2020

Attribution and Other Conditions of Lawful Countermeasures to Cyber Misconduct

Mary Ellen O'Connell
Notre Dame Law School, maryellenoconnell@nd.edu

ATTRIBUTION AND OTHER CONDITIONS OF LAWFUL COUNTERMEASURES TO CYBER MISCONDUCT

MARY ELLEN O'CONNELL*

INTRODUCTION

Malicious cyber conduct sponsored by governments is on the increase, as well-documented cases involving China, Estonia, Georgia, Iran, Israel, North Korea, Russia, Saudi Arabia, and the United States indicate. Iran and the United States are expected to pursue their conflict in cyberspace following missile attacks on each other in Iraq in early January 2020. States are pouring extraordinary resources into the capacity to carry out cyberattacks and other actions aimed at harming adversaries. The 2018 United States *National Cyber Security Strategy* seeks to justify the United States' share of expenditures, saying the goal is "to use cyber capabilities to achieve national security objectives."[1] The U.S. will impose "costs through cyber and non-cyber means."[2] In other words, U.S. government officials believe that introducing malware to computer systems, hacking into databases, accessing email and other forms of communication, and programming traps to ensnare trespassers will enhance a state's cyber security and national security in general. This is a highly contentious assumption on which to base massive commitments of resources. However, the question here is not whether intentional cyber misconduct can achieve security. The question is whether such practices are lawful.

The relevant answer to the question is international law.[3] Cyber space is quintessentially supra-national. That said, lawful responses to cyber wrongdoing rest on a principle found in all law, not just international law. The principle of legality mandates that enforcement of the law must comply with the law. While this principle should be obvious, it apparently no longer is. Various ideologies

---

* Robert & Marion Short Professor of Law, Notre Dame Law School, and Research Professor of International Dispute Resolution, Kroc Institute for International Peace Studies, University of Notre Dame.

[1] THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 3 (Sept. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[2] *Id.*

[3] *See generally* Mary Ellen O'Connell, *Cyber Security Without Cyber War*, 17 J. OF CONFLICT & SECURITY L. 187 (2012).

challenge respect for the rule of law today.[4] This article will engage only one: the view that no law governs cyber space, that it is a law-free zone.[5] No aspect of human society is a law-free zone. The sovereign state responding to violations of its rights, for example, is bound by the law of state responsibility. Action to enforce legal rights must target the agent legally responsible for the law violation.[6] The accused party must have public notice and a chance to answer the accusation in all but rare cases involving emergency situations of self-defense to armed attack. In the case of armed attack, the facts should be plain. Upon failure to comply with the law, the victim state may use coercive measures that are necessary and proportionate to the wrong. Necessity means coercion is a last resort and is likely to succeed in the circumstances.[7]

Plenty of examples exist of revenge attacks and collective punishment in the name of deterrence. Such actions are in themselves law violations. Lawful responses, by contrast, start with the threshold requirement of determining whether a wrong has occurred. If so, the response must be against the responsible party, and it must be necessary and proportional to the wrong. In the case of cyber wrongs, the detailed rules on attribution and lawful, coercive responses are to be found in the international law of responsibility.[8] Carrying out lawful cyber countermeasures to malicious cyber conduct is challenging given that perpetrators use sophisticated means to hide their identities. Accusations are often based on indirect evidence or inferences that are well below the international legal standard of clear and convincing.[9] For this reason, the great effort involved in creating and deploying offensive cyber measures is largely wasted by governments concerned with law compliance. Defensive strategies are the far better investment.

These conclusions are reached by first examining the cyber attribution issue in the context of today's malicious cyber conduct. The discussion will move on to the international law of attribution and other principles of responsibility. This

---

[4] Consider, for example, the ideology of realism, adhered to by the foreign policy establishment of most NATO member countries. Realism embraces an antipathy for law, preferring the strong man leader with unfettered power to use military force. REBECCA SANDERS, PLAUSIBLE LEGALITY: LEGAL CULTURE AND POLITICAL IMPERATIVE IN THE GLOBAL WAR ON TERROR 20–21 (Oxford University Press ed. 2018).

[5] *Id.*

[6] The International Law Commission has set out in detail when action is attributable to a state in its work known as the Draft Articles on State Responsibility, an effort accepted by the UN General Assembly in 2001 in lieu of proceeding toward a multilateral treaty. Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session: Draft Articles on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/10, at ¶ 76 (2001) [hereinafter Articles on State Responsibility]. The Articles on State Responsibility say little about why attribution must be made perhaps because the point is so widely accepted as basic fairness and common sense, concepts most people understand instinctually. For more on general principles, see generally BIN CHENG, GENERAL PRINCIPLES OF LAW: AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS *in* THE LIBRARY OF WORLD AFFAIRS 21 (George W. Keeton & Georg Schwarzenberger eds. 1953).

[7] *See infra*.

[8] The United Nations International Law Commission has drafted two sets of articles restating the general principles of responsibility applicable to states and international organizations respectively. International law principles of responsibility applicable to individuals (natural and juridical) are found in various sets of rules, including human rights, international criminal law, and international economic law treaties. *See* Int'l Law Comm'n, Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/10, at ¶ 76 (2001); Int'l Law Comm'n, Draft Articles on Responsibility of International Organizations, U.N. Doc A/66/10, at ¶ 87 (2011). This article will focus on state responsibility.

[9] *See infra* on standards of evidence in international law.

second Part will also set out the international legal standard of clear and convincing evidence for satisfying the conditions involved in lawful cyber countermeasures. This Part will underscore that while cyber offense is rarely lawful, cyber defense always is.

I. CYBER HACKS, ATTACKS, AND TRAPS

This Part looks at cases of cyber misconduct linked to governments. The cases provide an overview of the type of malicious cyber conduct that is prevalent in the world today. The law regulating such misconduct is discussed in the next Part.

On June 20, 2019, Iran used a missile to shoot down a United States Navy drone conducting, according to the U.S., intelligence gathering from outside Iran's borders. In response, the United States threatened to attack inside Iran using manned aircraft. President Trump tweeted that he called off the attack with ten minutes to spare because it risked killing an estimated 150 people. He deemed that such an attack would be disproportionate in response to the destruction of an unmanned drone. Instead, "U.S. Cyber Command conducted a cyber operation against Iranian missile and rocket command and control systems in response to the drone attack . . . ."[10] Later media reports indicated that U.S. cyberattacks wiped out Iranian databases and disrupted communications by an Iranian military unit concerned with maritime matters in the Persian Gulf.[11] The reports, based on information from "unnamed officials," indicated that the U.S. intended to avoid interference with Iranian missiles or rockets owing to the risk of escalation.[12] As with their earlier use of the Stuxnet computer worm against Iran during the Obama administration, U.S. officials apparently want adversaries and allies alike to know the U.S. has caused computer damage, while at the same time attempting some plausible deniability of actions that are in themselves unlawful.[13]

Some commentators criticized the attacks not because they were unlawful but because Iran and other adversaries learned of their systems' vulnerabilities and how U.S. hackers were able to exploit them. Once security weaknesses are

---

[10] Michael Schmitt, *Top Expert Backgrounder: Aborted U.S. Strike, Cyber Operation Against Iran and International Law*, JUST SECURITY (June 24, 2019), https://www.justsecurity.org/64669/top-expert-backgrounder-on-aborted-u-s-strike-and-cyber-operation-against-iran-and-international-law/.

[11] *See generally* Julian E. Barnes, *U.S. Cyberattacks Hurt Iran's Ability to Target Oil Tankers*, N.Y. TIMES (Aug. 28, 2019), https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html; Zak Doffman, *Secret U.S. Cyber Mission Devastated Iran's Attack Capabilities, Officials Say*, FORBES (Aug. 29, 2019), https://www.forbes.com/sites/zakdoffman/2019/08/29/secret-cyber-mission-devastated-irans-attack-capabilities-us-officials-say/#def2db75cb35.

[12] James Hilder, *Computer Virus Used to Sabotage Iran's Nuclear Plan "Built by US and Israel"*, AUSTRALIAN (Jan. 27, 2011), https://www.theaustralian.com.au/news/world/computer-virus-used-to-sabotage-irans-nuclear-plans-built-by-us-and-israel/news-story/08eaf40536d1a14ca4fb39db2d396e7e.

[13] Barnes, *supra* note 11; Robert Chesney, *A Cyber Command Operational Update: Clarifying the June 2019 Iran Operation*, LAWFARE (Sept. 3, 2019), https://www.lawfareblog.com/cyber-command-operational-update-clarifying-june-2019-iran-operation.

eliminated, U.S. intelligence agencies no longer have the access they once did.[14] Nor is lost access necessarily the worst consequence. The Stuxnet episode taught that those targeted by malware can do more than patch computer program security failures. A foe like Iran can be hit in new ways but also should be expected to develop the digital means to hit back.[15] One computer expert referred to such so-called "cyberwars" as "boomerang wars."[16]

The United States developed the Stuxnet computer virus, which was able to leap across most known defenses to sabotage Iranian nuclear research. This, however, inspired Iran to create Shamoon, a computer virus it used in an attack that wiped out the hard drives in over 30,000 computers at the Saudi Aramco company. Saudi Arabia is an ally of the U.S. and competitor of Iran for influence in the Middle East. Saudi Arabia reacted to Iran's attack by developing a cyberspace "garrison." "The Saudis had understandable reasons for arming themselves in cyberspace. Iran had reportedly launched the 'Shamoon' virus in mid-2012, crippling tens of thousands of Saudi computers that took nearly half a year to repair. The kingdom also faced deadly terrorist threats, especially after the fireball of the Islamic State exploded across Syria and Iraq in 2014."[17] In response to the 'Shamoon' virus, the Saudis contracted with the private Italian firm Hacking Team, Israeli firms NSO Group and its affiliate, Q Cyber Technologies, and the Emirati firm DarkMatter. Additionally, the Saudis acquired a sophisticated phone hacking system called Pegasus from Q Cyber Technologies with the permission of the Israeli government. While it would be surprising for Israel to permit the Saudi government to acquire such knowhow, in doing so, Israel could both improve relations with a long-antagonistic country and enhance its own intelligence gathering there and elsewhere.

Pegasus allows a hacker to access a smartphone's microphones and cameras to surveille the user. The Saudi government allegedly used the program in the well-publicized murder of Saudi journalist, Jamal Khashoggi, in October 2018.[18] Khashoggi had been part of an effort to counter Saudi government use of social media to repress legitimate political dissent. After threats to him and his family, arrests of colleagues, and a determined misinformation campaign, Khashoggi fled to the United States where he continued his efforts by writing for the *Washington Post*. Pegasus allowed the Saudis to learn of Khashoggi's plans to travel to Istanbul and the Saudi consulate to apply for a visa for his fiancée. While in the consulate, Saudi agents murdered and dismembered him.[19]

---

[14] P.W. Singer, *'Dark Territory: The Secret History of Cyber War,' by Fred Kaplan*, N.Y. TIMES (Mar. 1, 2016), https://www.nytimes.com/2016/03/06/books/review/dark-territory-the-secret-history-of-cyber-war-by-fred-kaplan.html.

[15] Ilan Gattegno, *Exclusive: Stuxnet Was Out of Control, Kaspersky Had to Reveal It*, ISRAEL HAYOM (June 13, 2013), https://www.israelandstuff.com/exclusive-stuxnet-virus-was-out-of-control-kaspersky-had-to-reveal-it.

[16] David Ignatius, *How a Chilling Cyberwar Ensnared Jamal Khashoggi*, WASH. POST (Dec. 7, 2018), https://www.washingtonpost.com/opinions/global-opinions/how-a-chilling-saudi-cyberwar-ensnared-jamal-khashoggi/2018/12/07/f5f048fe-f975-11e8-8c9a-860ce2a8148f_story.html. For a detailed look at Hacker Team and other similar companies, see Mattathias Schwartz, *Cyberwar, Inc. Inside the Global Software Industry That Turned Email Hacking Into a Weapon for Sale*, N.Y. TIMES MAGAZINE, (Jan. 8, 2017).

[17] Ignatius, *supra* note 16.

[18] *Id.*

[19] *Id.*

These various incidents give a sense of the widespread and variable uses of computers to harm. Every individual using a computer is both vulnerable to malicious cyber conduct and a potential perpetrator of it. This conduct can be divided into two general categories: cyberattacks and cyber espionage. Both categories involve the use of "malware." The word "malware" is a shortened form of the two-word phrase "malicious software."[20] Malware is used in cyberattacks, which are acts "of unauthorized altering, deleting, disrupting, damaging or suppressing data within targeted computerized systems or networks."[21] It is also used in cyber espionage acts "of accessing or storing"[22] confidential data on computers. Anyone with an email account is familiar with techniques used in attacks and espionage. Service providers and information technology (IT) departments warn constantly not to open suspicious attachments and to update systems with the latest computer security software. They are in a constant race with hackers looking for vulnerabilities. In the last several years, some computer security specialists have begun to advocate moving beyond "passive" to "active" cyber defense.[23] Passive measures are intended to remain within a computer or computer network, such as firewalls, antivirus programs, and intrusion detection software.[24] Active defenses are intended to affect other computers and external networks that have been or could potentially be the source of malicious cyber conduct aimed at the defender. Active cyber defenses include programs that track data thefts to identify hackers and even to retrieve stolen information.[25] Active defense programs also deploy traps to lure hackers to decoy networks or cause them to infect their own computers and networks with malware.[26]

There is no difference between malicious cyber conduct and active cyber defenses in some cases. The label depends on the perspective of the commentator. The United States government hacked into Iranian computers for defensive purposes, as did the Iranian government respecting Saudi computers. The Saudi government, in its turn, plainly considers people such as Khashoggi to be threats. Spying on him is part of a national security strategy. The financial incentives to produce offensive cyber measures are substantial. So, despite the law, by 2010, defense contractors were using Cold War terms and analogies to shape perceptions and government budgets.

> The United States is fighting a cyber-war today, and we are losing. It's that simple. . . . What is the right strategy for this most modern of wars? Look to history. During the Cold War,

---

[20] Alexandra Van Dine, *When is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures Under the Budapest Convention*, CHICAGO J. OF INT'L L. (forthcoming), citing Norton, *What is Malware and How Can We Prevent It?*, NORTON SECURITY CENTER, https://us.norton.com/internetsecurity-malware.html (last visited Nov. 4, 2018).

[21] *Id.*

[22] *Id.*

[23] Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J. L. & TECH. 429, 474 (2012); Paul Rosenzweig, *International Law and Private Actor Active Cyber Defense Measures*, 50 STAN. J. INT'L L. 103, 103–105 (2014).

[24] Kesan & Hayes, *supra* note 23, at 474.

[25] CTR. FOR CYBER & HOMELAND SECURITY, GEO. WASH. UNIV., INTO THE GRAY ZONE, THE PRIVATE SECTOR AND ACTIVE DEFENSE AGAINST CYBER THREATS 11–12 (Oct. 2016).

[26] *Id.* at 10.

> when the United States faced an existential threat from the Soviet Union, we relied on deterrence to protect ourselves from nuclear attack. Later, as the East-West stalemate ended and nuclear weapons proliferated, some argued that preemption made more sense in an age of global terrorism. The cyber-war mirrors the nuclear challenge in terms of the potential economic and psychological effects. So, should our strategy be deterrence or preemption? The answer: both. Depending on the nature of the threat, we can deploy aspects of either approach to defend America in cyberspace.[27]

Offensive cyberattacks, whether for defense, active defense, preemption or deterrence, however, will in almost no case meet the conditions of a lawful response.

The challenges of keeping the Internet secure for legitimate uses in such a reality are well known. Software developers are constantly creating defenses, but public and private actors also heavily invest in aggressive responses that flout the law in the name of the asserted higher goal of individual security. The attitude is consistent with a general decline in respect for the rule of law. It has led to uninformed commentary that there is no law or virtually no law applicable to cyberspace binding on sovereign states.[28] The next section lays out evidence to the contrary.

II. CYBER MISCONDUCT UNDER INTERNATIONAL LAW

International law, like all law, exists to provide an alternative to violence and status in creating good order within human communities.[29] Wherever people come together, examples of law can be found. This is as true of cyberspace as any tangible geographic location. For each of the examples of cyber misconduct just reviewed, international law provides restrictions. Certain narrow exceptions are permitted for coercive measures of law enforcement. This discussion will consider first the restrictions, then the exceptions.

---

[27] Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, DAILY CALLER (Feb. 20, 2012), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (paragraph breaks omitted).

[28] Stewart A. Baker & Charles J. Dunlap Jr., *What is the Role of Lawyers in Cyberwarfare?,* ABA JOURNAL (May 1, 2012, 10:00 AM), http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare.

[29] According to Zoller, anthropologists support this reason for the emergence of law. ELISABETH ZOLLER, PEACETIME UNILATERAL REMEDIES: AN ANALYSIS OF COUNTERMEASURES 4 (1984). *See also* H.L.A. HART, THE CONCEPT OF LAW 87–91 (2d ed. 1994); Ian Brownlie, *The Peaceful Settlement of International Disputes in Practice,* 7 PACE INT'L L. REV. 257, 257 (1995).

A. *THE PROHIBITIONS ON FORCE AND INTERVENTION*

This section begins with the use of force, which is the least relevant area of restrictive law for the cases reviewed above. Nevertheless, the United States government and legal scholars, heavily influenced by realism, have long sought to characterize cyberspace as falling principally within the military domain. After a brief explanation of why that characterization is unconvincing, the discussion will move on to other more applicable legal principles: non-intervention, property, and privacy rights.

Following World War II, the most catastrophic war in history, the United States led the way toward creating a legal regime to prevent future armed conflicts. The United Nations Charter restates the ancient, peremptory norm prohibiting the use of force in Article 2(4):

> 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 the United Nations.

Article 2(4) prohibits the use of armed force of some significance. Minor uses of force, such as shooting across the bow of a ship as part of an arrest operation or shooting across a border at people throwing rocks, fall below the scope threshold of Article 2(4). These forms of force fall within the scope of other prohibitory and protective principles.[30] In September 2005, the sovereign states of the world gathered in New York to reconfirm their commitment to strict compliance with Article 2(4) and the Charter's other provisions regulating the resort to force.[31] A violation of Article 2(4) requires significant physical damage or destruction. The focus is on the violence, not the means to produce it. That said, computers are a means to communicate with or control a potentially lethal force. They are not the lethal forces or weapons themselves. A simple analogy clarifies the point: an old-fashioned stick of dynamite might be used as a weapon once the fuse is lighted. We do not refer to the means of lighting the fuse, such as a lighter or match, as a weapon or an attack.[32]

---

[30] Mary Ellen O'Connell, *The True Meaning of Force*, AJIL UNBOUND (Aug. 4, 2014), https://www.asil.org/blogs/true-meaning-force (replying to Tom Ruys, *The Meaning of "Force" and the Boundaries of the* Jus Ad Bellum*: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?*, 108 AM. J. INT'L L. 159 (2014)).

[31] G.A. Res. 60/1, 2005 World Summit Outcome, ¶ 77–80 (Sept. 16, 2005).

[32] It is on the erroneous basis that the computer malware is the match and dynamite, not just the match, that underlies the approach of the INT'L GRP. OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (2013) [hereinafter TALLINN MANUAL], critically reviewed in Dieter Fleck, *Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New* Tallinn Manual,18 J. CONFLICT & SECURITY L. 331 (2013). For another example of this problematic approach, see YAROSLAV RADZIWILL, CYBER-ATTACKS AND THE EXPLOITABLE IMPERFECTIONS OF INTERNATIONAL LAW (2015). In the second version of the manual, where the authors appropriately emphasize countermeasures over the use of force, they still mention the view that cyber operations producing no physical destruction or injury to people could nevertheless be a use of force within the meaning of Article 2(4). INT'L GRP. OF EXPERTS, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 333 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

Scholars who apparently understand that international law is generally the relevant law for cyber security questions may still argue that it is difficult to fit cyber problems into the rules of international law with respect to the use of force.[33] Instead of concluding, therefore, that it is necessary to look at other international rules, such as those on non-intervention, countermeasures, economic law, and the like, these scholars advocate new interpretations of the rules on the use of force in order to have the right to respond to cyber problems with military force.[34]

None of the cases in Part I involve a violation of Article 2(4). The United States' plan to attack Iran with manned aircraft potentially killing 150 people would have been a clear violation. Article 2(4) prohibits even threatening such an operation, but threats are so common that the attempt to restrict them under Article 2(4), in distinction to actual attacks, has fallen into desuetude.[35] Iran's destruction of a U.S. drone and the U.S. response involving manipulation of Iranian computers fall under the principle of non-intervention and international economic law property protections.

The principle of non-intervention reaches these lesser forms of force, as well as forms of coercion not involving the use of armed force.[36] Many specific examples are provided in the United Nations General Assembly Declaration on the Inadmissibility of Intervention of 1981, including that it is the duty of a state "in the conduct of its international relations in the economic, social, technical and trade fields, to refrain from measures which would constitute interference or intervention in the internal or external affairs of another State . . . ."[37]

Non-intervention protects the equality of states under international law. Without it, a legal order could only be based on an imperial or hegemonic law-giver. The international legal system is founded on a principle of state equality, as the United Nations Charter reflects. The Charter confirms that a goal of the UN is to establish "friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace . . . ."[38] For Russell Buchan, the prohibition on intervention can be discerned in part by distinguishing the conduct prohibited under the rule from mere interference. Intervention involves coercion, while mere interference is an "inevitable by-product of an increasingly globalised world order where states are constantly interacting."[39] Coercion is

---

[33] *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 913, 920–23 (1999). *See also* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 103–08 (2002).

[34] Waxman returns to the advocacy of some scholars during the Cold War for expanded rights to use military force by resorting to novel interpretations of the plain terms of the UN Charter and rules of customary international law in Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 425–426 (2011).

[35] *But see* Nicholas Tsagourias, *The Prohibition of Threats of Force*, *in* RESEARCH HANDBOOK ON INTERNATIONAL CONFLICT AND SECURITY LAW: *JUS AD BELLUM*, *JUS IN BELLO*, AND *JUS POST BELLUM* 67 (Nigel D. White & Christian Henderson eds., 2013).

[36] G.A. Res. 36/103, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States (Dec. 9, 1981) [hereinafter Declaration on Non-intervention]; G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Oct. 24, 1970).

[37] Declaration on Non-intervention, *supra* note 36, at Pt. II, ¶ k.

[38] U.N. Charter art. 1(2).

[39] RUSSELL BUCHAN, CYBER ESPIONAGE AND INTERNATIONAL LAW 63 (2018).

the application of pressure to subvert the will of the target. In international relations, it is "dictatorial interference. . . in the affairs of another State for the purpose of maintaining or altering the actual condition of things."[40] Buchan concludes that inter-sovereign state cyber espionage, like espionage in general, is likely prohibited by international law only when it involves coercion.[41]

B. *SPYING AND THEFT*

Given the less stringent restrictions on non-coercive espionage, some states apparently attempt to characterize theft of commercially valuable data as espionage. China, for example, bases its very identity as a nation on its economy, and plausibly argues that promoting its economic interests by any means is the same as promoting its national security. The United States has taken issue with this perspective. In 2015, President Obama and President Xi agreed on several important conceptual points, including:

> The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
>
> Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic.[42]

International law protects the property rights of states and individuals. The right of states to sovereign control over geographic space—land territory, the air column above it, and maritime space appurtenant to it—is protected by the principles on the non-use of force and non-intervention. Additional property protections are found in the exceptions for both the use of force and other forms of coercion, including countermeasures that involve freezing assets and other forms of takings.[43] Other forms of property, such as natural resources and other economic assets, are protected by the principle of non-intervention, together

---

[40] *Id.* (citing LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE 305 (H. Lauterpacht, ed., 1955)).

[41] BUCHAN, *supra* note 39, at 65.

[42] White House, Office of the Press Sec'y, *Fact Sheet: President Xi Jinping's State Visit to the United States* (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[43] *See* U.N. Charter 2(4), 51. For a recent, comprehensive discussion of the international law of armed self-defense, which includes the role of the Security Council, see MARY ELLEN O'CONNELL, CHRISTIAN TAMS & DIRE TLADI, SELF-DEFENCE AGAINST NON-STATE ACTORS (2019).

with principles such as sovereign and diplomatic immunity extended to certain property to protect them from proceedings in foreign national courts.[44] States also have certain due process rights that must be honored before being deprived of non-immune assets. With respect to human beings, officials of states enjoy immunity when acting in their official capacity, which includes protection of their private property.[45] For private individuals, Article 17 of the Universal Declaration of Human Rights provides that "[e]veryone has the right to own property alone as well as in association with others." It also declares that no person will be deprived arbitrarily of property.[46]

Human beings clearly possess a human right to privacy. States may also take certain measures to protect their confidential information. Espionage to obtain policy-related secrets lacking a commercial application may be prosecuted in national courts for violation of domestic law but likely does not violate international law if coercive methods are avoided.[47] States may also protect the privacy rights of their nationals from cyber espionage using countermeasures. The nature of personal privacy rights is being developed through, in particular, the global application of the European Union's General Data Privacy Regulation.[48] For the purposes of this analysis, the even more important international law duty is the one that requires states to exercise due diligence over their nationals using the Internet.[49] States have a duty to take active steps to prevent cybercrimes.[50] Some cybercrimes did not exist before the invention of the personal computer, such as theft of Bitcoin. Others pre-date computers, but criminals use computers in carrying them out today, such as spying.

III. LAWFUL RESPONSES TO CYBER MISCONDUCT

As mentioned at several points above, the use of military force in response to malicious cyber operations not connected with kinetic violence is always unlawful. In contrast, countermeasures are generally lawful, so long as the conditions provided in international law are met. The same sort of coercive measures that are lawful to use against economic wrongs and violations of arms control treaties known as "countermeasures," or more colloquially

---

[44] G.A. Res. 59/38, annex, United Nations Convention on Jurisdictional Immunities of States and Their Property (Dec. 2, 2004).

[45] David P. Stewart, *The Immunity of State Officials Under the UN Convention on Jurisdictional Immunities of States and Their Property*, 44 VAND. J. OF TRANSNAT'L L. 1047 (2011).

[46] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948). *See also* Case C-402/05, Kadi and Al Barakaat International Foundation v. Council and Commission, 2008 E.C.R. I-6351.

[47] BUCHAN, *supra* note 39, at 66. *See also* Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SEC. L. & POL'Y 179, 185, 197–207 (2011).

[48] The GDPR has its own website: https://eugdpr.org/.

[49] For an excellent discussion of the general due diligence obligation of states vis-à-vis their nationals, see TIM STEPHENS & DUNCAN FRENCH, SECOND REPORT ON DUE DILIGENCE IN INTERNATIONAL LAW (2016), https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=1427&StorageFileGuid=ed229726-4796-47f2-b891-8cafa221685f.

[50] For details of what counts in the international community as "cybercrime," see Budapest Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13,174, E.T.S 185.

"sanctions,"[51] are lawful for use against malicious cyber conduct. Using cyber operations as countermeasures is more difficult to fit in the lawful countermeasure category. This Part analyzes the conditions of taking lawful countermeasures in response to cyber misconduct, focusing on the lawful purpose of countermeasures, attribution, necessity, and proportionality. The United Nations International Law Commission (ILC) has included the general principles of law regulating countermeasures in its Articles on State Responsibility, accepted by the General Assembly in 2001.[52] The 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* analyzes the Articles using examples of cyber operations, supporting the conclusion that countermeasures are the lawful means of applying coercive measures in response to interstate violations of rights associated with computers.[53]

Countermeasures are lawful actions taken in response to a prior unlawful action. The responding state must provide public notice of the claim of wrongdoing before instituting countermeasures. If, upon received notice, the accused does not end the unlawful conduct and provide a remedy within a reasonable period, the responding state has demonstrated the necessity of imposing a proportionate countermeasure so long as it is aimed at inducing law compliance.[54] The ILC defines countermeasures as a defense to an otherwise unlawful action: "[t]he wrongfulness of an act of a state not in conformity with an international obligation towards another state is precluded if and to the extent that the act constitutes a countermeasure taken against the latter state in accordance with" other conditions set out in the Articles.[55]

The Articles on State Responsibility explicitly require that the state taking countermeasures against another state be responding to a wrong under international law since the purpose of countermeasures is to procure compliance with an obligation or to serve as a remedy for a past violation. Recall from the discussion above that, in many areas of international law, the foreign state has committed a wrong both if it has directly violated a duty and if it has failed to exercise due diligence respecting nationals. Prior to taking the measure, the injured state must notify the state accused of wrongdoing of its intention and offer to negotiate. The Articles provide for an exception in cases of urgency,

---

[51] The definitions of the terms "countermeasures" and "sanctions" are not a settled matter in international law. White and Abass, for example, define countermeasures as non-forcible measures taken by states and sanctions as non-forcible measures taken by organizations. This would be a helpful distinction but for the fact that the United States, for example, labels its unilateral, non-forcible coercive measures "sanctions". *See generally* Nigel White & Ademola Abass, *Countermeasures and Sanctions*, *in* INTERNATIONAL LAW 531 (Malcolm D. Evans ed., 3d ed. 2010).

[52] Int'l Law Comm'n, Responsibility of States for Internationally Wrongful Acts, arts. 22, 49–54, U.N. Doc. A/56/10, at ¶ 76 (2001).

[53] TALLINN MANUAL 2.0, *supra* note 32, at 111–142. An earlier, though more limited, analysis is found in O'Connell, *Cyber Security Without Cyber War*, *supra* note 3 (drawing on the Articles on State Responsibility and Gabčíkovo-Nagymaros Project (Hung./Slovk.), Judgment, 1997 I.C.J. Rep. 7, 52–57 (Sept. 25)).

[54] Int'l Law Comm'n, Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/10, at ¶ 76 (2001).

[55] *Id.* at art. 22. *See also* Air Services Agreement (U.S. v. Fr.), Judgment, 1978 R.I.A.A. 417, 427 (Dec. 9).

although countermeasures may never involve the use of force unless consistent with the Charter regime, even in urgent situations.[56]

The *Tallinn Manual 2.0* authors do not mention the notice requirement in their discussion of procedural aspects of countermeasures law. They provide a hypothetical to exemplify a lawful cyber countermeasure, but in fact owing to the failure to provide notice, the countermeasure is unlawful. The scenario involves two states at the end of an armed conflict that agree to share information for family reunification. When one state does not provide the required information, the other hacks into the relevant database and obtains it.[57] The hypothetical measure is proportionate but nevertheless unlawful in at least two respects. As the ICJ pointed out in *Gabčíkovo-Nagymaros*, the countermeasure must aim at the entitlement of the injured state.[58] In this case, the entitlement is to be given information, not to have the information, let alone to take it. The *Manual* authors argue that the injured state is enforcing a wider obligation to aid in family reunification while getting the specific information it was promised. In *Gabčíkovo-Nagymaros*, however, Slovakia used a measure to obtain the equivalent of the final outcome of its treaty with Hungary. That is not, however, Slovakia's entitlement. It was to have Hungary's cooperation in obtaining the outcome. The countermeasure needed to aim at inducing Hungary's cooperation.

Specifically, on the issue of public notice, the *Manual* authors are silent. In *Gabčíkovo-Nagymaros*, Slovakia gave Hungary plenty of notice of the action it would take as a countermeasure if Hungary did not honor their bilateral treaty.[59] In the *Manual*'s hypothetical, no notice is provided to the state failing in its duty. Perhaps it would be enough for the injured state to say, "either provide the information, or we will obtain it clandestinely." That would surely cause the breaching state to reinforce security around the data—computer security as well as conventional. In the *Corfu Channel* case the ICJ admonished the United Kingdom for using unlawful means to obtain evidence for its case against Albania.[60] The UK entered Albanian waters without permission and for purposes other than navigation. Among the several problems with the UK action, one is that the UK failed to give notice to Albania of the measure it would take.

In order to provide this notice, the state planning to take a countermeasure must have clear and convincing evidence that the wrong is attributable to a foreign, sovereign state. More importantly, the actual wrong doer must be identified at the requisite level of legal certainty before a coercive measure to enforce legal rights may be imposed. To do otherwise is to offend principles of legality that require, as a matter of fairness, punishment be imposed only on the perpetrator and not on the innocent. A state must also be able to legally attribute the action before taking a coercive measure as an aspect of the principle of legality. As with the lawful exercise of force, a coercive response may only be against a state bearing legal responsibility for the wrong that triggered the right to take a countermeasure. Responsibility for that wrong is assigned through

---

[56] Int'l Law Comm'n, Responsibility of States for Internationally Wrongful Acts, art. 52(1)(b), U.N. Doc. A/56/10, at ¶ 76 (2001).

[57] TALLINN MANUAL 2.0, *supra* note 32, at 117.

[58] Gabčíkovo-Nagymaros Project (Hung./Slovk.), Judgment, 1997 I.C.J. Rep. 7, 52–57 (Sept. 25).

[59] *Id.*

[60] Corfu Channel (UK v. Albania), Judgment, 1949 I.C.J. Rep. 4 (Apr. 9).

principles of attribution. As secondary or process rules of fundamental importance, the law of attribution belongs with the general principles of necessity and proportionality.[61] The ICJ emphasized the importance of links of responsibility in the *Nicaragua*, *Congo*, and *Bosnia v. Serbia* cases.[62]

While the Articles on State Responsibility say little about why attribution must be made—perhaps because the point is so widely accepted as basic fairness and common sense, concepts most people understand instinctually—arguments to justify coercive action are heard so commonly today that it is worth emphasizing that acting against a party bearing no legal responsibility is itself a wrong. Regardless of whether it is used as a message or to deter other wrongdoers, it violates the law. With respect to the use of force, arguments are being made that dilute attribution to the vanishing point, with the aim of creating broader rights to use force on the territory of states bearing no legal responsibility for wrongdoing.[63] It is still the law, however, that attacking a state in such circumstances is itself a violation of the prohibition. The contrary view seems to have found a place in international law due to a belief that greater security can be won through greater use of military force and coercion of all kinds.

The standard of evidence for proving all the conditions required in countermeasures is the general one in government cases: clear and convincing. There is no standard for making mere accusations. As with threats, these are so common, that they remain in the ungoverned world of political rhetoric. Only in formal processes are standards set, such as the process of taking countermeasures in the enforcement of norms. The International Court of Justice has a standard in its rules, Article 38(2), which requires a "succinct statement of the facts and grounds on which the claim is based."[64] In the larger realm of inter-state claims and accusations that only rarely reach the ICJ, however, an accusation is no more than a retorsion. It may be an unfriendly act but in the world of diplomacy and inter-state communications, it is difficult to say that even unlawful threats of military force are prohibited given that they are so common. A potentially false accusation of malicious cyber conduct is well within that outer limit. The only real limit is political embarrassment should the accusation be disproved.

Prior to taking a countermeasure, however, the basic evidentiary standard for court actions and the one to use for credible accusations of cyber misconduct is clear and convincing.[65] The clear and convincing standard must be met as to

---

[61] NILS MELZER, TARGETED KILLING IN INTERNATIONAL LAW 294 (Oxford University Press 2008).

[62] Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 93–116 (June 27); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. Rep. 168, ¶ 148–66 (Dec. 19); Application of the Genocide Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶ 385–412 (Feb. 26).

[63] See, for example, the campaign for substituting a concept that a state is "unwilling" or "unable" to control terrorism on its territory as a substitute for principles of attribution as sufficient to exercise force in self-defense on the territory of the "unwilling/unable" state. *See also* Daniel Bethlehem, *Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM J. INT'L L.770, 773 (2012).

[64] *See* International Court of Justice, Rules of Court (1978), https://www.icj-cij.org/en/rules.

[65] "Clear and convincing" is higher than "preponderance of the evidence," which is generally required in civil cases, but lower than "beyond a reasonable doubt," needed for criminal cases. *See* Mary Ellen O'Connell, *Evidence of Terror,* 7 J. CONFLICT & SECURITY L. 19, 22–28 (2002).

attribution and the other conditions. The extensive attribution rules, of the Articles on State Responsibility,[66] are summed up in the *Tallinn Manual 2.0 on*

---

[66] Int'l Law Comm'n, Responsibility of States for Internationally Wrongful Acts, arts. 4–11:

Article 4
Conduct of organs of a State

1. The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State.

2. An organ includes any person or entity which has that status in accordance with the internal law of the State.

Article 5
Conduct of persons or entities exercising elements of governmental authority

The conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance.

Article 6
Conduct of organs placed at the disposal of a State by another State

The conduct of an organ placed at the disposal of a State by another State shall be considered an act of the former State under international law if the organ is acting in the exercise of elements of the governmental authority of the State at whose disposal it is placed.

Article 7
Excess of authority or contravention of instructions

The conduct of an organ of a State or of a person or entity empowered to exercise elements of the governmental authority shall be considered an act of the State under international law if the organ, person or entity acts in that capacity, even if it exceeds its authority or contravenes instructions.

Article 8
Conduct directed or controlled by a State

The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.

Article 9
Conduct carried out in the absence or default of the official authorities

The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority.

the International Law Applicable to Cyber Operations: "[c]yber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State."[67]

The Articles on State Responsibility also provide guidance for judging the proportionality and necessity of resorting to countermeasures. To be proportional, "[c]ountermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[68] They must not injure third states, and they must be necessary. Necessity involves both last resort and chance of success as indicated

---

Article 10
Conduct of an insurrectional or other movement

1. The conduct of an insurrectional movement which becomes the new Government of a State shall be considered an act of that State under international law.

2. The conduct of a movement, insurrectional or other, which succeeds in establishing a new State in part of the territory of a pre-existing State or in a territory under its administration shall be considered an act of the new State under international law.

3. This article is without prejudice to the attribution to a State of any conduct, however related to that of the movement concerned, which is to be considered an act of that State by virtue of articles 4 to 9.

Article 11
Conduct acknowledged and adopted by a State as its own

Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.

[67] TALLINN MANUAL 2.0, *supra* note 32, at 87.
[68] Int'l Law Comm'n, Responsibility of States for Internationally Wrongful Acts, art. 51.

in the Articles on State Responsibility,[69] as well as the general principle of necessity.[70]

All of these conditions of lawful countermeasures add up to formidable barriers to using malicious cyber conduct as a countermeasure. Coercive measures, including so-called "active cyber defenses," are a gamble that aim only at future deterrence. They do not work to achieve immediate protection. They have little or no chance of ending a wrong immediately or inducing a state to provide a remedy. Governments using malicious cyber operations have shown no inclination to announce ahead of time that they will use cyberattacks until the target state complies. Secrecy is the hallmark of cyber misconduct. Nor is proportionality achievable, let alone restricting effects to the wrongdoer. As with Stuxnet, the effects of malware are difficult to control. Stuxnet damaged "100,000 computers all over Europe. There was a need to stop it. Cyberwars act like boomerangs . . . . So, it would be advisable for governments not to enter cyber-wars because in a boomerang war there are no winners."[71]

---

[69] *Id.* at art. 25:

Article 25
Necessity

1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act:

(a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and

(b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.

2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if:

(a) the international obligation in question excludes the possibility of invoking necessity; or

(b) the State has contributed to the situation of necessity.

Article 49
Object and limits of countermeasures

1. An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under part two.

2. Countermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State.

3. Countermeasures shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question.

UN ILC, Articles on State Responsibility, art. 52 requires public notice and an opportunity to negotiate a settlement of the dispute prior to imposing countermeasures.

[70] BIN CHENG, *supra* note 6, at 70–7, 71, 74 (citing THE NEPTUNE, 4 INTERNATIONAL ADJUDICATION MANUSCRIPTS 372 (1797)).

[71] Gattegno, *supra* note 15.

The *Tallinn Manual 2.0* suggests that necessity is a discrete defense, separate from the law of countermeasures that may apply in the "cyber context" when taken to protect an "essential interest" of the state.[72] The argument, based on theory, rather than reality, of harming another state to protect the state's own "cyber infrastructure" cannot compare with using defensive measures.[73]

CONCLUSION

Plainly, it is difficult to meet these requirements when using cyber misconduct to respond to cyber misconduct.[74] Note the paradox when a state like the United States, which purports to want to "encourage universal adherence to cyber norms," uses malicious cyber operations for any reason:

> International law and voluntary non-binding norms of responsible state behavior in cyberspace provide stabilizing, security enhancing standards that define acceptable behavior to all states and promote greater predictability and stability in cyberspace. The United States will encourage other nations to publicly affirm these principle and views through enhanced outreach and engagement in multilateral fora. Increased public affirmation by the United States and other governments will lead to accepted expectations of state behavior and thus contribute to greater predictability and stability in cyberspace.[75]

Defensive measures that do not include offensive aspects, such as a "honey trap," are always lawful and require no attribution or satisfaction of the conditions of necessity and proportionality. In the 2019 U.S.-Iran case, no doubt many believe that damaging computers rather than killing people was laudable. They overlook that it was not an either-or choice. Responses in compliance with the rule of law—on which the right to life, prosperity, and security depend—also exist.

---

[72] TALLINN MANUAL 2.0, *supra* note 32, at 135.

[73] *Id.* at 137.

[74] Alexandra Perina, U.S. Dep't of State, Remarks at ASIL Annual Meeting: Countermeasures in Cyberspace (Apr. 10, 2014) (The various elements examined here are unlikely to have been part of the assessment in Remarks of Alexandra Perina, U.S. State Department, on necessity as a defense to the use of cyberattacks in responding to cyber espionage, theft and damage. ASIL Annual Meeting, Panel: Countermeasures in Cyberspace, Apr. 11, 2014.).

[75] THE WHITE HOUSE, *supra* note 1, at 20.