BOOK REVIEW

Projecting Power: How States Use Proxies in Cyberspace

CYBER MERCENARIES: THE STATE, HACKERS, AND POWER. By Tim Maurer. New York and Cambridge: CAMBRIDGE UNIVERSITY PRESS, 2018. PP. 259. $29.99

Syed Hamza Mannan*

INTRODUCTION

Nation states have long relied on proxies to do their bidding for various reasons, including escaping the application of international law,[1] maintaining plausible deniability by masking the identity of the culpable actor,[2] and engaging in warfare under circumstances where the public appetite for traditional military operations has waned.[3] Thus far, the literature on cyber operations has been state-centric (for example, concentrated on those cyber operations carried out by and on nation states), often overlooking the dynamic relationship between states and their cyber proxies.[4] And until now, the idea of proxies in cyberspace has not received much academic attention. In *Cyber Mercenaries*, Tim Maurer presents a new typology for thinking about how nation-states organize their relationships with cyber proxies and gives this underexplored topic the timely attention it deserves.

---

* J.D., Georgetown University Law Center.

1. *See* Beatrice A. Walton, Note, *Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law*, 126 YALE L.J. 1460, 1469-77 (2017) (explaining the gap in international law in dealing with low-intensity cyberattacks).

2. Justin Key Canfil, *Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity*, 70 J. INT'L AFF. 217, 218-20 (2016) ("One explanation is that states employ sympathetic cyber proxies in order to maintain the illusion of plausible deniability.").

3. *See* Kevin A. O'Brien, *Surrogate Agents: Private Military and Security Operators in an Unstable World*, *in* MAKING SENSE OF PROXY WARS: STATES, SURROGATES & THE USE OF FORCE 133-35 (Michael A. Innes ed., 2012) (discussing the "proxyization" of warfare and highlighting that one reason for their usage is because the actions of proxies are not subject to the same public spotlight as those of statutory forces).

4. TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER x-xi (2018). This observation is not just limited to the literature on cyber operations, but also applies to the legal framework that governs operations by non-state actors. Public international law today is primarily concerned about relationships between states, and has failed to account for the activities of non-state cyber actors. *See* Michael N. Schmitt & Sean Watts, *Beyond State-Centrism: International Law and Non-State Actors in Cyberspace*, 21 J. CONFLICT & SECURITY L. 1, 2 (2016).

The thrust of Maurer's main argument is simple. States today project power in cyberspace through non-state proxy groups, often in different ways, and a proper understanding of this relationship can help us navigate questions attendant to that relationship: what are the different ways a state's relationship with a cyber proxy is organized? How and why do states use cyber proxies to project power? Why do some states lean closer to these proxies than others, and what does this distance reveal about how a state views them?

Answers to these questions, and the others Maurer poses in this book, are critically important today. Non-state actors today have capabilities that reach far across state boundaries.[5] Consider the following incident. In 2016, alleged North Korean hackers attempted to steal nearly $1 billion from the Bangladesh Central Bank by hacking into the bank's computer network. These hackers quietly waited and watched for months to better familiarize themselves with the bank's operation, all the while collecting passwords and squeezing their way into the "military grade" protected SWIFT network, which thousands of financial institutions use to send and receive information about financial transactions.[6] The hackers managed to get only five of their orders through – orders which totaled $81 million. Cybersecurity experts analyzed the details of this attack and concluded that the North Korean state was closely linked to the hackers.[7]

Understanding the relationship between North Korea and the hackers behind the Bangladesh bank heist, as set forth in a Department of Justice criminal complaint against one of the alleged hackers, is key to appreciating how North Korea employed a proxy to conduct malicious activities on its behalf.[8] The North and South Korean governments initially established Chosun Expo, a company which was meant to be a "joint venture . . . established to be a Korean e-commerce and lottery website."[9] South Korea reneged on its commitment, and North Korea continued operating the business, which supplied goods, software, freelancing services, and gambling products.[10] But the company was also a "front for the North Korean government," which employed Park Jin Hyok, who worked as part of a broader "conspiracy to conduct computer intrusions and commit wire fraud by co-conspirators working on behalf of the government of [North Korea]."[11] Importantly, the company maintained some distance from the government, operating as a proxy, instead of a public agency affiliated with the government. A

5. U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command*, Apr. 2018, at 3, https://perma.cc/T5NY-W96G ("Cyberspace threats are growing. They transcend geographic boundaries and are usually trans-regional in nature."); MAURER, *supra* note 4, at 4 ("For the first time, non-state actors can have global reach through hacking . . .").

6. Joshua Hammer, *The Billion-Dollar Bank Job*, N.Y. TIMES (May 3, 2018), https://perma.cc/AK86-NE7P.

7. *Id.*

8. *See* Criminal Complaint, United States v. Park Jin Hyok, Case No. MJ 18-1479 (June 8, 2008).

9. *Id.* at 136.

10. *Id.*

11. *Id.*

manager oversaw the activities of the employees, and a "separate political attaché" monitored their activities.[12] Moreover, the company still sold services to non-government paying clients for information technology and non-malicious programming projects.[13] By empowering non-state actors to carry out this operation, North Korea allowed these forces to use the "tools and prerogatives" of coercion in which the community of nations share a common interest in keeping in governmental hands.[14] The differences in control over those tools, as Maurer explores in this book, lie in the extent to which states control the rein on that leash. At the same time, the use of cyber proxies gives states the added advantage of avoiding attribution for their nefarious actions, while still retaining those tools of coercion.

Understanding this relationship between the state and cyber proxies is useful for several reasons. Cyberspace represents a new domain of conflict, adding to the existing domains of use of force by land, air, sea, and space.[15] Although there is still a live classification debate on whether attacks in cyberspace can constitute an armed conflict under international law, cyberattacks undoubtedly have the potential to inflict great harm.[16] States today hack banks,[17] steal intellectual property,[18] interfere in elections,[19] and have attempted to infiltrate public utilities.[20] As the cyber tactics behind these operations become harder to detect, such as in the case of an alleged Chinese hack on the hardware of tech companies,[21] knowing the motivations behind the state's use of proxies, as well as advantages that

12. *Id*.

13. *Id*. at 5.

14. *See* W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW 72 (1992).

15. *See* Kevin M. Woods & Thomas C. Greenwood, *Multidomain Battle: Time for a Campaign of Joint Experimentation*, JOINT FORCE Q., Jan. 2018, at 14 (discussing how cyber operations are now prompting a "re-examination of all previous military concepts and doctrines"). The U.S. Army's senior commander of Training and Doctrine Command, Gen. David Perkins, emphasizes this point: "The world I grew up in, during the Cold War, you would have ground forces fighting ground forces, air forces fighting air forces. Cyber didn't even exist when I was a lieutenant." Michelle Tan, *The Multi-Domain Battle*, DEF. NEWS (Oct. 3, 2016), https://perma.cc/5ZQD-WR4X.

16. *See* Michael N. Schmitt, *Classification of Cyber Conflict*, 89 INT'L L. STUD. 233, 239-250 (2013), https://perma.cc/EQ24-A792 (discussing the challenges in classifying cyberattacks as armed conflicts).

17. Hammer, *supra* note 6.

18. Adam Segal et al., *Hacking for Ca$h: Is China Still Stealing Western IP? Report No. 2/2018*, AUSTRALIAN STRATEGIC POL'Y INST. (Sept. 25, 2018), https://perma.cc/F2Y8-ZWNS.

19. David E. Sanger & Scott Shane, *Russian Hackers Acted to Aid Trump in Elections, U.S. Says*, N.Y. TIMES (Dec. 9, 2016), https://perma.cc/NQ6C-8D4F (detailing that American intelligence agencies have "high confidence" that Russia influenced the U.S. presidential elections); *The Impact of Russian Interference on Germany's 2017 Elections: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (2017) (testimony of Dr. Constance Stelzenmüller, Robert Bosch Senior Fellow, Brookings Institution).

20. Arthur H. House, *We'd Be Crippled by a Cyberattack on Our Utilities*, WASH. POST (Oct. 14, 2018), https://perma.cc/G7M2-34BU.

21. Jordan Robertson & Michael Riley, *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, BLOOMBERG BUS. (Oct. 4, 2018), https://perma.cc/LWE6-G6ZD. Hardware hacks, as opposed to software hacks, are incredibly rare and require a great degree of sophistication. As one

proxies offer in certain types of operations, will help in several ways. This knowledge will allow states to better develop methods of deterrence, international monitoring, and a shared understanding on the norms and legal framework that should govern these behaviors.

Part I of this review presents an introduction to cyber proxy relationships, detailing why such relationships exist, the motivation of states in using proxy groups, and the different types of relationships that states have with their cyber proxy groups. Part II looks to the implications of the different models of relationships, and Part III offers some thoughts on the areas where Maurer's model presents special challenges. Finally, Part IV concludes with a brief discussion on the continuing challenges in this area that remain unresolved.

I. THE ANATOMY OF CYBER PROXY RELATIONSHIPS

A. Why Do Cyber Proxy Relationships Exist?

States purposefully use cyber proxies for several reasons. First, many of the non-state groups which have cyber capabilities have used them for a longer period of time than states themselves.[22] Therefore, some states face a talent gap and have struggled to attract people who can work in the cyber units that their governments establish.[23] As a result, some states tend to work with informal groups in order to bridge the gap in their cyber capabilities. Second, proxy relationships allow states to maintain plausible deniability.[24] This is true especially in cyber operations, because the internet's structure and character makes attribution for attacks difficult.[25] When the victims of cyber operations are left without ways to locate the origins of the attacks, or accurately pinpoint the perpetrators, states are left to operate under circumstances which create incentives for the use of proxies. Third, states use cyber proxies to avoid engaging in direct conflict, which can result in casualties and quickly reduce the tolerance for direct military engagement.[26] Offensive operations by way of cyber proxies do not always impose this same cost of heightened casualties and also tend to be cheaper to execute.[27]

---

hardware hacker explains in the Bloomberg report, "Having a well-done, nation-state-level hardware implant surface would be like witnessing a unicorn jumping over a rainbow." *Id.*

22. MAURER, *supra* note 4, at 36. There are however certain exceptions, such as the United States. *Id.*

23. Tim Maurer, *Cyber Proxies and Their Implications for Liberal Democracies*, 41 WASH. Q. 171, 172 (2018).

24. MAURER, *supra* note 4, at 39-40.

25. *See, e.g.*, Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J. L. & TECH. 376, 386-91 (2018) (discussing why proper attribution for cyberattacks is a problem in cyber operations).

26. *See, e.g.*, Scott S. Gartner & Gary M. Segura, *War, Casualties, and Public Opinion*, 42 J. CONFLICT RESOL. 278, 295 (1998) ("The human costs of a conflict provide a powerful explanation of wartime opinion. When marginal casualties increase, they capture the erosion of support better than other measures of casualties.").

27. *See, e.g.*, Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 158 (2009) (Benefits of cyber operations include "less physical destruction, less cost than other types of traditional warfare, and the ability to still achieve the same results with less risk to military personnel"); Julian Jang-Jaccard & Surya Nepal, *A Survey of Emerging Threats in*

Moreover, governments in democratic societies can face negative electoral repercussions for engaging in direct conflict, which in turn incentivizes states to make use of non-state proxy groups. Fourth, states may also use cyber proxies to decrease the likelihood of non-state actors disrupting the work of government agencies themselves.[28] Groups that are attached to the government, the thinking goes, will be less likely to attack government agencies.

B. The Framework of Cyber Proxy Relationships

Maurer's most useful contribution to the literature on cyber proxies is the framework he develops to help readers and practitioners think about the various models of state-proxy relationships in cyberspace. In Maurer's typology, states can either (1) delegate authority to proxies, (2) orchestrate the relationship by enlisting proxies to achieve the state's objectives, or (3) sanction the behavior of proxies by passively tolerating the proxy's malicious activities. These activities, however, are located on a spectrum, and states can (and do) shift between delegating, orchestrating, or sanctioning the behavior of proxies. For each type of relationship, Maurer populates that framework by assigning case studies of the United States, Iran, Syria, Russia, and China, helping readers grasp the different models of interaction between the state and cyber groups.

At the outset, Maurer defines cyber proxies as "intermediaries that conduct or directly contribute to an offensive cyber action that is enabled knowingly, whether actively or passively, by a beneficiary."[29] Using a broad definition of cyber proxies gives him the benefit of capturing the behavior of groups that are passively enabled by the government, and have weak direct ties to the state. A more traditional definition of a proxy – such as, "a person authorized to act for another"[30] – belies the real-world relevance of the different ways in which a state can interact with non-state groups. An added benefit of Maurer's approach is that he views proxy relationships on a continuum, instead of as stand-alone categories.[31] In doing so, he is able to account for some of the relationships that fall in the gray zones and do not neatly fit into the categories that other scholars have previously identified.[32] It also gives him the benefit of capturing movement along

---

Cybersecurity, 80 J. COMPUTER & SYS. SCI. 973, 973 (2014) (noting that cyberattacks thrive because they are "cheaper, convenient, and less risky than physical attacks").

28. *See* MAURER, *supra* note 4, at 40.

29. *Id*. at xi.

30. *Proxy*, Merriam-Webster Online Dictionary, https://perma.cc/L5KF-7FZ7 (Nov. 2, 2018).

31. MAURER, *supra* note 4, at 30-32.

32. Some of these categories include sponsor-client, sponsor-proxy, patron-client, patron-proxy, principal-agent, among others. *See* Yaacov Bar-Siman-Tov, *The Strategy of War by Proxy*, 19 COOPERATION & CONFLICT 263, 269-72 (1984) (discussing proxy relationships as a kind of patron-client relationship); Marc R. DeVore, *Exploring the Iran-Hezbollah Relationship: A Case Study of How State Sponsorship Affects Terrorist Group Decision-Making*, 6 PERSP. ON TERRORISM 85, 89-90 (2012) (discussing the relationship between Iran and Hezbollah as one between a state sponsor and a non-state proxy); Kristina Kausch, *State and Non-State Alliances in the Middle East*, 52 INT'L SPECTATOR 36, 37-38 (2017) (discussing the different types of relationships between states and non-state actors and noting that they are "as varied as the kinds of non-state actors").

that spectrum, since some countries over time may change their approach to how they interact with proxy groups.

While proxy groups are non-state actors, detached from the government, there are different levels of detachment they maintain from the state. Maurer's typology places these different ways of characterizing a state's relationship with its cyber proxy into three categories, although these categories run on a spectrum and are not isolated definitional buckets.[33] The three types of relationships are: (1) delegation, (2) orchestration, and (3) sanctioning.[34]

1. Delegation

Where a state delegates authority to the proxy group to act on its behalf, it forms a type of relationship in the classic sense of the phrase "principal-agent."[35] Maurer observes that in an ideal world, the principal requires its agent to act in a certain way, and the agent complies with the principal's command.[36] Reality, however, is more complicated: agents have their own interests,[37] they can take more risks than were anticipated by the principal,[38] and morph into an entity that is beyond the principal's expectations.[39] To mitigate the problem, principals try and reduce risks by screening agents, monitoring them, and using several agents to leverage competition as a buffer against rogue actions by the agent.[40]

Countries relying on the delegation model include the United States. Their efforts to delegate cyber operations are best seen by the example of the proliferation of contracts awarded to private companies for their expertise in this area.[41] What is unique, however, is the tight leash on which these private contractors are held in a delegation model.[42] Although the United States government delegates to

33. MAURER, *supra* note 4, at 42 ("It is important to emphasize that these three categories fall along a spectrum of control and detachment between the beneficiary and proxy.").

34. *Id*.

35. *Id*.

36. *Id*. at 43.

37. Daniel Byman & Sarah E. Kreps, *Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism*, 11 INT'L STUD. PERSP. 1, 6-7 (discussing the principal-agent problem and showing that agents can have different goals and priorities than their principals).

38. Idean Salehyan, *The Delegation of War to Rebel Organizations*, 54 J. CONFLICT RESOL. 493, 495 (2010) (discussing the problem of "Agency Slack" in the context of the principal-agent problem, where an "agent takes actions that are not consistent with the preferences of the principal once delegation has been established").

39. *Id*. at 504-05 (detailing that one risk of delegating to an agent is that the agent can turn against the principal). This problem, as Maurer observes, is also referred to as the "Frankenstein problem," to refer to situations where the governments empower an agent that acts contrary to its desires and is beyond its control. *Id*. at 43-44.

40. MAURER, *supra* note 4, at 44.

41. Private companies that have been awarded contracts by the United States government include Raytheon, BAE Systems, ManTech, as well as smaller companies like ReVuln. These companies offer a range of services, including intelligence and cyber operations as well as counterintelligence. *See id*. at 74.

42. As Maurer highlights, the relationship between private companies and the United States government represents the "ideal-type versions" of the delegation relationship and the tight control that the U.S. government maintains over its proxies. *Id*. at 76.

these non-state proxy actors certain responsibilities, it maintains close monitoring channels to ensure that these actors act in kind with the government's demands. By way of example, the United States Cyber Command rigorously screens private companies before offering contracts,[43] closely monitors their activities,[44] and punishes its proxies when necessary.[45] In this way, the government reduces the likelihood of rogue proxy behavior, and ensures that its cyber proxies will continue to act on its behalf. This represents a close relationship, where the proxies are held on a tight leash. Maurer also argues that this relationship is the ideal model toward which states should tend. When states keep their proxies on a "tight leash" and maintain strong control over their actions, the risks for the proxy group taking rogue action are reduced.[46]

2. Orchestration

A relationship based on orchestration is different from delegation in that in an orchestration model, the state "enlists and supports intermediary actors" as a means of achieving its goals.[47] The state (orchestrator) will work with an intermediary to influence the target that the state seeks to undermine.[48] In addition, under this model, the state does not merely tolerate the behavior of the proxy group, or passively provide support to the proxy, but also fails to take action to prevent the hackers from engaging in malicious activities.[49]

The main difference from the delegation model is that the state provides the intermediaries with "ideational and material support," and uses them to "address target actors in pursuit of political goals."[50] The distinction from the delegation model comes by way of the central assumption holding this framework together, which is that the intermediary's cooperation is based on similar goals – ideational, political, or otherwise – to that of the orchestrator.[51] This is quite different from the delegation model, where the state's main concern is controlling the non-state actor, and the relationship with its proxy group is more tightly

43. The screening criteria includes requirements that the firms be U.S.-owned or possess a "favorable National Interest Determination," that the employees working on the delegated work be U.S. citizens and possess a top secret security clearance. *Id*. at 78.

44. Contractors are not allowed to work remotely, and some even work in the same physical building in which their government counterparts work. *Id*.

45. Punishment can include sanctions, civil penalties, and arrests, for activities such as outsourcing work to other countries and stealing and disclosing confidential information. *Id*.

46. Maurer cites to the example of the U.S. Cyber Command keeping the contractors it employs in close sight, including by imposing strict monitoring requirements, maintaining a close physical distance, and imposing strict confidentiality rules on the contractors. Because of the structure of this relationship, the contractors are less prone to taking rogue action. *Id*.

47. Kenneth W. Abbott et al., *Orchestration: Global Governance Through Intermediaries*, *in* INTERNATIONAL ORGANIZATIONS AS ORCHESTRATORS 4 (Kenneth W. Abbott, et al., eds., 2015).

48. *Id*.

49. MAURER, *supra* note 4, at 92.

50. MAURER, *supra* note 4, at 45.

51. *See* Abbott et al., *supra* note 47, at 14.

knit.[52] The orchestration model is the proper framework for describing those relationships between the state and proxy which are more distant and loose. In these types of relationships, the state encourages, tolerates, and affirmatively protects its proxy, while exercising a more detached control over that relationship.

The Iranian government, for example, has long been concerned about the influence of outside actors on its domestic internal stability. With the rapid development of cyber power in other countries, this paranoia took on new forms. The government recently, after witnessing the spread of protests against the state through the internet and attacks against its nuclear infrastructure allegedly at the hands of the U.S. and Israeli governments, quickly mobilized to develop its own cyber capabilities.[53] Since developing these capabilities, Iranian hackers have carried out attacks against the United States. In one such attack, Iranian hackers acting on behalf of the Islamic Revolutionary Guard Corps, a branch of the country's armed forces, gained access to a dam twenty miles outside of New York City.[54]

Drawing from the first indictment against a state-sponsored proxy that the U.S. Government unsealed, Maurer shows that the Islamic Revolutionary Guard Corps employed cyber proxies which were already politically motivated and provided them with greater fuel to carry out the government's desired ends.[55] In other words, formerly independent groups who were acting on their own volition over time were conscripted by the state.The Iranian state then provided these groups with resources, and certain members of the group also provided training to members of the Iranian intelligence community.[56] This relationship fits squarely within the orchestration model because the Iranian government affiliated itself with a group that had a previous ideological and political commitment, and provided the group with resources instead of simply tolerating the group's actions.

3. Sanctioning

Sanctioning represents the most distant relationship among the three types. Where a state overlooks and passively tolerates the activities of the non-state actor, it is said to sanction that behavior.[57] This type of relationship is quite

52. Maurer explains this difference in the following terms: "[T]he concept of delegation captures the proxy relationships that operate above the threshold of effective and overall control – what is described as 'state- sponsored' in the counterterrorism literature. Orchestration, on the other hand, covers the broad spectrum of activities taking place below this threshold – from financing to the provision of arms, intelligence, and logistical support – that nonetheless can be considered 'state-supported.'" MAURER, *supra* note 4, at 46.

53. Collin Anderson & Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*, CARNEGIE ENDOWMENT FOR INT'L PEACE, 10-15 (2018), https://perma.cc/RNM9-SNTC.

54. Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*, N.Y. TIMES (Mar. 25, 2016), https://perma.cc/TF62-4Z8F.

55. MAURER, *supra* note 4, at 84-86.

56. *Id*. at 88.

57. *Id*. at 46, 94.

different from delegation or orchestration, because the state does not actively provide the non-state actor with support, but turns a blind eye to the non-state group's malicious activities.[58] A state may opt for this type of relationship as opposed to a delegation or orchestration-based relationship for a couple of reasons. If the non-state group's activities have widespread support among the domestic population, then clamping down on its activities could potentially create backlash.[59] In addition, the state may overlook the behavior of the non-state group because the non-state group indirectly allows the state to project a veneer of power that it may otherwise lack.[60] Finally, sanctioning behavior is seen as a more internationally palatable form of engagement with proxy groups than is more active support, such as orchestration or delegation.[61] For this reason, a state may wish to distance itself from proxy actors, while still benefitting from their offensive cyber operations.

States that sanction the behavior of cyber proxies include countries in the former Soviet Union, and Russia in particular. Maurer notes that the Russian government does not mind if hacking groups in Russia are conducting malicious cyber operations, so long as those operations are extraterritorial.[62] For example, in 2007 Russian groups launched a Distributed Denial of Service (DDoS) attack in Estonia, after the Estonian government decided to relocate a Soviet era statue from its capital city's downtown area.[63] The Russian government had warned against the move, but Estonia nevertheless proceeded to relocate the statue. Thereafter, Estonians found themselves without access to newspapers, bank accounts, government websites, and other parts of the internet. This attack was carried out by a pro-Russian youth movement, whose activities were consciously overlooked by the Russian government.[64] Maurer points to this example, along with Russia's involvement in Ukraine and Georgia, to argue that there is a consistent pattern of the Russian government sanctioning the behavior of cyber proxy groups.[65]

Although Maurer's examples point to clear cases of the Russian government sanctioning the behavior of its proxy groups, recent events involving the election interference investigation in the United States muddy those

58. *Id*. at 46-47.

59. For example, the activities of Al Qaeda in Pakistan or the Irish Republican Army in Ireland were sanctioned by the state in both countries.

60. Maurer refers to this difference as the "discrepancy between the state's projected capacity or aspirational status and its *de facto* capacity and power." MAURER, *supra* note 4, at 47.

61. *Id*.

62. *Id*. at 95 (quoting cybercrime expert Misha Glenny) ("Russian law enforcement and the FSB (Federal Security Service) in particular have a very good idea of what is going on and they are monitoring it, but as long as the fraud is restricted to other parts of the world they don't care.").

63. Emily Tamkin, *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?*, FOREIGN POLICY (Apr. 27, 2017, 8:30 AM), https://perma.cc/H6LM-LJGY.

64. MAURER, *supra* note 4, at 97.

65. *Id*. at 102 (noting that cyberattacks in Estonia, Georgia, and Ukraine are examples of sanctioning, and that the government was "fully aware of the malicious activities taking place yet [did] not act to stop malicious activity or to prosecute the hackers except in a few isolated cases").

waters. The Senate Select Committee on Intelligence in May of 2018 released an initial, unclassified finding of its investigation, concluding that "cyber actors affiliated with the Russian government" interfered in the United States' electoral process and successfully targeted the election systems of eighteen states.[66] Consequently, the Treasury Department sanctioned five entities along with nineteen individuals for their role in election interference.[67] As the character of the players used by the Russian government becomes clearer, we will know more about how the Russian government used such actors to conduct its offensive cyber operations on the U.S. election infrastructure. For now, what we do affirmatively know is that the Russian state does not merely tolerate the activities of non-state proxies but is also independently engaged in conducting its own transnational cyber operations through its own intelligence agencies.

C. Substantive Aims Behind the Different State-Proxy Relationships

Outside of just placing the various interactions between the nation-states vis-a-vis their proxies on a spectrum, Maurer also keys the reader into the ideological differences in how states see the role of cyber power as a tool in geopolitics. A state's relationship with its proxy can help explain the state's underlying substantive aims.How states characterize the use of cyber power, for example, is a telling indication of how they see the role of cyber power in organizing their own internal affairs. The United States and the other NATO members use the term "cybersecurity," whereas Russia and China opt for using the term "cyber information."[68] This distinction, though seemingly insignificant, is important because states such as the United States do not see cyber operations as tools for the mass surveillance and monitoring of information that could destabilize the state. That use of cyber operations is markedly different from how the United States and many of the European countries see the role of cyber power.

Countries that embrace their proxies in a close relationship, such as the United States, lean closer to the liberal democratic model.[69] In a liberal democracy, there are channels of accountability through which the government is held to account for its behavior. This in turn creates incentives for ensuring that proxy groups do not take rogue actions, and continue to sing to the tune of the state. Precisely how much influence a state's worldview has on its relationship with its proxy, though,

66. Senate Select Intelligence Committee, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations* 1 (May 8, 2018), https://perma.cc/T2ZV-HQWM.

67. Press Release, U.S. Dep't of Treasury, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber Attacks (Mar. 15, 2018), https://perma.cc/S5DK-42QX.

68. MAURER, *supra* note 4, at 50.

69. MAURER, *supra* note 4, at 79 ("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.").

is a question Maurer does not raise. For countries that are less free, the internet's role in the spread of information is a direct threat to their internal stability and a violation of the principle of non-interference.[70] As a result, the attacks from the less free countries tend to focus on information-spreading sources: newspapers,[71] the entertainment industry,[72] as well as broadcast networks.[73] Perhaps the best example of this is the 2014 attack on Sony Pictures Entertainment, in which the attackers erased over one hundred terabytes of data, released confidential documents of thousands of employees, and threatened more action if Sony released a satirical film about North Korea's Kim Jong Un called *The Interview*.[74]Maurer sees this incident as something that should more broadly be considered linked to a state's view of the role of information and the internet's role in spreading that information, which in turn can potentially undermine a state's tight grip over its civil society.[75]

Other states, particularly liberal democracies, disagree. For these states, the spread of information to countries that actively suppress information does not violate principles of sovereignty. Instead, the liberal democracies see their actions as permissible under Article 19 of the Universal Declaration of Human Rights, which provides that each person has a "right of freedom of opinion and expression," and encompassed within that broad right is the "freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[76] This means that one actor can characterize actions as genuine human rights concerns in the same instance that another can characterize those actions as an attack on its internal sphere.[77] At the least, explaining this dynamic in terms of how nation states view the role of cyber operations helps tether their actions to a more nuanced ideological underpinning. Understanding the motivations behind a state's reluctance to embrace the spread of information, for example, is critical for policymakers as they look into the

70. *Id*. at 51.

71. Paul Mozur, *China Appears to Attack GitHub by Diverting Web Traffic*, N.Y. TIMES (Mar. 30, 2015), https://perma.cc/D3DM-E44X. The Chinese government uses a firewall to prevent access to certain websites. GitHub, a popular software development platform, offers users an end-run around the censorship, by accessing mirrors of the blocked websites, such as the New York Times and BBC. The Chinese government launched a DDoS attack on the website in an attempt to bring it down and prevent it from offering access to censored content. *Id*.

72. Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, WASH. POST (Dec. 19, 2014), https://perma.cc/VF96-F4SP.

73. Gordon Corera, *How France's TV5 was Almost Destroyed by 'Russian Hackers'*, BBC NEWS (Oct. 10, 2016), https://perma.cc/A74B-WCHU.

74. *See* David Robb, *Sony Hack: A Timeline*, DEADLINE (Dec. 22, 2014, 1:25 PM), https://perma.cc/LRH9-5ZQZ; *see also* Catherine Shoard, *Sony Hack: The Plot To Kill The Interview–a Timeline So Far*, GUARDIAN (Dec. 18, 2014, 6:35 PM), http://www.theguardian.com/film/2014/dec/18/sony-hack-the-interview-timeline.

75. *See* MAURER, *supra* note 4, at 51.

76. Universal Declaration of Human Rights, G.A. Res. 217A, U.N. GAOR, 3d Sess., 1st plen. mtg., Art. 19, U.N. Doc. A/810 (Dec. 12, 1948).

77. MAURER, *supra* note 4, at 58 ("Analysts of Russian policy emphasize that the Russian government has been primarily concerned about internal stability and external efforts to undermine it.").

future for a possible international multilateral and multilayered agreement on the use of cyber power.

Aside and apart from how states view the role of information spreading, states have other underlying ideological motivations that explain their interaction with proxies. Countries that wish to influence geopolitics cheaply and with some degree of anonymity use cyber operations for geopolitical goals, too. For instance, an Iranian proxy group called Magic Kitten, which is separate from the State but has ties to the intelligence community in Iran, not only targets opposition leaders in Iran, but has conducted cyber operations in most Middle Eastern countries.[78] Elsewhere, the United Arab Emirates formed Dark Matter, a separate private sector company, hired former National Security Agency and Central Intelligence Agency employees, and has targeted foreign government ministries for geopolitical reasons.[79]

II. IMPLICATIONS OF CYBER PROXY RELATIONSHIPS AND HOW STATES CAN MANAGE THEIR BEHAVIOR

International law standards are currently weak and offer limited protection against cyber-attacks. In 2012, Professor Harold Koh, the then Department of State Legal Advisor, outlined the state of the law in cyberspace from the United States' perspective.[80] In a speech to the U.S. Cyber Command Inter-Agency Legal Conference, Koh argued that international law applies to cyberattacks, and there are rules that govern this emerging domain.[81] He noted that cyber activities can constitute a use of force in certain circumstances where those activities "proximately result in death, injury, or significant destruction," and that a state can respond to these attacks by exercising its self-defense right, limited by international law principles of necessity and proportionality.[82] Importantly, he explained that states can be held responsible for the activities of their proxies, if the State has sufficiently strong control over the proxy group which commits an internationally wrongful act.[83] However, attributing the cyber operation to a state

78. Anderson & Sadjapour, *supra* note 53, at 20-21.

79. Mark Mazzetti, Adam Goldman, Ronen Bergman & Nicole Perlroth, *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments*, N.Y. TIMES (Mar. 21, 2019), https://perma.cc/E3VL-SJA9.

80. Harold H. Koh, Legal Advisor, U.S. Dep't. of State, Remarks at USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012).

81. *Id.*

82. *Id.*

83. *Id.* ("If a State exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act, just as if official agents of the State itself had committed it."); Brian J. Egan, Harold Koh's successor as Legal Adviser to the Department of State, also made this point clear: "[C]yber 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." Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L. L. 169, 177 (2017). The flip side of this discussion is whether truly non-state cyber actors can themselves be held responsible, and whether their actions can trigger a states' right to use force against them. For an insightful discussion on this debate, see Matthew

remains difficult, because of the architecture and nature of the internet.[84] In simpler terms, cyber operations easily allow for anonymity of the attacker and conceal the location and the identity of the device that is the source of the harm. The upshot is that states which are behind the cyber operation can maintain their innocence and/or plausibly deny their involvement with a proxy group's operation. This is not to say that attribution itself is impossible, but to point out that attribution for cyber operations *can be* a painstaking and months long endeavor. And even where analysts are able to locate the source of the attack and tie the attack to a certain group, merely tracing the attack to a server within a country does not itself suggest a state's involvement. States can intelligently and effectively establish distance between the formal apparatus of the state and a private cyber proxy group's operations.

The fault lines of the debate, then, are mined at the crossroads of the outer limit of the harm cyber operations cause, whether the operation can be linked to a state, and what constitutes sufficient state control over the proxy group for assigning responsibility. As Maurer observes, states can either actively direct or offer passive support for cyber operations, but current international law standards on the concepts of direction and control are "so high that they are unlikely to be useful for most situations encountered by political decision-makers today."[85] Precisely because of the difficulty of assigning malicious behavior to a state, Maurer finds that there is an increased focus on the idea of due diligence, which asks of states to refrain from *knowingly* allowing cyber actors to fester in their territory and commit internationally wrongful acts.[86] As the International Court of Justice explained in *Corfu Channel*, every state has an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states."[87] The concept of due diligence, in turn, helps to offer a solution to the problem of attributing responsibility for an attack to a state.[88] That is, because of the difficulty of attributing a given act to a state, in the absence of which the victim state is unable to take legal countermeasures, the legal obligation arising out of the concept of due diligence can help solve that problem.[89]

But this legal obligation of preventing groups from operating within a country's territory is murky at best, and states lack a shared view of the obligations that derive from this concept.[90] In addition, resorting to a due diligence grounded

C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L. L. 421, 443-48 (2011).

84. *E.g.*, Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 5 (2015).

85. MAURER, *supra* note 4, at 129.

86. *Id.*

87. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (Apr. 9).

88. For a wider discussion, see Eric Talbot Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer*, 95 TEX. L. REV. 1555, 1558 (2017).

89. *Id.* at 1564-66 (2017).

90. For a good review on the limitations of the concept of due diligence, see Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L. L. 30, 53-55 (2018).

response will nevertheless allow the state responsible for undertaking the cyber operation to escape responsibility.[91] While Maurer acknowledges the various problems that the due diligence substitute poses as a solution to the attribution problem, his contribution is in suggesting a framework of actions that states can take in the period where the due diligence principle has not been incorporated to the cyberspace domain. Maurer suggests that states can adopt what he refers to as the DIML(LE) framework – focusing on diplomacy, information, military, economic, and law enforcement tools for influencing another state's relationship with its proxy.[92] For controlling proxies within their own borders, Maurer suggests that states should follow the U.S. model and hold proxies on a tighter leash.[93] This can take shape in several ways, including imposing reporting requirements on proxies and having discussions on how the goals of proxies remain aligned with those of the central government.[94] Facing this tall order, Maurer suggests that states should temper their expectations towards "being able to nudge rather than to dictate to others, and expecting to manage instead of prohibit[ing] the development and spread of cyber capabilities."[95]

III. COMMENTARY

Overall, Maurer's book is well researched and draws from a wide range of fields, from international relations and history to law. He gives readers a nuanced sense of how states interact with cyber proxies, together with a useful analytical framework for guiding future discussion on how the law should adapt to the architecture of state-proxy relationships. His contribution to the literature on how states interact with their proxies is timely, valuable, and future researchers can use his framework to develop a more empirical analysis of these relationships. Maurer also forces readers to think differently about how cyber proxies should be classified, asking them to push away from models that classify groups based on their intention. The narrative that a clear classification of non-state proxy groups based on intent is available to us is one without legs, since "[i]ntent is limited as a characteristic because proxies' motives may be multifaceted or may change over time."[96] Instead of simply rejecting an outdated approach, Maurer offers a fresh way of thinking about proxy relationships and details how international law can evolve to meet the resulting challenges. By doing so, he helps readers better understand how conduct in cyberspace is organized.

Nevertheless, Maurer's framework still raises important questions about whether certain groups should even be classified as proxies. WikiLeaks, for instance, can be classified in different ways, as journalistic and otherwise, but it also has the characteristics of a typical proxy group when acting as a conduit for

91. Jensen & Watts, *supra* note 88, at 1575.
92. MAURER, *supra* note 4, at 138-42.
93. *Id*. at 144.
94. *Id*.
95. *Id*. at 150.
96. *Id*. at 22.

state governments. For example, the Democratic National Committee (DNC) in the lead-up to the 2016 U.S. general election hired an intelligence firm to investigate some of its suspicions about a potential breach. The firm, CrowdStrike, determined that the Russian military intelligence and their primary intelligence agency were on the DNC's network, and used WikiLeaks as a distribution channel to leak internal emails and documents.[97] Later, U.S. intelligence services confirmed that the Russian state was responsible for the DNC hack and used WikiLeaks as a distribution source.[98]In his role as the Director of the Central Intelligence Agency, Mike Pompeo declared WikiLeaks to be a "non-state hostile intelligence service."[99] Maurer's typology as it stands would likely classifythe behavior of WikiLeaks as a cyber proxy group.[100] But WikiLeaks is not a cyber proxy group, and its status falls more appropriately in a gray zone – as a quasi-cyber proxy actor.

It also seems that Maurer is stretching the concept of cyber proxies too thin in order to accommodate the various state-proxy relationships in his framework. There is a big difference between the organization and operation of Raytheon, a private defense contractor which the United States government sometimes looks to for servicing its cyber operation needs, versus the Syrian Electronic Army, which describes itself as "a group of enthusiastic Syrian youths," and whose origins trace to minor DDoS attacks, which the Syrian President Bashar al-Assad publicly supports.[101] Treating Raytheon and the Syrian Electronic Army in kind as non-state proxy groups is a bit of a reach, because both groups share fundamentally different operations and have different relationships to the central government. Raytheon or the other private defense contractors used by the United States government help the government in meeting its cyber needs, but the offensive actions are nevertheless carried out by the central government. On the other hand, a non-state proxy such as the Syrian Electronic Army actively carries out the offensive cyber operation. And international law, too, would treat actions by these very different groups, with very different relationships to their sponsoring governments, very differently: For private military contractors, such as Raytheon, there are no international laws that *specifically* deal with their activities, but there have been plenty of attempts to regulate the behavior

97. David E. Sanger & Nick Corasaniti, *D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump*, N.Y. TIMES (June 14, 2016), https://perma.cc/4KPP-TB8H; Julian Assange, the founder of WikiLeaks, denies this. When asked about his source behind the leak, he stated: "Our source is not the Russian government and it is not [a] state party." Fox News, *Julian Assange: Our Source is Not the Russian Government*, YOUTUBE (Dec. 15, 2016), https://www.youtube.com/watch?v=Kc0AKGJwX9o.

98. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections" : The Analytic Process and Cyber Incident Attribution* (Jan. 6, 2017), https://perma.cc/7UMA-KYX5.

99. Matthew Rosenberg, *Mike Pompeo, Once a WikiLeaks Fan, Attacks It as Hostile Agent*, N.Y. TIMES (Apr. 13, 2017), https://perma.cc/EU7D-YB7D.

100. *See supra* Part I.B, for a discussion on how Maurer defines proxies.

101. MAURER, *supra* note 4, at 89.

of mercenaries.[102] The International Convention Against the Recruitment, Use, Financing, and Training of Mercenaries, adopted in 1989, provides that no state shall "recruit, use, finance, or train mercenaries and shall prohibit such activities . . . ."[103] Proxy groups, however, are able to escape the application of those laws.

Additionally, Maurer perhaps does not fully account for the motivations that drive states to interact with cyber mercenary groups. A key part of Maurer's argument is that some states are motivated by regime stability as the driving concern behind their cyber operations. This is to say that domestic concerns predominate in a state's use of cyber operations.[104] Maurer writes that the Russian government is "primarily concerned about internal stability and external efforts to undermine it," and further argues that events such as the removal of Ukrainian president Viktor Yanukovych—who remained a key ally of the Russian government—led to a new vision of Russia's approach to cybersecurity, which revealed its focus on "territorial integrity" in response to a "heightened sense of threat."[105] But states like Russia are driven by other objectives, too, and ascribing a predominant intent to their actions is difficult at this point. One could just as easily point in the direction of Russian's cyber operations in Ukraine—or, for that matter, in Estonia and Georgia—and argue that the driving motive is for a return to a greater power status.[106] Considered within Maurer's framework of state-proxy relationships in cyber operations, and realizing that the actions of certain states can also be driven by "status ambition,"[107] suggests that the relationship between the Russian government and its cyber proxies may be one of orchestration as much as sanctioning. Expressed differently, Russia does not simply sanction the behavior of cyber proxies, but actively orchestrates the behavior of its proxies to meet

102. *See*, *e.g.*, Natasha Arnpriester, *Combating Impunity: The Private Military Industry, Human Rights, and the "Legal Gap,"* 38 U. PA. J. INT'L L. 1189, 1209 (2017) (discussing the "legal gap" in which private military contractors operate); Marie-France Major, *Mercenaries and International Law*, 22 GA. J. INT'L & COMP. L. 103, 108 (1992) (discussing the various attempts at regulating the conduct of mercenaries).

103. G.A. Res. 44/34, U.N. GAOR 6th Comm., 44th Sess., 72d plen. mtg., Annex, Agenda Item 144, U.N.Doc. A/44/766 (1989).

104. MAURER, *supra* note 4, at 58, 61, 81 (discussing the view that Russia, China, Iran are motivated by an internal regime stability in their cyber operations).

105. *Id*. at 58, 60.

106. *See* Deborah Welch Larson & Alexei Shevchenko, *Status Seekers: Chinese and Russian Responses to U.S. Primacy*, 34 INT'L SEC. 63, 67 (2010) (arguing that there was an effort to expand Russia's sphere of influence because of the failure on part of Western countries to grant Russia status as a great power.); Ruth Deyermond, *What are Russia's Real Motivations in Ukraine? We Need to Understand Them*, GUARDIAN (Apr. 27, 2014, 8:59 AM), https://www.theguardian.com/commentisfree/2014/apr/27/russia-motivations-ukraine-crisis ("[T]he objectives of the Putin government appear to be both limited and rational: the protection of its regional security interests and great power status.").

107. STEVEN WARD, STATUS AND THE CHALLENGE OF RISING POWER 210 (2017) ("Contemporary Russia is not a rising power and has not been one for decades, but for much of its post-Cold War history, Russian foreign policy has been aimed at reestablishing Russia's position as a great power."). Ward also thinks that Russia's eastward move was a result of the "threat to Russian status ambition" and explains Russian action in Georgia and Ukraine. *Id*.

its geopolitical vision.[108] Maurer does account for this, however, by noting that there is disagreement on whether the relationship between the Russian government and its proxies during the 2008 Russo-Georgian war, whose cyber component included a DDoS attack, was a case of orchestration or sanctioning.[109]

On a final note, fully expressed with the understanding that one book can only cover so much ground, Maurer's research raises an important though unanswered question: Are states responding to the shifting international legal landscape which classifies the conduct of mercenaries as forbidden, but does not expressly prohibit the use of proxy groups, by changing the very nature of those relationships? That is, are states increasingly using private sector proxy actors because international law has not yet caught up to the changing ground realties? And moreover, once the international law framework does catch up, how will states then adapt their association with proxy groups? Perhaps these are questions better suited for a fuller exploration in another project.

CONCLUSION

Today nation states can develop cyber capabilities quickly. Already, there are over sixty countries that are developing tools for cyber operations, twenty-nine of which have formal military or intelligence cyber units.[110] Against the backdrop of this new reality, where the line between non-state and state actors is fast blurring, comes Maurer's take on the framework of the relationships between states and their cyber proxies. Embedded within this framework are answers that reveal how states today think about projecting power, retaining a semblance of plausible deniability, and using non-state groups in different ways. In this area, still, there are challenges that remain: the current international law framework remains weak, states continue to disagree on basic norms of responsible behavior in cyberspace, and risks of escalation have increased in an environment where access to tools for cyber operations are easy to acquire and cheap to operate. Maurer deftly navigates the challenges and presents his take in sober terms.

108. For more on this discussion of Russia's active involvement in offensive cyber operations, see *supra*, Part I.2.C.

109. MAURER, *supra* note 4, at 101.

110. Jennifer Valentino-DeVries & Danny Yadron, *Cataloging the World's Cyberforces*, WALL ST. J. (Oct. 11, 2015, 8:45 PM), https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

***