack constitute a use of force." *Id.* at 333.

[91] *Id.*

[92] *Id.* at 333–36.

[93] *Id.* at 334.

[94] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

Immediacy: The immediacy of the manifestations of the consequences of a cyber attack is relevant and material because a cyber operation that produces immediate effects means there is little or no time for states to seek a peaceful accommodation to prevent or mitigate the effects of the operation.[95] A cyber operation may take weeks or months to achieve its effects, and if detected in time, states have the ability to engage in diplomatic or other non-military means to resolve the threats.[96] Thus, even if a cyber operation's consequences are potentially catastrophic, if the effects are not immediate, there is time for states to prevent the operation from turning into an event that causes loss of life or property damage, at which point it would clearly constitute a use of force.

Directness: In contrast to immediacy, which focuses on the temporal pace and succession of events in a cyber operation, directness focuses on the chain of causation.[97] Drawing from a parallel in kinetic warfare, Note 9 points to the example of an explosion (say, from a missile).[98] The explosion directly harms people and property. Not only is the effect immediate, but the cause and effect are also direct. A hypothetical counter-example might be a cyber operation directed by one state at the strength of another state's national economy. A state could engage in misinformation disseminated through cyberspace about the economic strength or weakness of another country, and even produce glitches in the sales of a nation's government bonds through cyber operations to hinder a country's ability to borrow in global capital markets. Such activities might lead to higher borrowing costs for a country, which then, in turn, might slow down economic activity, resulting in higher unemployment, and potential harmful effects on those who lose their jobs. Even if it were possible to piece together this cause and effect relationship, it is highly unlikely that the international community would view this as an unlawful use of force because the relationship between the initial cause and the eventual effects are too indirect.

Invasiveness: This factor focuses on the degree of a security breach or intrusion into a highly secured system, specifically, the degree to which the breach or intrusion is directly contrary to the interests of the target state.[99] For example, the invasiveness factor is probably not violated by a cyber intrusion into an openly accessible system

---

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

of a country's public university.[100] On the other extreme, a cyber intrusion into highly secure systems of the Pentagon or the Central Intelligence Agency would undoubtedly violate the invasiveness factor.

Measurability of effects: A cyber operation is more likely to fall into the category of use of force if its effects are apparent, identifiable, and quantifiable. Rule 69, again, borrows from examples from kinetic warfare. Traditional uses of force, such as an attack by military aircraft, give rise to numerous ways to assess the success of the mission. There is satellite and video evidence, and the preparation of battle damage assessments based on objective and quantifiable facts.[101] In cyberspace, the ability to quantify and identify the consequences of a cyber operation enables a state to determine if the operation has risen to the level of a use of force. Therefore, a cyber operation that can be measured in terms of damage such as "amount of data corrupted, percentage of servers disabled, number of confidential files exfiltrated" is more likely to fall within the category of a use of force.[102]

Military character: This factor speaks for itself because if a cyber operation is originated by a state's military forces, it is obviously more likely to fall into the category of use of force. This factor is also based upon and reinforces the U.N. Charter's main concern with military actions.[103]

State involvement: This factor focuses on the nexus between direct involvement by the state and the cyber operation in question. Operations conducted by the state itself (through its military or intelligence services) are more likely to fall into the category of use of force.[104] This factor can quickly become a complicated knot of issues because cyber operations can be conducted by individuals or organizations with varying degrees of connection to a state, and varying degrees of accountability or control by a state. The individuals or organizations may, in fact, have no connection to a state, may not be acting at the request or instruction of a state, and may simply be taking an action to further a self-adopted patriotic or national agenda. A state may also guide or instruct non-state actors over whom it has

---

[100] *Id.* Any discussion of Invasiveness must, however, acknowledge the openly accepted practice of espionage. Every technologically capable country has penetrated, or is attempting to penetrate, highly secured systems of other countries to gain unauthorized access to information. However, international law does not place espionage into the category of unlawful use of force. *Id.*

[101] *Id.* at 335.

[102] *Id.*

[103] *Id.* at 336.

[104] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

influence to maintain operational distance and deniability in the event the hackers are identified. Obviously, though, the clearer and closer the connection between a state and the cyber operation, the more likely that it may rise to the level of state use of force.[105]

Presumptive legality: As a general matter of international law, acts that are not forbidden are permitted.[106] Therefore, so long as a cyber operation does not fall within an express prohibition such as the U.N. Charter, treaty, or customary international law principles, it is presumptively legal.[107] This is perhaps just another way of returning to the original question posed by this article: Is the planting of malware in another state's critical infrastructure prohibited under international law?

The *Tallinn Manual 2.0* addresses this question but manages to avoid answering it. The issue of planting malware is addressed in at least two different Rules. In Note 16 under Rule 92, the *Tallinn Manual 2.0* observes:

> By analogy, the introduction of malware or production-level defects that are either time-delayed or activate on the occurrence of a particular event is an attack when the intended consequences meet the requisite threshold of harm. For the majority, this is so irrespective of whether they are activated. Some members, however, took the position that although there is no requirement that the cyber operation be successful, an attack only transpires once the malware is activated or the specified act occurs.[108]

This issue is addressed again under Rule 97.[109] Note 9 of Rule 97 provides:

> A particularly important issue in the cyber context is that of 'delayed effects.' An example is emplacement of a logic bomb designed to activate at some future point. Activation may occur upon lapse of a predetermined period, on command, or upon

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.* at 419.

[109] Rule 97 provides: "Civilians enjoy protection against attack unless and for such time as they directly participate in hostilities." *Id.* at 428.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

> the performance of a particular action by the target system (e.g., activation of the fire control radar of a surface-to-air missile site).[110]

In both discussions of the planting of malware, the attack occurs when the consequences or effects become manifest (i.e., when something explodes, or someone is killed). However, the *Tallinn Manual 2.0* appears to be silent on the legality of at least two issues: (1) Is the emplacement of the malware, by itself, illegal? (2) What is the legality of the situation in the period between the time the malware is planted and the time when the malware is activated (the period of dormancy or latency)? Is it illegal if the malware is never activated?

Some guidance may also exist in the International Court of Justice's ("I.C.J.") advisory opinion regarding the threat or use of nuclear weapons. The use of cyber weapons resulting in violent consequences would constitute a use of force or armed attack. However, the development, existence, and perhaps even use of cyber weapons in the absence of such consequences appears to be legal under international law. This is the logical conclusion from a reading of the I.C.J.'s advisory opinion: "These provisions [in the Charter] do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons."[111] It follows that if nuclear weapons are neither prohibited nor permitted under the U.N. Charter, then the same applies to cyber weapons.

B. Does Placement of Malware Constitute a Prohibited Threat of Use of Force Under Article 2(4)?

So far, it seems that the law may be interpreted to mean that the placement of malware does not constitute a use of force unless and until violent consequences and effects occur. This leaves open the question of the legality of the placement and presence of the malware while it is dormant, not manifesting any consequences or effects (grave or otherwise). Security and military experts around the world openly acknowledge that most, if not all, technologically capable states have planted malware in the CI of potential adversaries for possible future use.

The planting of malware is obviously a cyber operation directed against another state. However, not all such cyber operations constitute attacks or use of force. These

---

[110] *Id.* at 431.

[111] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8).

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

terms do not encompass or include cyber espionage.[112] Rule 32 provides: "Although peacetime cyber espionage by States does not *per se* violate international law, the method by which it is carried out might do so."[113] Espionage is widely practiced, has always been widely practiced, and customary international law does not attempt to prohibit it.[114] To be sure, the essence of espionage is secret and clandestine activity.[115] It is meant to be undetected. The reason for these obvious observations is that these are also the essential characteristics of a successful cyber operation to plant malware for future use. The entire point is for the malware to be planted secretly and remain undetected. In this way, there is a common feature between espionage and the cyber operations discussed in this article.

Given that the purpose of planting malware is to engage in secret, undetected activity, such activity does not seem to violate the Article 2(4) prohibition on the "threat" of use of force. The commonly accepted legal definition of "threat" is "a communicated intent to inflict harm or loss on another or on another's property, esp. one that might diminish a person's freedom to act voluntarily or with lawful consent . . ."[116] In other words, a threat is something that is communicated. Acting in a way to avoid detection is the opposite of the nature of a threat. For this plain reason, the planting of malware does not appear to violate Article 2(4)'s prohibition on threats of use of force.

---

[112] *See* TALLINN MANUAL 2.0, *supra* note 39, at 418.

[113] *Id.* at 168. Rule 32 defines "cyber espionage" as: "[A]ny act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather, or attempt to gather information. Cyber espionage involves, but is not limited to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information." *Id.*

[114] *Id.* at 169. *See also* Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321 (1996) (intelligence activities are now accepted as a common, even inherent, attribute of the modern state); Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Cover Action*, 79 GEO. WASH. L. REV. 1162, 1175 (2011) (international law does not condone or proscribe espionage).

[115] *See* Demarest, *supra* note 114, at 325, 347.

[116] *Threat*, BLACK'S LAW DICTIONARY (9th ed. 2009). In *Virginia v. Black*, 538 U.S. 343 (2003), the Supreme Court described "true threats" as "those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence . . . ." *Id.* at 359.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

C. *Does Planting of Malware Constitute a Violation of the Territorial Integrity of the Target State in Violation of Article 2(4)?*

This final issue in the analysis of Article 2(4) is probably also the thorniest (similar to the discussion of sovereignty). The activity at issue involves the emplacement of malware within the critical infrastructure systems located within the borders of the target state. By any definition, this would seem to constitute an unauthorized intrusion or violation of the target state's territory. However, the precise issue is whether such conduct amounts to a violation of territorial integrity *for purposes of Article 2(4)*. The concept of territorial integrity is as old as the concept of the sovereign state and is one of the rights inherent in sovereignty and independence.[117] The essence of what it means to be a state is inseparably connected to the concept of territory. The definition of state requires four essential elements: (a) *a defined territory*; (b) a permanent population; (c) a government, and (d) a capacity to conduct international relations:[118]

> The concept of territorial sovereignty is concerned with the nature of the authority exercised by the State over its territory. The ideas of territory and sovereignty are closely linked in international law, since the concept of territory itself is concerned

---

[117] Michael Wood, *Territorial Integrity*, ENCYCLOPEDIA PRINCETONIENSIS, https://pesd.princeton.edu/?q=node/271 (last visited May 24, 2018).

[118] MARK W. JANIS, AN INTRODUCTION TO INTERNATIONAL LAW 185 (4th ed. 2003). Another commentator adds:

> Territorial integrity and political independence are two core elements of Statehood. Territorial integrity refers to the territorial 'oneness' or 'wholeness' of the State. As a norm of international law it protects the territorial framework of the independent State and is an essential foundation of the sovereignty of States. It extends principally over land territory, the territorial sea appurtenant to the land, and the seabed and subsoil of the territorial sea. Political independence refers to the autonomy in the affairs of the State with respect to its institutions, freedom of political decisions, policy making, and in matters pertaining to its domestic and foreign affairs. The two concepts of territorial integrity and political independence are thus linked as the foundation of the sovereign State. They provide the basis for the external affirmation by the international community of the sovereignty of a State and the legitimacy of the occupation and use of its territory free from outside external interference or threat, and the right of the State to make decisions affecting its territory.

Samuel K.N. Blay, *Territorial Integrity and Political Independence*, OXFORD PUB. INT'L L., http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1116 (last updated Mar. 2010).

> with those geographical areas over which sovereignty or sovereign rights may be exercised. Territorial sovereignty is, therefore, centred upon the rights and powers coincident upon territory in the geographical sense. As such it has provided the basis for modern international law.[119]

Many, perhaps all states would view the planting of potentially destructive malware within their borders as a violation of the right to exercise exclusive power within its territory. It seems axiomatic that states exercise sovereign control over cyber infrastructure and operations within their territory.[120]

The crucial issue is, however, whether the creation of cyberspace requires reconsideration of the concept of territoriality and what it means to violate territoriality. In prescient observations from more than 30 years ago, Shaw saw that new technological developments were minimizing the importance of the concept of territory:[121]

> As far as security is concerned, modern developments have shown that the mere possession of territory cannot of itself guarantee the protection of its inhabitants. The era of aviation, missiles, and various devices of mass destruction has meant that no State can provide absolute security for its people. Therefore, States have sought to establish their security by other means, such as mutual deterrence, international agreements, international organizations, and so on. Boundaries as the

---

[119] MALCOLM SHAW, TITLE TO TERRITORY IN AFRICA 11 (1986). Shaw also observed:

> Territory is, of course, itself a geographical conception relating to physical areas of the globe, but its centrality in law and international law in particular derives from the fact that it constitutes the tangible framework for the manifestation of power by the accepted authorities of the State in question. The principle whereby such a State is deemed to exercise exclusive power over its territory can be seen as a fundamental axiom of classical international law. More than this, Hill declares that 'international relations in their more vital aspects revolve about the possession of territory.' This crucial role, thus played by territory and its attendant legal concepts, has been evident in all stages of the development of international law and changes in the nature and structure of international law cannot but be expressed in the light of this fact.

Id. at 1. This captures the widely accepted understanding of territoriality and sovereignty. The Russian Military Encyclopedia "defines sovereignty as the supremacy of governmental authority within a country . . . ." AYERS, *supra* note 31, at 46.

[120] *See* Lotrionte, *supra* note 22, at 829.

[121] *See* SHAW, *supra* note 119, at 4.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

> geographical barriers protecting the inhabitants of a territory now play a much more humble role. Modern technology has also meant that the function of territory as a means of excluding the activities of other entities has been much diminished.[122]

Shaw made this observation when the Internet and cyberspace, as we know it, did not exist. Yet, even the state of technology in the 1980's caused him to observe a decline in the ability to enforce protective boundaries.[123] More recent observers have echoed this theme. The concepts of cyber attack and cyberwar are difficult to reconcile and frame within the traditional contextual boundaries of "territorial integrity" and "political independence."[124]

The borderless nature of cyberspace and the basic foundation of territoriality in international law gives rise to an uneasy co-existence. The structure of the Internet is globalized, and the basis of sovereignty is territorial.[125] Can these concepts be reconciled in the existing legal framework? The issue is currently under consideration at the highest levels of the world's militaries: "[T]here is uncertainty among experts, both within the United States and internationally, over the exact meaning of sovereignty in international law and its applicability in cyberspace—

---

[122] *Id.* at 3–4.

[123] Shaw also raised questions relating to the foundation of international law established by Westphalia. "These factors have led a number of writers to postulate the decline of the Westphalian system of international law based fundamentally on sovereign territorial states." *Id.* at 4. This concern over Westphalian principles goes to the heart of the foundational structure of international law.

> Indeed, contemporary international law gives each state a right to be free, independent, and uninhibited from foreign control and forcible coercion. Sovereignty, a fundamental principle of international law since the Treaty of Westphalia of 1648, holds that each state retains exclusive authority over activities within its borders. The principle of state sovereignty over national territory is a basic tenet of international law, universally accepted as customary international law. This customary rule of territorial sovereignty is codified in modern international law. Any limitation on the authority a state has over its territory is subject to the consent of the state.

Lotrionte, *supra* note 22, at 851. "The notion of territorial integrity is fundamental to the Westphalian State system, and underlies the contemporary rules of international law on the use of force, as embodied in the Charter of the United Nations and customary international law." Wood, *supra* note 117.

[124] Hoisington, *supra* note 32, at 91.

[125] *See* AYERS, *supra* note 31, at 72.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

specifically whether the unauthorized access of computers or networks located in another country violates territorial sovereignty and/or international law."[126]

There are at least three competing views on this issue. One takes a strict view of sovereignty, and adopts a principle based on an international rule of trespass, meaning that any non-consensual entrance into the territory of another state is a violation of international law.[127] Under this view, the planting the malware in another state would be a clear violation.[128] Another view acknowledges the importance of territorial sovereignty as a foundational principle, but "not a rule in and of itself."[129] The proponents of this view assert that "one must look to the U.N. Charters prohibition against the use of force, or the customary international law principle of non-intervention, to assess the legality of states' actions in cyberspace."[130] There is a third, more nuanced view, and the nuance is there by design (when considering the source). While some argue that "hacking" to access a computer network is hostile in and of itself, in 2012 the Chairman of the Joint Chiefs of Staff, General Martin Dempsey, stated that hacking was not automatically hostile, but that hacks on critical infrastructure could be.[131]

---

[126] *Id.* at 83.

[127] *Id.* at 84.

[128] This strict view seems to be consistent with the following observation:

> Although information contained in the cyber realm may be located in a 'cloud' and the full stream of information flow may not travel through national territory per se, the physical aspects of cyberspace, such as computers, servers, phones, and fiber optic cables, are owned by a state or by private companies that operate in accordance with a state's laws, and such assets are located within the borders of a governed state territory. The fact that a state's physical cyber assets located in its territory are connected to the global Internet does not waive a state's territorial sovereignty over those cyber assets and the activities involving them. The principle of sovereignty extends to the state's authority over these assets, providing the state the right to restrict or protect access to the Internet. States maintain sovereignty over cyber assets within the state's territory, and therefore these cyber assets are subject to the state's legal and regulatory control and are protected by the state's territorial sovereignty.

Lotrionte, *supra* note 22, at 852.

[129] AYERS, *supra* note 31, at 84.

[130] *Id.* at 84.

[131] *See* Jack McDonald, *Blind Justice? The Role of Distinction in Electronic Attacks*, *in* ETHICS AND POLICIES FOR CYBER OPERATIONS: A NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE INITIATIVE 19 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017).

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

The view expressed by General Dempsey makes perfect sense. Why would any technologically advanced nation (whether it is the United States, Russia or China) adopt a view that its capabilities and undetected activities are automatically hostile or illegal? And any nation would reserve the right to view a cyber operation against its critical infrastructure as potentially hostile. These would be the views of any rational state actor:[132]

> For cyberspace specifically, major nations want stability, but they also want to use cyber attacks for intelligence and actions in crisis or conflict. If crisis occurs, they want to avoid unintended escalation—but to be better able to escalate than others. And, whatever the rules of the road, they want to be as effective as possible in cyberspace.[133]

The existence of at least three views on the issue return the matter to one of the issues raised earlier in this article. Can the set of issues raised by cyber operations be integrated and incorporated into the existing systems of rules and structures of international law, or are the issues and technology so fundamentally new and different a whole new set of rules and structures is required?[134]

---

[132] Parallels to the current state of cyberpower have been made to historic and contemporary naval power.

> As major naval powers have claimed wider powers in war at sea, similar latitude will likely be claimed (or exercised) by those states that are most active in the new field of cyber conflict. The most serious challenges will arise from states that can sustain heavy investments to develop and deploy the most advanced means of attack. Probably fewer than a dozen states have the financial resources, the requisite base of technical capacity, and the military commitment to compete in this field. We should not expect agreement among these powers on limiting their capacities, especially if they must negotiate such limits with vast numbers of bystanders, as has now become the accepted practice regarding treaties on the law of armed conflict.

Jeremy Rabkin & Ariel Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea*, 14 CHI. J. INT'L L. 197, 210 (2013).

[133] Davis, *supra* note 63, at 330.

[134] The issue of territorial sovereignty was much more important as a matter of national security and defense when it developed out of the Westphalian principles of 1648, and remained important for centuries. Until the rise of modern technology, territorial space was a key basis of national security. An adversary needed to physically advance into, or disrupt, territory to harm a state. Advancing into another state's territory required time, resources and logistics. With cyber operations, physical intrusion is rendered unnecessary, along with all the supporting features necessary to support physical intrusion. Even outside of the cyber world, the concept of territoriality as a key to national defense seems to be diminishing in importance. For example, in March 2018, Vladimir Putin announced to the world that Russia possesses

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

V. CONCLUSION: IS THE PLANTING OF MALWARE IN OTHER STATES LEGAL?

So this leads back to the original question: Is the planting of malware legal?[135] The analysis of this question assumes two facts (which may or may not be accurate): (1) All states with the capability engage in this activity,[136] and (2) no state has engaged in this activity to the point where it has risen to the level of use of force.[137] Assuming these facts, international legal support for such activities may be found in two principles: (1) that which is not expressly prohibited is permitted; and (2) there may be an absence of *opinio juris* to support the view that such activities are illegal.[138] The argument on the second point would be that if states engage in such activities, there is no sense of a legal obligation to refrain from such activities.[139]

---

an intercontinental missile capable of reaching a speed 20 times the speed of sound. *See* Alastair Jamieson, *Putin Unveils New Russian Nuclear Missile, Says it Renders Defenses Useless,'* NBC NEWS (Mar. 1, 2018), https://www.nbcnews.com/news/world/vladimir-putin-set-state-union-speech-election-looms-n852211. Like cyber weapons, hypersonic missiles would reduce the importance of time and distance as defenses.

[135] One side issue is what prevents nations from engaging in cyber attacks through the use of undetected malware. The simple answer is deterrence. If one technologically advanced state engaged in a cyber attack on another advanced state, the target state would respond in kind. *See generally* Davis, *supra* note 63, at 336–37.

[136] Cyber attacks are already pervasive, commonly in use for spying, harassment, theft, and intimidation, but remaining below the level of "armed attack." *See* Rabkin & Rabkin, *supra* note 132, at 255.

[137] This assumption is complicated by the events surrounding Stuxnet. Stuxnet caused significant physical damage within Iran, and it is widely assumed that the United States and Israel developed and employed Stuxnet. However, neither country has ever admitted its role involving Stuxnet, and the international community is unwilling or unable to squarely place liability for Stuxnet on either state. In my own discussions with leading experts on matters of cybersecurity, every one of the experts began his discussion of Stuxnet with the phrase "assuming the United States and Israel were responsible," and at least one of the experts (whom I met in Geneva) had no reason to take a sympathetic view of U.S. actions.

[138] The widely accepted understanding of opinio juris is that for a principle to become customary international law, the principle must reflect consistent state practice, and that states must engage in such practice out of a sense of a legal obligation (opinio juris). *See* JANIS, *supra* note 118, at 46–47.

[139] Several commentators urge the issue of cyber operations to be taken out of the realm of customary international law or unaddressed legal prohibitions, and be placed into the realm of formal agreements.

> At the extreme, a cyber attack might produce catastrophic effects. A determined enemy might, for example, devise a cyber offensive which disabled the electric power grid of a target state for an extended period. In a full-scale conflict, a blow of that kind might have strategic effect, but also cause vast suffering. Without rail service or reliable refrigeration, portions of the civilian population might be exposed to extreme food shortages, even to

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

Perhaps this leaves the legality of planting malware in the same murky area of legality as espionage. The Experts who wrote the *Tallinn Manual 2.0* acknowledged that espionage is not prohibited by customary international law.[140] Instead, it seems to lack a clear legal justification, even though all states engage in it.[141] However, Professor Schmitt made an interesting observation in response to those who attempt to justify the legality of cyber operations through comparisons to espionage:

> For espionage conducted on another state's territory to be lawful, it would have to constitute a customary exception to the general principle of territorial integrity and inviolability. While extensive state practice offers support for this proposition, the lack of *opinio juris* cuts the other way. As Quincy Wright opined in 1962, the 'frequent practice has not established a rule of law because the practice is accompanied not by a sense of right buy by a sense of wrong.' Indeed, if contrary state practice alone sufficed in the abstract to undercut a customary norm, both the prohibitions on intervention and the use of force would be at risk.[142]

In other words, states engage in espionage not out of a sense of legal obligation, but with the understanding that they are engaged in legally dubious activity. This is especially true given that each state criminalizes espionage when it is the target. The same can probably be said of the practice of planting dormant malware in another state's CI. States engage in the practice of espionage knowing that its legality is dubious, and criminalize it when they are the target.

> the spread of epidemic diseases. A long line of commentators has, accordingly, warned that cyber weapons might prove so devastating to civilians that their use should be constrained by formal international agreements. Other commentators have argued that with all their potential for catastrophic harm to civilians, cyber attacks would not likely secure decisive results in military terms. No first strike could hope to knock out the target state's capacity to retaliate, even in the cyber realm. Nor could the state that absorbed an initial cyber attack strike hope to eliminate the attacker's capacity to launch further cyber strikes. Some analysts conclude, therefore, that the most sensible course would be to head off a costly and futile arms race in cyberspace by negotiating formal agreements never to deploy cyber attacks for military purposes.

Rabkin & Rabkin, *supra* note 132, at 252–53.

[140] *See* TALLINN MANUAL 2.0, *supra* note 39, at 169.

[141] *See* Raphael Bitton, *The Legitimacy of Spying Among Nations*, 29 AM. U. INT'L L. REV. 1009, 1010 (2014).

[142] Schmitt & Vihul, *supra* note 33, at 217.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

At the same time, it is impossible to ignore the reality of state practice and international relations. Powerful states with the ability to engage in the conduct will not abandon the practice simply because some commentators object to it, and such states will not make an admission that their conduct is unlawful (assuming they acknowledge that they engage in the practice in the first place). Again, as Professor Schmitt observed:

> Of course, we are sensitive to the fact that states generally act pragmatically in their international relations. Most have an interest in engaging in espionage, although conversely they do not tolerate espionage on their own territory, as evidenced by its universal criminalization in domestic law. The situation is inherently paradoxical—states proscribe the very conduct in which their own agents engage. It is accordingly rational that international law does not prohibit espionage per se, since it is so prevalent, but rather only certain methods by which it is conducted.[143]

So, perhaps this is the current status of the law when it comes to cyber operations to plant malware in the CI of other states. It is highly likely (if not certain) that states with the technological ability to engage in malware operations do engage in them. Such states are able to argue with principled support that such practices are not explicitly proscribed. Perhaps ironically, it would also not make sense for any state that engages in them to openly advocate legality because then it would draw attention to a practice that is, by design, meant to be unknown and undetected. At the same time, it would be irrational for such states to advocate that such practices should be illegal.

The only states that would rationally express open objection to the practice would be states that are not as technologically adept as the states that can engage in such practices at the most advanced levels. However, that lack of technological power would also be an indication of a lack of power to influence customary international law, change state practice, or influence *opinio juris*. It would also indicate a lack of power and influence to advocate for and advance efforts to achieve written international agreement on the matter. Under these circumstances, the legal uncertainty and murkiness may remain the prevailing situation for the foreseeable future, and it seems highly unlikely that such practices will become explicitly unlawful under international law (pending unforeseen changes in circumstances and technology). To return to Professor Schmitt again, he concluded an article with this warning:

---

[143] *Id.* at 218.

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu

> Lastly, we must be realistic. States, whether they are allies of the United States or not, whether they know of the purported U.S. counterterrorist operations occurring on cyber infrastructure located on their territory or not, and whether they are cyber capable or not, are unlikely to tolerate foreign cyber operations on their territory. Given U.S. technological supremacy and the fact that territorial states are often oblivious to effects manifesting on their cyber infrastructure, it may seem sensible to refuse to acknowledge the normative firewall that sovereignty represents. But in the long term, this approach is bound to backfire, with political damage potentially outweighing what can be gained from such cyber operations. Advocates of the approach will inevitably learn that sovereignty-violating cyber operations can only be pursued as a measure of last resort and with full knowledge of the likely reactions.[144]

Despite this warning, if the reports of malware planted by China on America's power grid and *vice versa* are accurate, and if the allegations in the Snowden film are also accurate, one wonders whether actual state practice has already gone far beyond what such warnings are trying to prevent.

[144] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) • DOI 10.5195/lawreview.2018.593
http://lawreview.law.pitt.edu