Over 30 countries are pursuing offensive cyber capabilities, Director of U.S. Intelligence James Clapper testified in 2016.¹ That’s a fivefold increase compared to only six years earlier when the U.S. Department of Defense declared cyberspace a new operational domain and experts still counted only some half a dozen states in the exclusive club.² To project cyber power, these states rely on hackers that do not wear uniforms and are not part of the intelligence community—cyber mercenaries or, more broadly, cyber proxies. For example, the largest data breach in history, the Yahoo hack compromising all of its three billion email accounts, was allegedly the work of modern-day privateers, namely a 29-year old wanted Russian cybercriminal and a 22-year old Canadian working together with two members of Russia’s intelligence service, the FSB.³ In March 2018, the U.S. government unsealed an indictment and issued sanctions against nine Iranian hackers tied to the Islamic Revolutionary Guard Corps (IRGC) allegedly responsible for hacking and stealing data from over 300 universities and private companies in more than 20 countries as well as government agencies.⁴

The definition of cyber proxies is based on gaining unauthorized access or carrying out distributed denial of service attacks against computer systems. It excludes actors that place content such as WikiLeaks’ publication of confidential or secret material or the Internet trolls of the Internet Research Agency in St. Petersburg. Both types of actors deserve attention, specifically by governments of liberal democracies, but they are conceptually different as the latter carry out actions


Copyright © 2018 The Elliott School of International Affairs
The Washington Quarterly • 41:2 pp. 171–188
https://doi.org/10.1080/0163660X.2018.1485332

THE WASHINGTON QUARTERLY • SUMMER 2018 171
that are forms of propaganda and information operations, whereas cyber proxies engage in hacking and other types of offensive cyber operations.

There are several reasons why these cyber proxy relationships exist. First, most states are struggling to attract the quantity and quality of talent required to fill the ranks of the newly established cyber commands or units. Relying on hackers only from time to time or through more informal arrangements can help narrow the gap. Second, relatedly, some evidence suggests that these non-state hackers are part of the reason why states have been able to achieve much more disruptive effects much faster than was commonly expected. For example, when four Iranians in their mid-twenties joined the campaign of three others with ties to the IRGC, it turned the campaign from “a few yapping Chihuahuas into a pack of fire-breathing Godzillas” in the words of The New York Times. Also, engaging hackers through nebulous arrangements is a manifestation of the revival of “plausible deniability” more broadly alongside “little green men” taking over Eastern Ukraine and murders with chemical agents that are difficult to trace.

These proxy relationships between states and hackers detached from the state matter for a variety of reasons. Chief among them are the implications for international stability. At a time when the world is inching closer toward conflict, accidents and miscalculation can have disastrous consequences. The risk is even higher during periods of significant technological change, when new pieces are introduced to the geopolitical game of chess while it remains unclear how far and how flexibly they can move and whether they can only advance or retreat. The impact of the invention of railroads and trains on the wars in Europe at the turn of the twentieth century is an oft-cited, powerful historical parallel.

The use of proxy actors introduces additional risk because of the well-known principal-agent problem. The further detached an agent from a principal’s control, the higher the risk that the agent carries out an action that the principal did not intend. This includes cyber proxies. How can their relationship with states be tightened to reduce the risk of accidental or unintentional escalation?

Before discussing what can be done to shape proxy relationships, the first part of this article outlines what cyber proxies are. The second part describes several case studies shedding light on who cyber proxies are, where and when they have been active, as well as how they have been used. The third part offers more details about why cyber proxies and their activities matter, with a specific focus on the
implications for liberal democracies. The penultimate section considers options for what to do about those on a loose leash, before concluding with implications.

What Are Cyber Proxies?

“States must not use proxies to commit internationally wrongful acts”—15 states including the United States, Russia, and China agreed to this statement in a 2013 UN report on cybersecurity without specifying what “proxies” are. This lack of specificity is emblematic of how vaguely defined the term proxies remains overall. The common theme across its use remains its Latin origin procurare, “pro” meaning “on behalf of” and “curare” meaning “to attend to; to take care of.” Therefore, cyber proxies can be defined as intermediaries that conduct or directly contribute to an offensive cyber action that is enabled knowingly, whether actively or passively, by a beneficiary.

This definition is a deliberately broad approach to conceptualizing proxies. It is designed to capture relationships where proxies are under the effective control and on a tight leash by their masters as well as proxies that receive support indirectly when a government is aware of but ignores a proxy’s activity. For example, under this definition cybersecurity contractors of the U.S. government are considered cyber proxies. The purpose is to point out that all states rely on hackers detached from the state in one form or another to project cyber power and, more importantly, to highlight that the differentiating factor is not whether a state uses a proxy or not, but how much control a state exercises over that proxy.

In other words, U.S. cybersecurity contractors are the ideal type—ideal in its aspirational sense—for how much control a state should exercise over a proxy if it chooses to use the latter. They are examples of proxies under such tight control that they physically sit next to their government counterparts at the respective agencies, thereby mitigating the inherent risks associated with such relationships from an international stability perspective.

At the other end of the spectrum, the definition is also comparatively broad by including the concept of “passive support.” The reason here is to capture behavioral patterns where states repeatedly and consistently turn a blind eye to activity considered malicious by those targeted and are unwilling yet often able to stop them. For example, the Russian government not taking action against Russian hackers accused of cybercrime by other countries—yet acting swiftly to arrest Russian hackers if they target systems in Russia—is a paradigmatic case of passive support for cybercrimes that do not work against the country’s interest.

Overall, the spectrum of proxy relationships can be divided into three main categories based on the level of control: (1) delegation—relationships in which hackers are under what international law would consider the effective control of
the state, (2) orchestration—relationships with hackers on a looser leash yet acting in concert with a government’s objectives, and (3) sanctioning—or passive support—with governments sanctioning hackers’ activity knowingly by not taking action to end that activity. Importantly, this spectrum can be applied to both a specific operation as well as to the broader model states pursue systematically in how they structure their relationships with hackers detached from the state.

Finally, the use of the term “proxy” instead of “mercenary” is deliberate to avoid implying a primarily profit-driven motivation often associated with the term “mercenary.” Hackers who have joined forces with governments often exhibit political motivations including not only hacktivists—politically-driven activists that hack—but also cyber criminals such as Vladislav Horohorin, also known as “Bad B,” who post videos describing their thefts as a patriotic undertaking. With hackers being able to reach their targets remotely, they might also be carrying out one activity during the day, driven by one motive, and another activity at night, driven by another, making intent an even more fluid concept in this field than it always has been. Also, this definition relies on an offensive cyber action being carried out. It therefore excludes actors merely developing code that could serve as a cyber weapon but is not deployed. The former is rather akin to arms dealers and the latter to mercenaries.

Who Are Cyber Proxies and What Activities Do They Engage In?

Cyber proxies have been around for nearly as long as the Internet has existed. In the late 1980s, for example, German hackers targeted systems including Lawrence Berkeley National Laboratory and sold their stolen data to the Soviet Union.11 Yet for nearly 30 years, evidence of such relationships remained scarce and mostly the subject of gossip rather than fact. That changed in the spring of 2016, when the U.S. government started unsealing several indictments, described in this section. The indictments made clear that it is indeed possible to attribute malicious activity online; in fact, they explicitly mention names and included photos of the accused. In short, the indictments provided unprecedented insight into proxy relationships between states and hackers. What used to be rumors swirling around in the secretive information security community became public accusations with detailed information collected to withstand
the scrutiny of a court process. As a result, it has become much easier to describe who cyber proxies are.

**Hacktivists Sponsored by the State: Iran**

In March 2016, for the first time ever, the U.S. Department of Justice unsealed an indictment against state-sponsored proxy hackers, namely sponsored by Iran’s IRGC. The indictment lists seven Iranian citizens, ranging from ages 23 to 37, who were part of two companies, ITSecTeam and Mersad Company. These two companies “performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps, on computer hacking charges related to their involvement in an extensive campaign of over 176 days of distributed denial of service (DDoS) attacks,” targeting SunTrust, JPMorgan Chase, CitiGroup, Wells Fargo, US Bancorp, Capital One, PNC, and HSBC among others. Responding to the incident cost these companies millions of dollars. In addition, one of the seven, Hamid Firoozi, is allegedly responsible for trying to hack the Bowman Dam, located 20 miles north of New York City in the fall of 2013.

Following the breadcrumbs in the indictment leads to an interesting connection to hacktivist groups. Three of the men—Sadegh Ahmadzadegan (also known by his online pseudonym “Nitr0jen26”), Omid Ghaffarinia (a.k.a. “PLuS”), and Nader Saedi (a.k.a. “Turk Server”)—were members of two hacker groups, the Ashiyane Digital Security Team and Sun Army. The Ashiyane Digital Security Team has been involved in political hacktivism and cyber

**Figure 1. Organizational Structure and Timeline of Hackers Mentioned in 2016 U.S. Indictment of Seven Iranian Hackers**

crime for many years. Screenshots of websites taken over by Sun Army were posted between February 17, 2010 and March 17, 2012 listing the online personas Nitr0 jen26, PLuS, and Turk Server. Importantly, the postings end in the spring of 2012, the same year that the U.S. government’s indictment accuses the hackers of beginning their involvement in the malicious activity targeting U.S. financial institutions as shown in Figure 1:

In short, this proxy relationship between Mersad Company and the Iranian government illustrates the more general descriptions of the Iranian government’s efforts to build and project coercive cyber power leveraging hackers detached from the state targeting foreign companies, foreign governments, as well as dissidents at home and abroad. The structure and evolution of the malicious activity between December 2011 and May 2013 fits this description, especially since another hacker mentioned in the indictment “provided training to Iranian intelligence personnel,” also highlighting their influence on the state’s own capabilities.

In Support of the State: Syrian Electronic Army

In March 2016, the U.S. Department of Justice also unsealed an indictment against three members of the Syrian Electronic Army. The Syrian Electronic Army first established a Facebook presence in April and May 2011, describing itself as “a group of enthusiastic Syrian youths who could not stay passive towards the massive distortion of facts about the recent uprising in Syria.” The group launched DDoS attacks against media organizations seen as critical of the Assad regime and targeted Assad opponents with spyware that “coupled with geo-location services … puts those targets at risk of kinetic [i.e. active physical] attack.” In other words, the information gathered through hacking could be used to arrest, potentially torture or otherwise target opponents.

According to the indictment, rather than being “sponsored” by the Syrian government, two of the three acted “in support of the Syrian Government and President Bashar al-Assad.” The third, Peter (a.k.a. Pierre) Romar, stands out because unlike the other two, who are believed to reside in Syria, he was living in Germany until his extradition to the United States in May 2016. In addition, John Carlin, U.S. Assistant Attorney General for National Security at the time, pointed out that, “While some of the activity sought to harm the economic and national security of the United States in the name of Syria, these detailed allegations reveal that the members also used extortion to try to line their own pockets at the expense of law-abiding people all over the world.” This included, for example, stealing data from companies and exhorting them for money.

The two men believed to be in Syria also made headlines when they managed to hijack the Twitter account of the Associated Press. They then posted a tweet with the fake announcement of an explosion at the White House injuring President
Obama. The Dow Jones Industrial subsequently plunged by 100 points and wiped US$136 billion from the S&P 50 index before bouncing back shortly thereafter. While the technique used was simple, the effect they caused was nevertheless enough for them to be added to the list of the FBI’s Cyber Most Wanted.

The State/Crime Nexus: Russia
In March 2017, the U.S. government unsealed a new indictment accusing three Russian citizens living in Russia, including two FSB officers, as well as a Canadian national residing in Canada to be responsible for the largest data breach in history (to date): the Yahoo hack. The two FSB officers—Igor Anatolyevich Sushchin (43), and Dmitry Aleksandrovich Dokuchaev (33)—worked with the Russian citizen Alexsey Alexseyevich Belan (29), also known as “Magg”; and the Canadian, Karim Baratov (22), also known as “Kay,” “Karim Taloverov” and “Karim Akehmet Tokbergenov.” According to the indictment, the two FSB officers “protected, directed, facilitated and paid [the] criminal hackers to collect information through computer intrusions in the United States and elsewhere.” The organizational structure of the hacking is illustrated in Figure 2.

The two non-FSB members are essentially modern-day privateers. Belan had been on the FBI’s Cyber Most Wanted criminals list since November 2013. He was arrested in Europe in June 2013 but managed to escape to Russia. In spite of Interpol issuing a Red Notice for his arrest in July 2013, the Russian government refused to arrest him and instead “used him to gain unauthorized access to Yahoo’s network.” The FSB officers provided Belan with information to “avoid detection by US and other law enforcement agencies outside Russia, including

Figure 2. Organizational Structure and Timeline of Hackers Mentioned in March 2017 U.S. Indictment of Russian Hackers

information regarding FSB investigations of computer hacking and FSB techniques for identifying criminal hackers.” The FSB officers also turned a blind eye to Belan enriching himself on the side by using his access for credit card fraud, spam campaigns, and “by fraudulently redirecting a subset of Yahoo’s search engine traffic.”

The arrangement with Baratov was slightly different, with him being paid a bounty in return for gaining access to additional email accounts with providers other than Yahoo after Belan had gained access to their Yahoo accounts. According to the indictment, “When Baratov successfully obtained unauthorized access to a victim’s account, he notified Dokuchaev and provided evidence of that access. He then demanded payment – generally approximately US$100 – via online payment services. Once Dokuchaev sent Baratov a payment, Baratov provided Dokuchaev with valid, illicitly obtained account credentials.” Baratov was arrested in Canada on March 2017 and pleaded guilty in November.

Ultimately, this indictment offers unprecedented insight into the state-crime nexus that is particularly prevalent in the former Soviet Union. While the number of people involved and the cost of the Yahoo operation were low, it caused significant economic damage. It caused the deal between Verizon and Yahoo to be cut by US$350 million when the data breach became public—a disturbing result for a group of four people.

**Why Do Cyber Proxies Matter?**

How much control a state exercises over its proxies—whether the state directly sponsors, only supports, or indirectly enables criminal activity—matters because it has direct implications for national security decision making that affects international peace and security. For example, in 2014, reports emerged that Nasdaq had been hacked. Only a few years after the world’s worst financial crisis since the Great Depression, targeting a pillar of the global financial system with a novel cyber weapon made senior national security officials nervous enough to brief U.S. President Barack Obama on the incident as the investigation proceeded. In particular, the National Security Agency (NSA) was concerned that Russia could be responsible. Yet, given the Russian government’s laissez-faire approach toward cyber criminals, Moscow’s involvement was far from certain. Ultimately, the assessment was that this was not the action of the Russian government but of independent criminals who had stolen Nasdaq’s software for profit-driven reasons. Nevertheless, this example illustrates how under different circumstances—for example, with further heightened tensions or with a more impulsive leader—such an incident could spiral out of control before its source and intention could be assessed with high confidence.
A review of the behavior of cyber proxies also points to some interesting findings specific to liberal democratic countries. To start, based on currently available data, liberal democracies seem more likely to exercise tight control over cyber proxies whereas other non-democratic regimes seem more comfortable with looser arrangements. One potential factor explaining this divergence is that the political system of liberal democracies imposes accountability through parliaments and ultimately elections. While looser relationships might exist for covert operations and other limited areas, overall there are significant constraints representative of the modern conception of the nation-state and its monopoly over the legitimate use of force.

Another relevant finding is that some of the countries use cyber proxies not only to target foreign companies or governments but dissidents at home and abroad, illustrating the human rights dimension of this issue. Beijing and Tehran, for example, view information itself as a potential threat to regime stability, which is why their focus on information security is as much about the control of information as it is about securing their systems against potential intrusions. The plausible deniability provided through these proxy relationships makes it particularly challenging to effectively respond to such behavior.

What Can Be Done About Cyber Proxies?

So, what can be done to reduce the potential risk of miscalculation and accidental escalation when it comes to other states’ proxy relationships? One framework that can guide a country’s strategy is the DIME(LE) model—diplomacy, information, military, economy, and law enforcement—that leverages different instruments of statecraft to create incentives and disincentives to shape proxy relationships of another country:

Diplomacy: A good example of how diplomacy was used to encourage a government to tighten control over some of its proxies are the public and private statements by various governments urging the Chinese government to take action against cyber-enabled economic espionage. These calls have ranged from German Chancellor Angela Merkel’s complaints to Wen Jiabao in 2007 after her office had been hacked to Secretary Hillary Clinton’s demarche following the hack of Google in 2009 and President Obama raising the issue quietly during his meetings with President Xi.

Information: Information itself can be a powerful tool to nudge actors or at least to send a clear message. For example, the series of indictments that have been
unsealed also serve the function of information published as part of a naming-and-shaming strategy. The indictments make clear that attributing cyber attacks is not only possible but that it goes as far as having photos of the people behind it. In the Chinese case, naming and shaming has been partly credited for Beijing reining in some of its hackers (at least temporarily).\textsuperscript{41}

**Military:** The third element of DIME(LE)—military action, here considered to also include covert action—can be employed to change a state’s proxy relationships.\textsuperscript{42} So far, there is no public evidence pointing to the use of such tools vis-à-vis proxies. However, it is not unthinkable that an approach similar to that taken to disrupt terrorist groups or the hacktivist network Anonymous, which targeted a wide range of companies and governments, may be used. For example, this could include targeting communication networks or using fake personas or informants to sow mistrust between the proxies and those supporting them.\textsuperscript{43}

**Economy:** In 2015, the White House created the foundation for imposing cyber-specific economic measures through executive order 13694, which makes it possible to block the property of individuals engaged in significant malicious cyber-enabled activities.\textsuperscript{44} Used against several Russian citizens for their involvement in the 2016 election interference, this sanctions authority was also used in March 2018 against nine Iranian hackers responsible for hacking hundreds of universities, companies, and government agencies.\textsuperscript{45} (Trade restrictions are technically another possible form of economic measures taken but are a rather rare instrument that has not seen much use until recently. For example, concerns over the continued cyber-enabled theft of intellectual property reportedly contributed to President Trump’s decision to impose tariffs against China in February 2018.)\textsuperscript{46}

**Law Enforcement:** In the search for effective tools to counter the new cybersecurity threats from abroad, the U.S. government has increasingly turned to use indictments by U.S. law enforcement agencies as part of its broader effort to counter malicious cyber threats. While the prosecution of hackers living abroad is highly unlikely—especially if they are in countries such as Russia, Iran, and China—it has led to the arrest and extradition to the United States of at least two people mentioned in the indictment.

The DIME(LE) framework can be applied to both actions taken in direct response to an ongoing campaign and as part of a strategy to change a state’s systematic approach toward proxy relationships over time. The concept of sovereignty is particularly important in this context. While the states who have allegedly actively or passively sponsored cyber proxies in the past usually vehemently deny any responsibility, some of them count among the most fervent defenders of sovereignty in its classic, more absolutist sense. This matters because sovereignty implies a claim of authority and control within the jurisdictional boundaries of a state’s territory. This has led to the rise of expectations
about states exercising due diligence, “by which states are responsible for ensuring their territories are not used for activities harmful to other states.” In other words, independent of whether a state was responsible for a proxy’s actions or not (and can therefore be held accountable), the state can nevertheless at least be expected to take action against activities harmful to other states. This logic explains the focus in international cybersecurity discussions on state behavior, which is also an important lever to affect the behavior of cyber proxies.

China is a particularly interesting case study worth mentioning in this context because the Chinese government has increasingly tightened its control over the past two decades. From initially turning a blind eye to the patriot hacktivist activity in the 1990s, the government started issuing statements calling on the hacktivists to stop their activities and began establishing information warfare militias throughout the country. Within the span of a few years and by the time Hu Jintao became the new president of China in 2003, experts agreed that the hacker groups in China represented independent actors that were “state tolerated” or “state encouraged.” Xi Jinping further centralized control over the past two decades. How much of this change was due to foreign pressure and how much driven by internal factors remains uncertain, but China’s rapidly changing nature of the state appears unique in history. Ultimately, plausible deniability is becoming increasingly implausible for Beijing when it comes to malicious cyber activity emanating from China; given the capabilities and reach of the state, Beijing should at least be able to stop such activity if it is willing.

**Takeaways and Implications**

A comprehensive analysis of proxy relationships between states and hackers to date reveals several insights. First, a common theme across countries is the impressively small number of individuals involved in such networks and campaigns, usually less than a dozen. The resources involved also appear to be very little, ranging in the thousands of dollars to perhaps the low millions at most. At the same time, the hackers can achieve effects that present new risks to international peace and stability. Perhaps most important is that all examples occurred within the past decade suggesting a rapid development and evolution of the threat landscape.

Second, proxy relationships differ from country to country. While new relationships could be assumed given how cheap it is to organize such operations, the known proxy relationships reflect a high degree of path dependence. In other
words, how Moscow, Tehran, and Beijing have engaged with hackers emulates how they have engaged with other non-state actors in the past. That is good news and bad news. The good news is that cyber proxies are much like old-fashioned proxies. The bad news is that cyber proxies are much like old-fashioned proxies. This means that cyber proxies are therefore not an entirely new or unique phenomenon and that lessons learned from conventional proxies can be applied. At the same time, it is clear that proxy relationships are strongly tied to a country’s political, economic, legal, and cultural system, taking decades rather than years to transform. Iran, for example, is known for its use of proxies throughout the Middle East, yet little progress has been made over the past few decades to significantly shift Tehran’s approach and use of this model.

The relationship between hackers and governments tells us a lot about the political and economic realities in those countries, rather than just the role that hackers play. For example, 25 years after the Soviet Union’s collapse, it is clear that the economic situation remains dire enough to provide fertile ground for criminal activity and corrupt government officials—activity that in the digital age can be far removed from the victim and allow the perpetrator to avoid arrest and often even detection.

In the absence of alternatives, a strategy based on a mix of DIME(LE) instruments remains the most promising avenue to nudge governments to exercise effective control over their proxies. Which instruments to prioritize for achieving this objective is an important question that requires monitoring and adjustments over time, and will vary from state to state. Indictments, for example, have been a focus of the U.S. government in recent years. Unsealing them sent a clear signal to the respective governments as well as the victims, often companies, that the government was taking action and that the attribution of cyber attacks is possible. Yet, their effects on the perpetrators have been limited to denying travel to countries that might arrest and extradite to the United States, freezing of assets in U.S. jurisdiction, and in a few cases arrest and incarceration. The latter two do not apply to most hackers and to what extent not being able to travel to some “100 countries without fear of arrest and extradition to the US”51 constitutes a severe limitation and deterrence most likely depends on each individual’s view on the remaining 90 countries.

Reviewing the strategies and priorities of the past decade, and developing a more robust and comprehensive international law enforcement strategy is needed to more effectively address cyber proxies in the long term. So far, the
U.S. government has prioritized developing strategies for diplomacy as well as the military, and a new executive order enhanced the use of economic measures in response to malicious cyber activity. Yet, while law enforcement made an important contribution through the indictments, a comprehensive strategy focusing on international law enforcement cooperation is missing. Promoting joining the Convention on Cybercrime and claiming success when less than a handful of countries join each year, putting its current number of signatories at some 50+ member states, cannot be enough.

The trends point toward greater challenges in the future creating more urgency for such a strategy. Already, third countries are being used as safe havens by criminals. For example, in 2014, reports emerged that several dozen Chinese were discovered by the Kenyan authorities conducting cybercrime out of Nairobi. Eastern European hackers are routinely arrested in South East Asia for cybercrime and reports suggest that North Koreans operate from India. As attribution becomes easier, states might try to hide their tracks by using more sophisticated techniques or by sending proxies to third countries to conduct their campaign. If this happens, local law enforcement agencies need to have capacity to detect them, otherwise hackers will come and go without being noticed. So far, this type of capacity building and law enforcement cooperation has not been a priority. While mentioned in strategies, the resources and attention dedicated to it pale in comparison to other priorities such as the Pentagon’s efforts or even the State Department’s focus on advancing international norms.

In addition to a shift toward a greater focus on law enforcement capacity building and international cybercrime cooperation, further advancing the concept of due diligence and clarifying expectations for its application to cyberspace, remain important. Without a country’s ability to exercise due diligence and understanding how to respond appropriately to potential requests, developing a framework based on state responsibility will not be effective. Beyond creating the normative and legal environment, more resources are also needed to support such a strategy and policy shift. Following the money, which is concentrated in the military, this could include leveraging options such as the authorities given to the Pentagon through the 2015 National Defense Authorization Act to support law enforcement agencies to counter transnational organized crime.

The toughest challenge is the evolution of the threat landscape. To date, the number of sophisticated hackers is relatively low, likely a few hundred or perhaps a few thousand. Their malware and attacks stand apart from the thousands of less sophisticated hackers. However, in recent years, sophisticated tools developed by states have been leaked, stolen, or deployed. While their exploits can usually be patched, this takes time and leaves systems vulnerable. At a more abstract level, studying their design, composition, and operation can help others
reach new levels of sophistication. In other words, it does not require a sophis-
ticated hacker to use sophisticated malware. Importantly, a more sophisticated 
hacker can be more precise when targeting systems, whereas a less sophisticated 
hacker runs a higher risk of indiscriminate attacks. Focusing merely on trying to 
arrest the most sophisticated hackers or to nudge their activity away from malici-
ous toward beneficial endeavors is therefore not sufficient. How to manage 
the development, deployment, and potential leaking or theft of cyber tools 
requires particular attention.

It is worth highlighting that the indictments focus on proxy relationships in 
countries considered cyber powers during the past decade. North Korea is a note-
worthy exception, not because of its lack of ambition or intent but because experts 
from the United States to South Korea consider its hackers not proxies but direct 
agents of the state. With more than 30 countries now pursuing offensive cyber 
capabilities, the coming years will likely witness reports about similar relationships 
between states and hackers in other countries. The framework offered in this 
article is an attempt to help classify prototypical cases to compare them with 
those coming to light in the future.

Against this background, it is worth ending with a note of caution: attempting 
to influence another state’s use of proxies is not without risks of its own. Some of 
the more aggressive steps in the DIME(LE) framework could escalate the situation 
and trigger more aggressive actions by the proxy, the beneficiary, or both. Such 
attempts could also backfire by increasing domestic support for a non-state 
actor, or by pushing the state from passive into active sponsorship.\textsuperscript{57} Another chal-
lenge is that proxies may need to be weighed against other important issues in the 
bilateral relationship. In short, the DIME(LE) is a helpful framework, but not a 
silver bullet.

Notes

   R. Clapper, Director of National Intelligence, Marcel Lettre, Undersecretary of Defense 
   for Intelligence, and Michael S. Rogers, US Cyber Command Director, National Security 
   Agency), https://www.armed-services.senate.gov/hearings/17-01-05-foreign-cyber-threats-
to-the-united-states.
   www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain. The list 
   usually included the United States, Russia, China, the United Kingdom, Israel, (sometimes 
   France), soon followed by Iran and North Korea.
   email-hack-n733716.

5. Max Smeets, “Europe Slowly Starts to Talk Openly About Offensive Cyber Operations,” Council on Foreign Relations, November 6, 2017, https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations. I write “some” because Israel is arguably an interesting exception where the mandatory multi-year military service continuously trains a sufficient amount of people with additional programs such as the Talpiot program designed to also identify the top quality talent, see Jason Gewirtz, Israel’s Edge: The Story of the IDF’s Most Elite Unit — Talpiot (Jerusalem, Israel: Gefen Publishing House Ltd., 2016).


9. For the purposes of this article, the beneficiary-proxy relationship is limited to governments being the beneficiaries. In Tim Maurer, Cyber Mercenaries: The State, Hackers, and Power (Cambridge, England: Cambridge University Press, 2018), other scenarios such as companies hiring another company, for example to hack back, are also discussed with the latter being considered a proxy of the former.


12. The indictment against three members of the Syrian Electronic Army that was unsealed two days earlier on March 22, 2016, explicitely refrains, unlike in the case of the Iranian hackers, from referring to the three as having been “state-sponsored.” Meanwhile, the five Chinese mentioned in the 2014 indictment were not proxy actors but officers of the PLA and therefore direct agents of the Chinese military and state. “Manhattan US Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against US Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities,” US Department of Justice, March 24, 2016, www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.


29. Ibid.
30. Ibid.
33. Ibid.


Nigel Inkster, China’s Cyber Power (New York: Routledge, 2016), 40.


In addition, some limitations imposed by domestic law that prevent a state from taking actions cannot be reasonably expected to change, such as laws to protect minors (which might come into play in the case of a juvenile hacker) or the freedom of speech protections in the United States (which came into play in the context of the IRA sympathizers in the United States, see Daniel Byman, “Passive Sponsors of Terrorism,” Survival 47, no. 4 (2005): 131).