the
LAWFARE
BOOK REVIEW

States and Their Proxies in Cyber Operations

VALENTIN WEBER

Review of Tim Maurer, "Cyber Mercenaries: The State, Hackers, and Power" (Cambridge, 2018).

An ancient saying goes that whoever hires Swiss mercenaries wins the war. While Swiss mercenaries are nowadays not as feared as they once were, the Swiss Pontifical Guard still reflects the splendor of Renaissance warriors for hire. Yet the history of mercenary engagement in conflict is not only confined to land warfare. In the 17th and 18th centuries, the high seas were roamed by privateers who deployed their capabilities in favor of states that were unable to realize their goals without them. More recently, in Iraq, private companies such as Academi, Titan Corp., and CACI were widely present in supporting the U.S. military.

While such cases as these are well documented in historical and international security literature, overall the phenomenon of "mercenaries" in the digital realm has been largely understudied. Tim Maurer's book, "Cyber Mercenaries: The State, Hackers, and Power," succeeds at filling this void and makes a valuable contribution to the emerging literature of cyber international relations.

Maurer aims first to establish an analytic framework that allows for the study of "proxy" actors in the cyber domain. He defines a proxy as "an intermediary that conducts or directly contributes to an offensive cyber operation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect." Building a framework of analysis helps in finding the answers to the following questions: What do state-proxy relationships look like, and how do states use them to project power? Why do some states build close formal relationships with some proxies while treating other proxy relationships as distant and deniable?

"Cyber Mercenaries" takes up these and related questions in three parts. The first part sets out an overall framework for analysis, including how concepts such as conflict, proxies and mercenaries are drawn over from international relations generally to cyber international relations. The second illustrates this framework through several case studies (the United States, China, the former Soviet Union, Iran, and Syria). The last part considers the consequences of theory and empirics for practice in the larger space of international

politics and geopolitics.

The first part of the book gives an introduction into what proxy relations are, which ones currently exist, and why and how they emerged. States, in the terminology of Maurer's analytic framework, either "delegate," "orchestrate" or "sanction." Which of these a state does in given circumstance, the book says, will depend on many factors, including the state's preexisting relations with nonstate-actor proxies, as well as the state's domestic landscape (public-private relations, crime and employment levels, and so forth.). "Delegation" presumes a state's effective control over a proxy to which certain cyber tasks have been handed over. "Orchestration" means that a state actively backs a nonstate actor that shares its ideology and supports its goals, enabling the nonstate actor's activities with financial and logistical means. "Sanctioning," by contrast to the other two, translates into ignoring the activities of a proxy—where sovereign inaction, however, effectively enables the proxy's activities.

The state-proxy relationship (delegation, orchestration, sanctioning) as well as how proxies are actually used, varies depending on how a given state views cyber or information security. This introduces another basic analytic category in "Cyber Mercenaries." NATO countries view cybersecurity as the protection against the possibility of causing harm through destructive attacks and the gathering of intelligence. China and Russia, by contrast, perceive cybersecurity as information security and control over it, thus putting more emphasis on the content as a potential threat to domestic stability. The United States and Europe focus predominantly on the military and intelligence aspects of the cyber domain and thereby disregard the information/content aspect that ranks high in Moscow and Beijing. The difference is partly a disagreement over the appropriate concern of a sovereign in regard to information and its own domestic population.

Russia's particular perception of information security, the book says, was one factor that led the Kremlin to meddle in U.S. elections. Russia did what it did in part, according to "Cyber Mercenaries," as retaliation for then-Secretary of State Hillary Clinton fomenting, in its view, protests against the Kremlin in 2011. In support of this claim, "Cyber Mercenaries" references the January 2017 U.S. intelligence community assessment on Russian interference. That document says that "Putin most likely wanted to discredit Secretary Clinton because he has publicly blamed her since 2011 for inciting mass protests against his regime in late 2011 and early 2012, and because he holds a grudge for comments he almost certainly saw as disparaging him." Iran similarly directs its attention toward information operations and civil-society actors that it views as proxy actors of the West. The visible efforts of Russia and Iran are hence not directed toward destructive attacks against the critical infrastructure of the U.S. or its allies (though elections are now considered critical infrastructure), but instead against threatening content at home and abroad—in line with their perceptions of information security.

The book's second part illustrates this theoretical framework through case studies. It provides further answers as to why and how the United States, the former Soviet Union, China, Iran, and Syria use their proxies. The United States, for example, has had a strong inclination toward privatization of its wars and intelligence gathering since 9/11 (and well before that). The trend towards privatization has been also taking place in the cybersecurity sector. Major companies like Raytheon and Booz Allen Hamilton have jumped on the wagon and have become major suppliers of the offensive and defensive capabilities used in cyber operations.

Due to the U.S. government's particular relationship with its private business

sector, however, ties between public and private are (mostly) public and formalized in contracts. Maurer dubs this phenomenon "delegation," and he sees it as a reason for U.S. proxies being on a relatively "tight leash." In other aspects, the separation between public and private is less clear. In particular, a sizeable part of the cybersecurity workforce oscillates between government agencies like NSA and private entities such as Raytheon—an instance of the so-called "revolving door." Here one could draw a comparison with Russia, where the boundary between cybersecurity experts in the FSB, the Russian Federation's successor to the Soviet-era KGB, and the criminal underground remain fluid.

Maurer cites Iran and Syria as instances of states that "orchestrate." In these cases, proxies are "on a loose leash." Starting with the former, since 2012 Iran has used students who had previously acted independently, coordinating them toward its purposes and providing them with financial support to carry out their ideologically-driven actions against the United States. Damascus has similarly orchestrated the Syrian Electronic Army, which is part of the Assad-controlled Syrian Computer Society, using it to provide military intelligence and in particular targeting the Syrian opposition.

The book's chapter on today's countries that emerged out of the former Soviet Union describes how and why "sanctioning"—cyber proxies "on the loose," as Maurer puts it—has become the prevalent type of state-proxy relationship in this region. Maurer explains that a highly skilled workforce, a lack of employment opportunities, and a weak law enforcement environment have brought about a space where proxies are available and their malign activities tolerated—including many private criminal ones—as long as their activities are directed at targets abroad. Similarly, the availability of Russian proxies means that they can be mobilized quickly for patriotic purposes, such as in support of Moscow's operations against Estonia (2007), Georgia (2008), and Ukraine (2014). Maurer coins the term "Blitz Orchestration" to define this occurrence.

China serves as an instance of an evolving state-proxy relationship. It started off with sanctioning (presidency of Jiang Zemin, 1994–2003); moved on to orchestration (Hu Jintao, 2003–13); and eventually embraced delegation as the predominant type of state-proxy relationship (Xi Jinping, 2013–Present). As Maurer points out, the Chinese government's increasing control over proxy actors, exercised via traditional militia groups, has intriguingly coincided with an incremental tightening of the screws on China's internet in general.

The third part of the book is focused on international law and practical questions of international politics. Maurer gives a short overview of how states can be held accountable for proxies that are involved in offensive cyber operations. His conclusion is that it is quite hard to do so at the present moment, since most cyber operations fall below the threshold of what international law considers a use of force in the "physical" world, and because of yet-underdeveloped international legal provisions (which might remain underdeveloped, given that important parties likely prefer ambiguity to legal clarity on these issues).

In order to deal with the current challenging environment, Maurer explores the concept of "due diligence." This norm expects states to not knowingly allow proxies to act from their territory harming other states. States that have a loose relationship with their proxies need to tighten the leash in order to avoid being accused of not having fulfilled their "due diligence." While some might argue that they have no interest in doing so—because the closer the state-proxy relationship, the harder it is to deny responsibility for offensive operations—Maurer mentions why greater control over proxies should be in the inherent interest of states: "to be in

control of escalation and, second, because of the potential proliferation of capabilities."

As with other books in the cyber international relations field, the author has had to cope with the classified documents and contradictory factual claims, where, for example, one country accuses and the accused country, in response, denies. However, many other realms of study, such as military Special Operations literature or nuclear weapon and strategy studies, have long had to deal with similar issues. Yet they have still been able to produce high-quality research.

Since, according to Maurer, data is still rare concerning the cyber domain and cyber operations, this is a strong reason why inductive analysis, such as case-study research and case-study interviews, is for now the right approach to gain insight into the most contested issues of cyber international relations. Maurer intends his book to serve as a framework of analysis that "can be populated as more data becomes available." The case studies, then, are to serve as ideal types for the study of a growing number of countries that gain cyber capabilities.

Certainly I agree that data gathering is challenging in the cyber domain—scattered as it is across government, private, civil society, unclassified intelligence documents, and other categories of sources. Still, in my view, Maurer is too modest about the availability of information and evidence. Indeed, "Cyber Mercenaries" is the best proof of it. A committed reader has only to delve into the book's 70 pages of illustrative endnotes; it offers one of the most comprehensive bibliographies on cyber proxies.

A strong point of "Cyber Mercenaries" is the author's diverse background in various fields. This allows Maurer to successfully break barriers between academic and policy disciplines that otherwise tend to stay inside their individual silos. He deploys a multidisciplinary approach to international cybersecurity—he succeeds in convening what amounts to a "Congress of Disciplines," to use a term coined by another scholar of cybersecurity, Lucas Kello. "Cyber Mercenaries" adeptly combines history, international relations, international law, human rights and technical aspects of cybersecurity, to provide an insightful answer to state-proxy relationships. This cross-disciplinary approach ably demonstrates that we need history and human rights to understand the emergence of state-proxy rapports and their use in offensive cyber operations. We need international relations to build a framework of the relationship. We need a technical understanding of cyber operations in order to understand and explain actions. And eventually, we require international law to regulate proxy use. Omitting any of these aspects would tell an incomplete story of state-proxy relations. Having married all these realms, Maurer contributes to the wider literature and demonstrates that such a multidisciplinary approach is not only helpful, but essential in the study of international cybersecurity.

"Cyber Mercenaries" questions the prevalent state-centrism in international relations. He does so convincingly by showing how some proxies can be more powerful than certain nation-states. Nonstate actors from Iran, for example, have infiltrated a dam in the United States. Private companies, such as Hacking Team, sell intrusion techniques to states that, among other things, allow governments to gain access to smartphones. Many of these capabilities would otherwise very unlikely be within the technical capabilities of such states as Zimbabwe or South Sudan.

States have thus never enjoyed an exclusive access to cyber weapons. Quite to the opposite, nonstate actors have always been in possession of advanced capabilities. One good example of this is the Morris Worm, launched by a student in 1988, and which brought down thousands of computers, a sizeable amount of the internet infrastructure of that day. By

making this point, Maurer complements Joseph Nye's "Future of Power," in which Nye skillfully describes the diffusion of power from state to non-state actors. In this vein, Maurer states "while the Internet certainly leads to a diffusion of power generally, cyber power itself was diffuse from the start."

I noted at the outset that "Cyber Mercenaries" accepts the widely held view that Russia and China see cybersecurity largely through the lens of content. Hence, while most NATO countries, Maurer says, prefer the

term cybersecurity, Russia, China, and members of the Shanghai Cooperation Organization prefer the term information security, which is tied to the controversy around information operations, control over content, and the free flow of information.

According to Maurer, then, it is important to understand the viewpoints captured in such terminology, at least if the purpose is to explain how different states use proxies in different ways and to different ends. However, this binary of content (information security) versus military and intelligence (cybersecurity) seems too simplistic. Maurer observes that Russia deploys destructive cyber-actions only rarely; instead, it uses "information operations to achieve its goals." This might be, however, not because of its perception of information security and its implications for the use of proxies, but instead simply because deterrence at the high end of the spectrum of cyber destruction works.

Moreover, the U.S., despite its predominant emphasis on intelligence and military facets of the cyber domain, also focuses on content. The U.S. government across many decades has always had the promotion of democracy inside weak or non-democratic countries as part of its self-perceived mission in the world. These goals are reflected in the policy strategies and calculations of the State Department, the CIA, USAID, U.S. government-sponsored and -funded information outlets such as Voice of America, and many other agencies of the U.S. government. These activities have long included financial and other support to civil society groups, both inside and outside a particular country. William J. Daugherty, a former CIA employee, says in an interview about U.S. democracy promotion: "I assume they're [the CIA] doing a lot of the old stuff, because, you know, it never changes. The technology may change, but the objectives don't." The U.S. government, of course, sees nothing objectionable in these activities, and certainly does not accept Russia or China's viewpoint that they are, or can be, one sovereign meddling in the internal affairs of another sovereign.

Whether U.S. democracy promotion abroad is legally or morally distinguishable from what the Russian government and its cyber proxies did in the 2016 U.S. elections, it appears that, as a matter of policy and behavior, the U.S. is focused on content abroad but not at home. This, indeed, is why it was surprised by Russian election meddling in 2016. On the other hand, due to their regime-survival concerns, Moscow, Tehran, and Beijing direct their attention to content both at home and abroad—which in turn informs and structures their use of cyber proxies.

Accepting, however, that a state's perception of cyber and information security is not necessarily binary, but rather on a spectrum ranging from an emphasis on military/intelligence, on the one extreme, and content-related information operations, on the other, has implications for Maurer's argument. Among other things, it means that states might as well situate themselves somewhere along the spectrum, in the middle or leaning to one side or the other—but without giving up the possibility of attending to both, to one degree or another. This in turn might inform a state's use of cyber proxies and in particular give it a reason to have more varied cyber proxies, specialized toward different ends of the

spectrum—sometimes focused on carrying out content-related operations and at other points in time focused on attacking and damaging one or another part of the national critical infrastructure.

Another important point is the author's distinction between delegation (effective control over the proxy) and orchestration (financial and logistical support of an ideologically driven non-state actor). The book portrays delegation as an exercise in rational choice decision-making, neutral and instrumental, and which does not rely necessarily on ideology. Maurer cites U.S. government relations with various cybersecurity companies as an example. However, if one takes a step back, one perceives that ideology is inherent in the U.S.'s state-proxy relationship. To a large extent, it might be argued, it is ingrained in the political notion of the relationship between public and private, both their differences and interrelationships, in U.S. political and legal culture.

Contractors, for instance, have to be U.S. citizens and are required to obtain a certain security clearance to support the U.S. government in cyber-related operations. In this sense, at least, nationality, as a condition for contracting work, presumes a certain ideological orientation and common goals between the beneficiary and the proxy. This ideological component or state allegiance is reflected, moreover, in the "voluntary" work of U.S. cybersecurity companies for the U.S. government. U.S. firms, for example, remain hesitant to produce threat intelligence reports on U.S. or European APTs (Advanced Persistent Threats). FireEye's decision to publish reports on APT 1 (a Chinese threat actor) and APT 28 (a Russian cyber operations unit) was a voluntary one—and, within Maurer's analytic framework, it could thereby fall into the category of orchestration. It took Kaspersky Lab—a Russian cybersecurity company, not an American firm—to unveil the capabilities of Equation Group (which is presumed to be linked to the NSA).

"Cyber Mercenaries" makes another important statement in arguing that domestic concerns, such as regime stability, largely drive states' international cyber operations. While I agree that the domestic drives the international, one could just as well state that international concerns drive both the international and the domestic. First, the international impacts the international—the U.S.'s domestic, yet cross-border, indictment of five PLA officers located outside the United States for cyber activities, for example—which had the effect of reducing Chinese cross-border cyber espionage. Iran's switch to espionage activity after the nuclear deal, too, could serve as an example of this phenomenon.

Second, however, the international also impacts the domestic. This phenomenon could have been profitably highlighted more extensively in the book. In effect, "Cyber Mercenaries" says that "the Iranian government has been motivated by the same concerns over U.S. government-funded projects that drive the Russian and Chinese governments." However, the book does not explicitly draw or discuss the wider conclusions of this statement—the implication that there are international forces shaping domestic state-proxy relations. I would be curious to see this "international" impacting the "international" and "domestic" further unpacked.

But these are modest quibbles. "Cyber Mercenaries" is an excellent introduction to this topic for the general public, and at the same time it can serve as advanced reading for cyber pundits and specialists interested in the rising influence of non-state actors in the cyber domain. It is especially to be recommended for its (rare) ability to address and remain readable for a wide and heterogeneous audience, ranging across the general public, international relations scholars, historians, lawyers, and policy makers alike. The book more than credibly argues that proxies are a force to be reckoned with in the cyber domain,

today and into the future. And, still more importantly, it provides astute insight into how to understand and, one hopes, manage all manner of proxies in a way that will increase international cybersecurity.to these controversies, however, will do well to go beyond this volume.

Valentin Weber is a D.Phil. Candidate in Cyber Security and a Research Affiliate with the Centre for Technology and Global Affairs at the University of Oxford. His current work analyzes the diffusion of cyber norms.

Cite as: Valentin Weber, *States and their Proxies in Cyber Operations*. May 15, 2018. https://tinyurl.com/y9la73a7.