Using International Law to Deter Russian Proxy Hackers

Colonel Andrew D. Flor

> States are legally responsible for activities undertaken through "proxy actors," who act on the State's instructions or under its direction or control.
>
> —*Harold Koh*[1]

In 2014, Russia employed dozens of proxy trolls to engage in information warfare in support of its operations in Ukraine.[2] "Hundreds of fake social media accounts backed by Russian hackers using malware and cyber-attacks flooded the news and online community with disinformation designed to conceal the truth that these groups were backed by Russia to foment domestic dissent."[3] This hybrid warfare, developed during Russia's 2008 campaign in Georgia, helps Russia to "destabilize surrounding countries" and induces "perception management" that provides Russia with the illusion of "legal legitimacy."[4] Russia's perception management fed the false narrative that Russia had no choice but to support "Russian ethnic minorities" in Crimea who faced "Ukrainian oppression" and wanted to secede and pursue "self-determination."[5] When Ukrainian citizens attempted to search online for information about the impending Russian invasion, their searches found Russian disinformation spread by these proxy trolls that were legitimizing Russia's invasion.[6]

Fast-forward to 2022 and the Russian invasion of Ukraine: Russia continues to employ proxy hackers to destabilize Ukraine and cast doubt on the legitimacy of the Ukrainian government. The "Conti ransomware gang issued a warning" shortly after the war commenced threatening they "would respond to cyber activity against Russia using all their resources 'to strike back at the critical infrastructure of an enemy.'"[7] Other cyber proxy activity has targeted exploits in Microsoft Windows even as recently as June 2022 where the "Russian hacking group Sandworm" exploited a remote code execution vulnerability

COL Andrew D. Flor graduated from the United States Military Academy in 1997 with a Bachelor of Science degree in Computer Science. He commissioned as an Aviation officer and later received his Juris Doctor from the College of William and Mary School of Law in 2004 and is admitted to practice in the Commonwealth of Virginia. COL Flor holds an LL.M. from The Judge Advocate General's Legal Center and School, a Master of Strategic Studies (MSS) degree from the U.S. Army War College, and a Master of Military Art and Science (MMAS) degree from the U.S. Army Command and General Staff College. He currently serves as the Chief of Plans, Office of The Judge Advocate General (OTJAG), in the Pentagon.

called "Follina" in an effort to destabilize media organizations in Ukraine.[8]

Repeated Russian efforts to utilize this type of hybrid warfare will continue to present a problem in the future if the United States (US) and others do not impose costs on Russia. By using proxy hackers, Russia continues to obfuscate efforts to hold them accountable for invading former-Soviet Republics such as Georgia and Ukraine. The US should lead the international community in countering Russian proxy hackers through various means available under international law and norms, including criminal prosecution, sanctions on Russian officials who direct these illicit cyberspace operations, and, if necessary, the use of military force to prevent further non-State hacking efforts.

This article starts by defining proxy hackers and proxy hacking, and follows with a summary of the international law and norms that govern proxies. Recent actual and suspected proxy hacker events caused by Russia confirm some of the challenges of applying international law and norms to proxy hacking, including actions or inaction by victim States. The lack of available responses indicates an underdeveloped state of contemporary international law and reveals gaps the international community can fill by refining norms and applicable legal texts. This article concludes with specific recommendations on how to deal with the threat of proxy hackers, and otherwise deter Russia from using such hackers in the future.

Definitions and Russian Proxy Hacker Operations

Defining what constitutes a proxy hacker comes with inherent challenges. Merriam-Webster defines a proxy as "the agency, function, or office of a deputy who acts as a substitute for another."[9] In the cyber context, a proxy is an "actor b acting for actor a," or more specifically that non-State actor b conducts a cyberspace operation as a substitute for State actor a.[10] The first *Tallinn Manual*, a collection of international law provisions

related to cyber warfare drafted by an International Group of Experts, in Rule 6, "Legal Responsibility of States," declares that "[a] State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."[11] Commonly referred to as the attribution rule, commentary to this rule describes attribution as "a quintessential principle of international law," and that such a breach of international obligation can come from "either an act or omission."[12] The commentary also applies this rule to non-State actors, "where [the State] has 'effective control' over such actors."[13] However, the rule limits applicability to situations where "private citizens, on their own initiative, conduct cyber operations (so-called 'hacktivists' or 'patriotic hackers')."[14] The key difference in attribution comes down to situations where the State has provided "instructions, direction, or control" over the non-State proxy hackers.[15] Establishing attribution through sufficient evidence of "instructions, direction, or control" occurs from any number of State actions, to include funding for proxy hackers, allowing the hackers safe-harbor in State territory, or protecting the hackers from domestic prosecution or international extradition.[16]

As an example, the US hires contractors to conduct cyberspace operations on behalf of U.S. Cyber Command (USCYBERCOM).[17] While this type of relationship would fall within the definition above of a non-State actor, the use of contractors as a substitute for a State actor, USCYBERCOM, would not constitute the type of proxy hacker violation discussed in the *Tallinn Manual* because the contract between the US and the contractor creates a principal-agent relationship.[18] A principal-agent relationship means that the behavior of the contractor (the agent) is controlled by or authorized by the US (the principal). There is no intent by the US to avoid responsibility for contractor actions, even if great efforts are made to obfuscate the US' cyberspace operations.

Russian proxy hackers differ from USCYBERCOM contractors due to the lack of any acknowledged official relationship between these hackers and the Russian government. In some examples discussed later below, the hackers conduct their operations with minimal Russian oversight or control. In other examples, hackers, whether motivated by patriotism or self-interest, act completely on their own volition. While this independent-style action by patriotic hackers would seem to absolve Russia from responsibility for such malicious cyberspace activities, the law can attribute to Russia the acts of these patriotic hackers if Russia knows about their behavior and fails to stop them. Major General Joseph Berger, who previously served as the Army Cyber Command (ARCYBER) Staff Judge Advocate or senior legal advisor, objects to the phrase "patriotic hacker" because of the "status or imprimatur" accorded by this.[19] However, regardless of status, Russia's undeclared, and often obfuscated, support and direction of cyber hackers create an attribution challenge for the international community.

Brigadier General George Smawley, the Staff Judge Advocate to USCYBERCOM from 2019-2021, states that USCYBERCOM categorizes non-State adversaries into one of four groups: proxies, agents, aligned groups, or criminal organizations.[20] Each one requires different legal

authorities to address, and Russia has deployed cyberspace operations in each of these four categories.[21]

The 2018 Senate Report on Russian Interference provides an example of illicit proxy behavior, namely that "Kremlin-backed entities have spent years professionalizing a cadre of paid trolls, investing in large-scale, industrialized 'troll farms,' in order to obscure Moscow's hand and advance the aims of Russia's information operations both domestically and abroad."[22] These proxy trolls achieve their objectives through three main methods. First, they attack the media: "as Soviet-born author Peter Pomerantsev notes, 'The Kremlin successfully erodes the integrity of investigative and political journalism, producing a lack of faith in traditional media.'"[23] Second, they remain "ideologically agnostic" and "can simultaneously support far right and far left movements, so long as they are in competition with one another," in order to sow confusion.[24] Third, by "attempt[ing] to exploit societal divisions that already exist, rather than attempt[ing] to create new ruptures," Russia can further divide the targeted country with these cyber operations.[25]

Review of Current International Law and Norms

Proxy hackers will continue to present a major challenge for countries around the world. As Major General Berger puts it, proxy hackers are "not going away."[26] Understanding international laws and norms is a prerequisite for State use of proxy hackers and responses to their use. These laws and norms have shortcomings, which will later form the basis for this article's recommendations.

The Tallinn Manuals – International Law and Norms in Cyberspace

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (referred to here as the first *Tallinn Manual*), published in 2013, sought to summarize the state of international law and norms in cyberspace "applicable to cyber warfare."[27] The use of this wording by the authors, the International Group of Experts (IGE), was a deliberate attempt to inform the readers that the manual did not cover cyber activities short of war. This created challenges in applying any of the first *Tallinn Manual* provisions to proxy hackers. The 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (referred to here as *Tallinn Manual 2.0*), published in 2017, specifically applies to "cyber operations during peacetime."[28] *Tallinn Manual 2.0* experts modified some of the rules addressed in the first *Tallinn Manual*. As such, "*Tallinn Manual 2.0* supersedes the first *Tallinn Manual.*"[29] Yet, *Tallinn Manual 2.0* still does not "deal with international criminal law, trade law, or intellectual property . . . or domestic law."[30] As a result, some of the same challenges in applying the first *Tallinn Manual* provisions to proxy hackers persist with *Tallinn Manual 2.0*.

Much of what proxy hackers do or try to achieve in cyberspace could constitute criminal behavior. Holding proxy hackers liable for their behavior starts with a criminal indictment.[31] But Russia does not normally extradite proxy hackers, even when faced with overwhelming

attribution evidence that it approved their actions.[32] Extradition illuminates the challenge of holding hackers accountable for murky, possibly State-sponsored, hacking efforts. *Tallinn Manual 2.0* discusses extradition in "International Cooperation in Law Enforcement" (Rule 13),[33] which provides that "States are not obliged to cooperate in the investigation and prosecution of cyber crime."[34] Yet, Comment 8 of this rule specifies that "if extradition is refused on the basis of nationality of the person sought or because the requested State deems that it has jurisdiction over the offence, the requested State shall take action to prosecute."[35] Comment 8 should help resolve problems with prosecution in most Russian proxy hacker attacks. If Russia denies extradition, then it must prosecute. Unfortunately, Russia has thus far ignored this rule with impunity.

Tallinn Manual 2.0 addresses "Internationally Wrongful Cyber Acts" (Rule 14) that expands on the first Tallinn Manual rule on "Legal Responsibility of States" (Rule 6). *Tallinn Manual 2.0* states that "A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation."[36] The term "cyber-related act" vice "cyber operation" deliberately "denote[s] the fact that a State sometimes may bear responsibility for acts other than cyber operations that it conducts or that are attributable to it."[37] The commentary underscores a State's responsibility to curb proxy hacker behavior: "[s]ince non-State actors such as hacktivists often launch harmful cyber operations . . . a State's obligation to take measures to control cyber activities taking place on its territory looms large."[38]

Tallinn Manual 2.0 updates the attribution rule, "Attribution of Cyber Operations by Non-State Actors" (Rule 17),[39] providing that "Cyber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own."[40] This modification and amplification of commentary accompanying Rule 6 from the first *Tallinn Manual* clarifies the circumstances that render a State responsible for actions of non-State actors, such as proxy hackers.[41]

Tallinn Manual 2.0 "Due Diligence (General Principle)" (Rule 6) reads, "A State must exercise due diligence in not allowing its territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States." Again, *Tallinn Manual 2.0* expands on the first *Tallinn Manual* in several important ways. First, it imposes the term "due diligence" vice "knowingly" from the original rule.[42] Second, it removes the restriction "exclusive" from governmental control, which reduces the required level of control over the territory concerned, whether territory or cyber infrastructure.[43] Finally, it expands the level of operations a State must control to those that "affect the rights of" or "produce serious adverse consequences for" other States.[44] This due diligence rule, combined with a new rule, "Compliance with the Due Diligence Principle" (Rule 7), "requires a State to take all measures that are feasible in the circumstances" to end all cyber operations that violate the due diligence principle.[45] Of note,

the commentary to this rule states that a majority of the IGE believe this rule requires a State to act to prevent repeated violations that occur on its territory.[46]

United States Position on Tallinn Manuals

The Tallinn Manuals constitute a serious body of work backed by years of effort, but they do not establish binding authority or otherwise create an enforceable right or treaty. Generally, international law only develops when the actions of States become the customary state practice with regard to that topic.[47] The only other way for these practices and norms to become international law is through treaties or conventions, such as the Geneva Conventions.[48]

The US position on the Tallinn Manuals is illuminating, given the relative cyber power ranking of the US.[49] In a 2016 speech at Berkeley Law School, Brian Egan, a former State Department Legal Adviser, summarized the United States view of the Tallinn Manuals:

> The United States has unequivocally been in accord with the underlying premise of this project, which is that existing international law applies to State behavior in cyberspace. In this respect, the Tallinn Manuals will make a valuable contribution to underscoring and demonstrating this point across a number of bodies of international law, even if we do not necessarily agree with every aspect of the Manuals.[50]

While this speech pre-dated *Tallinn Manual 2.0,* it remains clear that the US position has not changed since then; namely that current international law applies to State behavior in cyberspace.

In contrast, Russia did not send a representative to the IGE that drafted and advised on the creation of the Tallinn Manuals. Indeed, Russia's Defense Ministry openly opposed release of the first *Tallinn Manual* with the following language: "Russia is trying to prevent the militarization of cyberspace by urging the international community to adopt a code of conduct in this sphere, the US and its allies are already agreeing to the rules for prosecuting cyber warfare."[51] Russian experts did profess optimism that "compromise is possible" on the *Tallinn Manual* provisions.[52]

US Position on Proxy Hackers

In his Berkeley speech, Brian Egan underscored the US's strong position on proxy hackers:

> Additionally, cyber operations conducted by non-State actors are attributable to a State under the law of state responsibility when such actors engage in operations pursuant to the State's instructions or under the State's direction or control, or when the State later acknowledges and adopts the operations as its own. Thus, as a legal matter, States cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies. When there is information—whether obtained through technical means or all-source intelligence—that permits a cyber act engaged in by a non-State actor to be attributed legally to a State under one of the standards set forth in the law of

> state responsibility, the victim State has all of the rights and remedies against the responsible State allowed under international law.[53]

This broad statement mirrors the Tallinn Manuals. Indeed, it closely tracks with Rule 17 of *Tallinn Manual 2.0* "Attribution of cyber operations by non-State actors,"[54] which makes sense given the law of State responsibility is well settled as a matter of international law.[55] Also of note is the position that the victim State can use "all of the rights and remedies" under international law.[56] This means that the US reserves the right to use military force to counter a cyber-attack conducted by non-State proxy hackers.[57]

Effective Control and Due Diligence

As mentioned above, and as Brian Egan reiterates, the international law that governs States responsibly for proxy hackers is premised either because they are operating as a State organ or that the State exercises effective control over the proxy under the international law of attribution.[58] This term "effective control" has also been called "direction and control" in other contexts.[59] If a State exercises effective control over the proxy, then it assumes responsibility for the actions of the proxy in international law. This rule of effective control predates the Internet, and comes from the 1986 International Court of Justice (ICJ) case of *Nicaragua v. United States of America*.[60] That case, stemming from the Iran-Contra affair, resulted in the Nicaraguan government holding the US legally responsible for military and paramilitary Contras activities based on the "effective control" the US exercised over the Contras.[61]

Even absent a proxy acting under the effective control of a State or acting as an organ of the State, a State may still be held responsible under international law for supporting or enabling the proxy.[62] The type of support varies, but could include providing software, monetary incentives, or even sanctuary from prosecution under domestic laws.[63] Failing evidence of attribution of support or enabling behavior by a State, a State likely cannot be held responsible for the actions of the proxy hackers.[64]

However, the international law principle of due diligence may provide another avenue for holding a State responsible for the actions of proxy hackers. Due diligence, as discussed above and in *Tallinn Manual 2.0,* generally requires a State to take action both to prevent their territory and infrastructure from being used to launch cyberspace operations against another State, and to take feasible actions to stop such cyberspace operations if aware of them.[65] Due diligence does not require a nation to prevent cyberspace operations, just to stop once it becomes aware.[66] If State A knows that proxy hackers are using State B infrastructure to launch cyberspace operations against State A, and State A informs State B of these operations, then State B is duty-bound to stop the proxy hackers, if feasible. If State B refuses or is unable to stop the proxy hackers, then State A can take reasonable countermeasures to end those cyberspace operations. State A's countermeasures against State B would normally violate international law, but due to State B's failure or refusal to act, these countermeasures become lawful.[67]

Applying the due diligence principle can be complicated because its parameters often depend upon the capabilities of both the victim State and the perpetrating State. Due diligence for the US means a fairly high standard, while due diligence for other States without as much cyberspace sophistication "migrate the standard downward."[68] Applying the same standard to a country with minimal cyberspace infrastructure would not work in the international law context. However, States like Russia might take advantage of this lower standard. One common hacker scheme to conceal attribution is the short-term leasing of servers in various countries, including the US, from which to launch cyberspace operations. Once the operation concludes, and long before attribution is established, the hacker terminates the lease and relocates, making attribution even tougher.[69] This leasing scheme can render due diligence very difficult, if not impractical, particularly in States of modest sophistication.

Other International Laws and Norms

To reiterate, typically victim States do not employ military force to counter hackers, but rely instead on criminal prosecution, which has become an international norm. For example, the US has indicted proxy hackers in the past, as has Estonia. The US indicted Alexsey Belan three times for proxy attacks, most notably for hacking 500 million Yahoo accounts in 2012-2013.[70] Estonia charged and convicted one Estonian student from Russia, Dmitri Galushkevich, with targeting a political party website related to the 2007 cyber-attack,[71] and there are other high-profile indictments of note.[72] Again, absent effective extradition, holding Russia accountable for proxy hackers can be futile.[73] Indeed, Alexsey Belan remains at large and on the FBI's most wanted list.[74]

Other norms that have developed over time include the use of sanctions to deter hackers. On December 29, 2016, along with the indictments noted above, the US imposed sanctions on Belan,[75] under Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," as amended by Executive Order 13757, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," signed on December 28, 2016.[76] These sanctions froze Belan's assets, along with the assets of another individual, Evgeniy Bogachev.

In addition to these measures, several high-profile legal advisors recommend a slow and steady approach to building international norms in cyberspace. Colonel (Ret.) Gary Corn, former USCYBERCOM Staff Judge Advocate, recommends that States not prematurely support international laws and norms in cyberspace, because nefarious actors will attempt to exploit States that artificially limit their cyberspace operations in support of these not yet fully developed laws and norms.[77] Brigadier General George Smawley recommends a gradual shaping of international norms to tackle the problem of proxy hackers.[78] Major General Berger urges a deliberate process in building norms *lex lata* (what the law is) without ceding to the international community pressure to build law *lex ferenda* (what the law should be).[79] The alternative approach would be to establish an international commission and attempt to create a

Hague treaty or a new Geneva Convention to govern cyber law. This approach, in the absence of more fully developed international norms would suffer from a lack of consensus. Indeed, even the IGE representatives who drafted the Tallinn Manuals do not always agree on the rules.[80] Even the definition of sovereignty has led to disagreements between the US and its closest allies and partners, let alone between the US and its adversaries, such as Russia.[81]

Colonel (Ret.) Gary Brown, USCYBERCOM's first Staff Judge Advocate, recommends the US make clear its *opinio juris* (opinion of law) regarding how international law should govern cyberspace activities.[82] That "line in the sand" approach could advance development of international law and norms. Colonel (Ret.) Brown views the Tallinn Manuals as "a starting point from which to deviate" in this regard.[83]

Review of Recent Proxy Hacker Events

To better understand some of the challenges of applying international law to proxy hackers, examples are summarized below.

Estonia

In 2007, Estonia suffered one of the first well-documented cyberspace operations. Early that year, the Estonian government planned to move a statue from the center of Tallinn, the Estonian capital, to a military cemetery on the outskirts of town. This Soviet Union-era statue, originally called the "Monument to the Liberators of Tallinn," but now known as the "Bronze Soldier," honored the Soviet defeat of the Nazis in Estonia in 1944.[84] The statue was controversial. Ethnic Estonians viewed the statue as a reminder of the harsh Soviet occupation from 1944 until the fall of the Soviet Union, while ethnic Russians living in Estonia saw it as a monument to victory over the Nazis and the Soviet claims on Estonia.[85] The planned statue move offended many Russians living in Estonia and offended senior officials in Russia. Sergei Lavrov, Russian Foreign Minister, threatened, "[Removal of the memorial and the ensuing clashes] is disgusting. ... There can be no justification for this blasphemy. It will have serious consequences for our relations with Estonia."[86]

After the statue was moved, Russia launched a coordinated distributed denial of service (DDOS) operation, targeting the Estonian government itself, including "the President, Parliament, police, political parties, and major media outlets."[87] This DDOS lasted over three weeks and cost Estonia billions of euros.[88] The operation appeared to come from patriotic hackers sympathetic to Russia.[89] Estonia charged and convicted one Estonian student from Russia, Dmitri Galushkevich, with targeting a political party website.[90] Yet, further attribution for the DDOS operation remained elusive. Some of the sources of the operation appeared to be in Transnistria, a pro-Russian breakaway republic situated between Moldova and Ukraine, and some Russian officials claimed responsibility for the DDOS.[91] Officially, Russia denied involvement, even claiming they too were victims of the DDOS operation.[92]

This DDOS operation, combined with other physical measures implemented by Russia, had a devastating impact on Estonia. At the same time as the cyberspace operation, Russia severed rail line traffic with Estonia for "repairs."[93] The DDOS operation also threatened to undermine public confidence in Estonia's government, particularly when loss of access to banking services occurred for several hours.[94] Finally, the operation appeared tailored to avoid triggering Article V of the NATO Treaty, the collective defense provision that renders "attack against one . . . shall be considered an attack against them all."[95] Estonia would have had difficulty describing how a DDOS operation qualified as an armed attack under this provision. While it caused losses and created confusion, such an attack does not cross the "threshold for reprisals."[96]

These cyberspace operations prompted NATO and Estonia to enhance their defenses. First, Estonia hardened its cyberspace defenses in light of this operation.[97] Second, NATO recognized and certified the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn in 2008.[98] Finally, the NATO CCD COE invited the International Group of Experts (IGE) in 2009 to create the first of two Tallinn Manuals (discussed earlier in this paper).

The primary principle of international law that could have been applied to hold Russia accountable for the DDOS attack was due diligence. While specific attribution remained elusive, Estonia built a compelling factual case that only Russian-backed proxy actors could have launched the DDOS attack.[99] This was true even if the Russian government did not specifically direct the proxy hackers. Additionally, the hackers that facilitated the DDOS attack from Transnistria could have been identified as mercenaries.[100] As a result, they could have faced criminal prosecution for their actions, assuming extradition would have allowed Estonia to gain jurisdiction over those proxy hackers.[101] Claiming combatant immunity under international law obviously would be non-availing for the hackers.

Georgia

The 2007 attack on Estonia was just the start of Russia's large-scale proxy cyberspace operations. In 2008, Russia invaded South Ossetia in Georgia. Simultaneously, a DDOS operation began against "fifty-four news, government, and financial websites" impacting "thirty-five percent of Georgia's Internet networks."[102] The National Bank of Georgia "had to suspend all electronic services" for eleven days due to the attacks.[103]

As with the Ukrainian example discussed at the beginning and again below, Russia launched these cyberspace-operations as part of its information warfare campaign. By disabling and disrupting the Georgian government's ability to communicate with its people, Russia was able to fill the void with its own false narrative of the invasion and falsely claim legal legitimacy.[104] This false narrative did not fool international third-parties as to Russia's claims on South Ossetia, but it did temporarily sow doubts about Russia's invasion at the local level.[105]

Proxy hackers conducted most of these operations against Georgia. Motivated in part by patriotism, these hackers received marching orders through hacker forums which provided "tools, vulnerabilities, and target lists" for the hackers to use.[106] Russia denied directing these proxy hackers, but these denials strain credulity when the timing and nature of these operations coincided with Russia's invasion of South Ossetia.[107]

Russia was clearly responsible under international law for the proxy hackers' cyber-attacks on Georgia. Apart from the telltale timing coinciding with the invasion, the presence of hacker forums that supplied tools and target lists proves Russia's control over these hackers beyond any rational doubt.

Ukraine

Russia learned from its experiences in Estonia and Georgia when launching its operations against Ukraine in 2014. Coinciding with Russia's invasion of Crimea, Ukraine faced a massive DDOS operation 32 times the size of the attacks on Georgia.[108] Apart from the sheer scale, what made this DDOS operation different was Ukraine's deployment of proxy hackers to counter by hacking Russian interests, who succeeded in defacing the Russia Today website, replacing the word Russia with Nazi.[109]

These DDOS operations made up just one portion of the cyberspace operations conducted by both Russia and Ukraine over a period of several years. As noted above, Russia employed dozens of proxy trolls to engage in information warfare in support of their operations in Ukraine in 2014.[110] These cyberspace operations continued throughout 2015, when Russian cyber-attacks disabled the Ukrainian power grid for several hours.[111] Later investigations revealed that the malware that disabled the grid was intended to physically damage it.[112] Normally only State governments have the resources to develop this type of cyber weapon, as evidenced by the Stuxnet cyber-attack against Iran.[113] In October 2020, the US indicted six persons for the power grid attack in Ukraine. All six indicted individuals work as officers of Russia's GRU military intelligence agency.[114] Proxy hackers rarely will have access to such a dangerous type of cyber weapon.[115] Among other take aways, the tit-for-tat cyberspace operations in Ukraine, with both proxy and non-proxy means, underscores the challenge of properly identifying cyber-attackers.

Under international law, the DDOS operation against Ukraine mirrored the Russian efforts in Georgia. Russia continued to exercise effective control over the proxy hackers and coordinated the operation to coincide with its invasion of Crimea. Separately, the sophisticated power grid cyber-attack could not have come from any source without direct Russian government involvement, as evidenced by the US indictment tying six Russian officials to the attack.

In March of 2022, Ukraine struck back with massive proxy attacks of its own, with over 300,000 people known as the "IT Army of Ukraine" working to disrupt the Russian government.[116] This group "has organized . . . distributed denial of service attacks on Russian

state websites," and attempted to inform the Russian people "about what is actually going on in Ukraine."[117]

Proposed Actions to Counter Future Russian Proxy Hackers

Several theories of strategy formulation could help the US develop a policy to counter future Russian proxy hackers, coercion theory remains the most relevant and applicable. As analyzed below, this theory allows the US to gradually escalate measures against Russia in a manner that complies with international laws and norms.

Coercion Theory

Coercion theory has two main methods, both of which have importance when countering proxy hackers. The first method, deterrence, seeks to use threats to prevent an actor (State or non-State) from taking an action it might otherwise take.[118] Deterrence threats can be threats of punishment or threats of denial.[119] The threat of denial seeks to deter by convincing the target state that it will not achieve its aim (that the aim will be denied).[120] The threat of punishment seeks to deter by convincing an actor that the coercer will inflict retaliatory punishment that exceeds the value of the desired stake.[121] In the case of cyber, deterrent threats can be used to dissuade actors from engaging in hacking and cyber-generated disruption of all forms.

Actors can be deterred for many reasons, thus allowing "enemies who have been deterred to save face," because the reasons behind a successful deterrence remain unclear.[122] The coercive threat might have caused the deterrent effect, or maybe something else entirely, which allows a State to attribute the reason they failed to act on whatever they can plausibly claim.[123]

The second method, compellence, seeks to force the target State to perform an act it would otherwise prefer not to perform, or to cease an act it has already started.[124] Because successful compellence forces the actor to take an action it would prefer not to take, there is no ambiguity or ability to save face. Actors typically do not want to be humiliated; they will seek therefore to evade or resist compellent threats. Other inherent challenges also make successful compellence difficult. First, timing is important. There must be a deadline that allows sufficient time for the target State to act, but at the same time places it on notice that consequences will occur by that deadline if no action has taken place.[125] Second, the coercing state "must convey specific information to the actor being coerced."[126] Without that specificity, compellence will fail.

Despite its drawbacks, coercion theory remains a useful framework for dealing with US adversaries. By structuring a chain of escalatory threats and actions tethered to international law, the US can succeed in deterring or terminating adverse cyberspace operations.

Defend Forward and Persistent Engagement

In 2018, the US released the Department of Defense Cyber Strategy. One key provision,

"Persistently contest malicious cyber activity in day-to-day competition," referred to as the "persistent engagement" or "defend forward" policy, has come to define USCYBERCOM operations.[127] The goal of defend forward is "the use of Defense Department cyber capabilities during day-to-day competition to disrupt or halt malicious cyber activity at or as close as practicable to its source."[128] Deterrence was not the specific goal of defend forward, but "[t]o the extent that defend forward contributes to deterrence, it does so incidentally by improving overall defense, reducing the likelihood of adversary operational success, and thereby constraining the adversary's strategic options and resetting its benefit calculus."[129]

One way that defend forward constrains the enemy, and imposes costs on proxy hackers, is USCYBERCOM's "practice of uploading malware samples to the VirusTotal website that are discovered through persistent engagement's routine operations and campaigns."[130] Brig. Gen. Smawley agreed that imposing direct costs on proxy hackers works.[131] He described a typical defend forward operation, done with the consent of the host State, where the cyber operators search for malware and then publicly advertise the capture of the malware through cooperation with the Department of Homeland Security (DHS), which typically tweets about the operation.[132] This causes public shaming of the hacker amongst his or her peers, and it makes worthless the money and time the hacker invested in the malware. The latter becomes worthless once DHS shares information with commercial entities that then patch systems to prevent the malware from working.[133]

Recommendations

The US can and should use both deterrence and compellence to counter the threat from Russian proxy hackers. Both methods follow existing international law and norms to counter a threat. First, the US can seek to deter actions, or compel Russia to cease ongoing operations, by threatening to expose and publicly attribute its proxy hackers' malicious cyberspace activities to Russia. This public attribution, backed with hard evidence of Russian involvement, can cause embarrassment to Russia in the international community. While the US has already attempted this public attribution several times in the past, such as with Alexsey Belan, some critics have noted the absence of hard evidence linking Russia to the proxy.[134] Whether or not there is hard evidence, Russia inevitably will continue to falsely claim innocence, and/or claim as they did in Estonia in 2007 to be a victim of the same attacks.[135] But calling Russia out will take a toll.

And when the threat of public embarrassment fails to deter Russia from using proxy hackers, the US should consider an escalatory campaign using all elements of national power – Diplomatic, Information, Military, and Economic (DIME). Any communicated threat that does not achieve the desired result should be followed by increasingly coercive actions to compel Russia to cease their use of proxy hackers. For example, diplomatic efforts should include specific threats of actions to be taken by a certain date if Russia does not take concrete and verifiable actions to stop proxy hackers. The specific threats could start with strong

economic sanctions and later progress to a proportional use of military force. This effort at compellence comes with definite risks of escalation, and should the US fail to back up the effort to compel with actions, Russia would then gain the upper hand because the threat of such actions would ring hollow in the future.

The table below depicts one possible progression of efforts to deter proxy hackers backed by State adversaries:

Table 1. Progression of Coercive Efforts.136

Phases	Phase 1	Phase 2	Phase 3	Phase 4
Possible US Deterrent Threats or Compellent Actions	• Public attribution of attacks backed by hard evidence • Diplomatic conversations with specific future actions and timelines	• Criminal prosecution of proxy hackers • Sanctions against Russian Government Officials and all known hackers	• Preliminary cyberspace operations against Russian interests backed by public statements • Military assets aligned against the Russian interests as a show of force	• Serious offensive cyberspace operations against Russian interests backed by public statements • Military force used against Russian cyber infrastructure
International Law or Norm Applicable	• *Tallinn Manual 2.0* Rule 17, Attribution of Cyber Operations by Non-State Actors[137] • International Norm	• *Tallinn Manual 2.0* Rule 13, International Cooperation in Law Enforcement[138] • International Norm	• *Tallinn Manual 2.0* Rule 20, Countermeasures, (General Principle)[139] • *Tallinn Manual 2.0* Rule 71, Self-Defence against Armed Attack[140] • International Norm	• *Tallinn Manual 2.0* Rule 23, Proportionality of Countermeasures[141]; • *Tallinn Manual* 2.0 Rule 20, Countermeasures, (General Principle)[142] • *Tallinn Manual 2.0* Rule 71, Self-Defence against Armed Attack[143]

The US can take additional steps where appropriate, but with the same desired effect; that is, a coerced Russia that is both deterred from supporting future proxy hacker attacks and compelled to stop proxy hackers from launching attacks from Russia.

Coercion has successfully worked in the past. One example from a real-world operation came after the downing of a $150 million drone by Iran in 2019.[144] The US could arguably have responded with a kinetic armed response under the UN Charter, Article 2(4), which states "All members shall refrain in their international relations from the threat of force or the 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."[145] This article is usually invoked by States as the right to self-defense. However, the US responded with non-kinetic cyberspace operations instead.[146] While this bypassed lower steps in the recommended deterrence or compellence actions, it shows the flexibility of coercion theory. It also illustrates application of the principle of proportionality: as noted in the reference, Iran's attack on the drone did not lead to a loss of life, but an armed attack against the missile base that shot down the drone almost surely would have. In other words, depending on the severity of the attack, a nation could skip directly to military force under a theory of self-defense, but proportionality may well indicate a better course of action.

CONCLUSION

As a leader in cyberspace operations, the US should, whenever possible, openly and transparently call Russia out for its flagrant violations of international law and norms and its support of proxy hackers. Absent public efforts by the US, Russia and other adversaries will continue to be emboldened to leverage proxy hackers. Unchecked, proxy hacking attacks will further undermine the rule of law in cyberspace and increasingly threaten if not cause irreparable harm to the international community. Unabated, proxy hacker attacks will spread disinformation, undermine public confidence in governments and diminish the ability of countries to maneuver freely in cyberspace.

The US should prioritize efforts to continue to defend forward and impose costs on proxy hackers and their supporters. Meanwhile, specific application of deterrence and compellence theories against proxy hacker efforts by Russia, combined with an effort to further develop international law and norms will help combat the problem. Over time, the use of proxy hackers may diminish under the pressure of such sustained efforts by the US and its partners.

NOTES

1. Harold Hongju Koh, State Department Legal Adviser, "International Law in Cyberspace" (lecture, USCYBERCOM Inter-Agency Legal Conference, Fort Meade, MD, September 18, 2012), http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/.
2. Thomas Deen, "Russian Expansion and the Development of Hybrid Warfare," *War Room* (blog), United States Army War College, November 24, 2020, https://warroom.armywarcollege.edu/articles/russian-expansion/.
3. Deen, "Russian Expansion and the Development of Hybrid Warfare."
4. Ibid.
5. Ibid.
6. Ibid.
7. Ionut Ilascu, "Ransomware gangs, hackers pick sides over Russia invading Ukraine," *Bleeping Computer,* February 25, 2022, https://www.bleepingcomputer.com/news/security/ransomware-gangs-hackers-pick-sides-over-russia-invading-ukraine/.
8. Bill Toulas, "Russian hackers start targeting Ukraine with Follina exploits," *Bleeping Computer,* June 13, 2022, https://www.bleepingcomputer.com/news/security/russian-hackers-start-targeting-ukraine-with-follina-exploits/.
9. *Merriam-Webster Dictionary*, s.v. "proxy," accessed February 15, 2021, https://www.merriam-webster.com/dictionary/proxy.
10. Tim Maurer, "'Proxies' and Cyberspace," *Journal of Conflict & Security Law* 21, no. 3 (2016): 387.
11. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013), Rule 6, 29.
12. *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Rule 6, Commentary note. 2., 29.
13. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, Commentary note. 10, 32.
14. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, Commentary note. 11, 33.
15. Ibid.
16. Michael N. Schmitt and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017), Rule 17, Commentary n. 9, 97.
17. Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, UK: Cambridge University Press, 2018), 76-78.
18. Maurer, 76-78.
19. Major General Joseph Berger, telephonic interview by author, February 9, 2021.
20. Brigadier General George R. Smawley, telephonic interview by author, February 9, 2021.
21. Smawley, interview. The fourth category, criminal organizations, falls outside of USCYBERCOM's jurisdiction, barring a nexus to Violent Extremist Organizations (VEOs) or an operation directed against the Department of Defense Information Network (DODIN). Criminal organizations are handled primarily by the Department of Homeland Security (DHS).
22. U.S. Senate Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views, 116th Cong., 1st sess., 2018, S Rep. 116-290, 18-19.
23. Select Committee on Intelligence, 20.
24. Ibid, 21.
25. Ibid, 21.
26. Berger, interview.
27. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, title page.
28. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* 3.
29. *Tallinn Manual 2.0*, 1-2.
30. *Ibid,* 3.
31. Eric Geller, "U.S. Charges Russian Hackers with Sweeping Campaign of Cyberattacks," *Politico,* October 19, 2020, https://www.politico.com/news/2020/10/19/russia-hackers-cyberattacks-430166. NATO Report, 2007 *Cyber Attacks on Estonia,* NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/hybrid-threats-2007-cyber-attacks-estonia, 61.

NOTES

32. See discussion accompanying notes 35 and 71 below regarding extradition rules and the case of Alexsey Belan, whom Russia has not extradited to the United States.
33. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 13, 75.
34. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Rule 13, 75.
35. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Rule 13, Commentary note. 8, 77.
36. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 14, 84.
37. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 14, Commentary note. 1, 84.
38. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 14, Commentary note. 5, 85.
39. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 94.
40. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* 94.
41. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Table of Concordance, xxxviii-xli.
42. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 6, 30.
43. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 6, 30.
44. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 6, 30.
45. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Rule 7, 43.
46. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Rule 7, Commentary note. 14, 46.
47. Martin Libicki, "Setting International Norms on Cyberwar Might Beat a Treaty," *US News & World Report*, June 8, 2012, https://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/setting-international-norms-on-cyberwar-might-beat-a-treaty.
48. For example, Convention (III) Relative to the Treatment of Prisoners of War, Geneva, August 12, 1949, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/375?OpenDocument.
49. Martin Libicki, "Correlations Between Cyberspace Attacks and Kinetic Attacks," *12th International Conference on Cyber Conflict* (Tallinn, Estonia: NATO CCDCOE Publications, 2020), 204, https://ccdcoe.org/uploads/2020/05/CyCon_2020_11_Libicki.pdf.
50. Brian J. Egan, State Department Legal Adviser, "Remarks on International Law and Stability in Cyberspace" (lecture, Berkeley Law School, Berkeley, CA, November 10, 2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.
51. Elena Chernenko, "Russia Warns against NATO Document Legitimizing Cyberwars," *Russia Beyond,* May 29, 2013, https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html.
52. Chernenko.
53. Brian J. Egan, State Department Legal Adviser, "Remarks on International Law and Stability in Cyberspace" (lecture, Berkeley Law School, Berkeley, CA, November 10, 2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.
54. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rule 17, 94.
55. Trevor McDougal, "Establishing Russia's Responsibility for Cyber-Crime Based on Its Hacker Culture," *Brigham Young University International Law & Management Review* 11, no. 2 (August 1, 2015): 67, https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1129&context=ilmr.
56. Brian J. Egan, State Department Legal Adviser, "Remarks on International Law and Stability in Cyberspace" (lecture, Berkeley Law School, Berkeley, CA, November 10, 2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.
57. Libicki, "Correlations Between Cyberspace Attacks and Kinetic Attacks."
58. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, Commentary note. 10, 32.
59. Compare *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 6, Commentary note. 10, 32 (effective control) with *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 17, 94 (direction and control).
60. International Court of Justice, Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America), Judgment of June 27, 1986, para. 292, 136.
61. Nicaragua v. United States of America, para. 1, 16.

NOTES

62. Colonel Gary Corn, U.S. Army Retired, telephonic interview by author, February 3, 2021.
63. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 17, Commentary note. 9, 97.
64. Corn, interview.
65. Corn, interview. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Rule 6, 30, and Rule 7, 43.
66. Corn, interview.
67. Corn, interview. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 20, 111.
68. Colonel Gary Brown, U.S. Air Force Retired, telephonic interview by author, January 29, 2021.
69. Smawley, interview.
70. "Most Wanted," Federal Bureau of Investigation, last modified March 15, 2017, https://www.fbi.gov/wanted/cyber/alexsey-belan.
71. NATO Report, 61.
72. Geller.
73. See discussion accompanying note. 35 above.
74. "Most Wanted."
75. US Department of the Treasury, "Sanctions Actions Pursuant to Executive Order 13694," *Federal Register* 82, no. 3 (December 29, 2016): 1424, https://www.govinfo.gov/content/pkg/FR-2017-01-05/pdf/2016-32017.pdf.
76. Barack Obama, Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," *Federal Register* 80, no. 63 (April 2, 2015): 18077, https://www.govinfo.gov/content/pkg/FR-2015-04-02/pdf/2015-07788.pdf. Barack Obama, Executive Order 13757, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," *Federal Register* 82, No. 1 (January 3, 2017): 1, https://www.govinfo.gov/content/pkg/FR-2017-01-03/pdf/2016-31922.pdf.
77. Corn, interview. For example, the IGE has already begun work on a new Tallinn Manual 3.0. The provisions from that new Manual might change or influence State practice. The website announcement specifically states, "The comprehensive 2017 edition will be updated in the light of emerging State practice," showing that the law is still evolving. "CCDCOE to Host the Tallinn Manual 3.0 Process," CCDCOE, last accessed on March 14, 2021, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.
78. Smawley, interview.
79. Berger, interview.
80. For example, the IGE could not agree on whether a State must disclose "evidence on which attribution is based whenever taking actions in response to cyber operations that purportedly constitute an internationally wrongful act." *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Commentary note. 13, 83.
81. Smawley, interview.
82. Brown, interview.
83. Ibid.
84. NATO Report, 53. Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News, April 27, 2017, https://www.bbc.com/news/39655415.
85. NATO Report, 56, 58.
86. NATO Report, 58. Other writers have compared the controversial nature of the "Bronze Soldier" statue to that of Confederate statues in the United States. Andrew Stuttaford, "Confederate Statues and the Bronze Soldier of Tallinn," *National Review,* August 17, 2017, https://www.nationalreview.com/corner/confederate-statues-and-bronze-soldier-tallinn/.
87. NATO Report, 55.
88. NATO Report, 53.
89. NATO Report, 59.
90. NATO Report, 61.
91. NATO Report, 61.
92. NATO Report, 53, 58-59.

NOTES

93. NATO Report, 53.
94. NATO Report, 61.
95. Article V reads, in part:

    > The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

    The North Atlantic Treaty, Washington, DC, April 4, 1949, art. 5.
96. NATO Report, 68.
97. NATO Report, 67.
98. NATO Report, 67.
99. NATO Report, 69.
100. *Tallinn Manual 2.0,* "Mercenaries" (Rule 90), states, "Mercenaries involved in cyber operations do not enjoy combatant immunity or prisoner of war status." *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Rule 90, 412. This means that any proxy hacker acting under color of authority from a State cannot avoid prosecution for its actions under international law, if they meet the six-part test from Article 47 of Additional Protocol I to the Geneva Conventions. That six-part test consists of:

    > A mercenary is any person who: (a) is specially recruited locally or abroad in order to fight in an armed conflict; (b) does, in fact, take a direct part in the hostilities; (c) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party; (d) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict; (e) is not a member of the armed forces of a Party to the conflict; and (f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.

    Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, art. 47, Mercenaries, https://ihl-databases.icrc.org/ihl/WebART/470-750057.
101. See discussion accompanying note. 35 above.
102. Sarah P. White, "Understanding Cyber Warfare: Lessons from the Russia-Georgia War," *Modern War Institute*, 1, https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.
103. White, 1.
104. Ibid 4.
105. Ibid, 5.
106. Ibid, 6.
107. David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* 2, January 6, 2011, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.
108. Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," *NBC News*, December 18, 2016, https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.
109. Pierluigi Paganini, "Crimea – The Russian Cyber Strategy to Hit Ukraine," *INFOSEC*, March 11, 2014, https://resources.infosecinstitute.com/topic/crimea-russian-cyber-strategy-hit-ukraine/.
110. Deen.
111. Andy Greenberg, "New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction," *Wired*, September 12, 2019, https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.
112. Greenberg.
113. Josh Fruhlinger, "What Is Stuxnet, Who Created It and How Does It Work?" *CSO Online*, August 22, 2017, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

NOTES

114. Geller.
115. David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 26, 2013, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
116. Christopher Hutton, "'IT Army of Ukraine: 300,000 hackers work together to fight Russia online," *Washington Examiner*, March 15, 2022, https://www.washingtonexaminer.com/news/it-army-of-ukraine-300-000-hackers-work-together-to-fight-russia-online.
117. Hutton.
118. Tami Davis Biddle, "Coercion Theory: A Basic Introduction for Practitioners," *Texas National Security Review* 3, no. 2 (Spring 2020): 98, https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/.
119. Biddle, 101.
120. Ibid, 101.
121. Ibid, 101.
122. Ibid, 102.
123. Ibid, 102.
124. Ibid, 98-99.
125. Ibid, 102.
126. Ibid, 102.
127. Department of Defense, Cyber Strategy, 2018, 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
128. Gary Corn, "SolarWinds Is Bad, but Retreat From Defend Forward Would Be Worse," *Lawfare,* January 14, 2021, https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.
129. Corn.
130. Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect," *Lawfare*, February 6, 2020, https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.
131. Smawley, interview.
132. Ibid.
133. Ibid.
134. Roger A. Grimes, "Why It's So Hard to Prosecute Cyber Criminals," *CSO Online*, December 6, 2016, https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html.
135. NATO Report, 53, 58-59.
136. Table created by author.
137. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Rule 17, 94.
138. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 13, 75.
139. Rule 20 states, "A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that is owed by another State." *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Rule 20, 111.
140. Rule 71 states, "A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inher*ent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effect." Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 71, 339.
141. Rule 23 states, "Countermeasures, whether cyber in nature or not, must be proportionate to the injury to which they respond." Tallinn Manual 2.0 on the I*nternational Law Applicable to Cyber Operations,* Rule 23, 127.
142. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 20, 111.
143. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Rule 71, 339.
144. David Martin and Grace Segers, "Trump Approved Cyber Attacks against Iran, Sources Say," *CBS News*, June 23, 2019, https://www.cbsnews.com/news/pentagon-launched-cyber-attacks-against-iran-with-trumps-backing-sources-say/.

NOTES

145. United Nations Charter, Article 2(4), San Francisco, CA: United Nations, June 26, 1945, https://www.un.org/en/charter-united-nations/.

146. Martin and Segers.