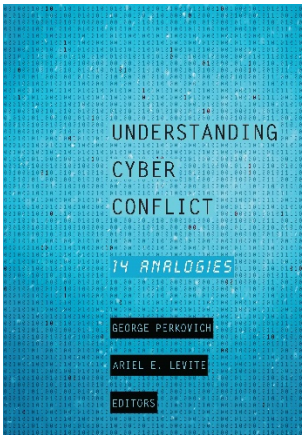

Cybersecurity and the Age of Privateering

Florian Egloff

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



14 Cybersecurity and the Age of Privateering

FLORIAN EGLOFF

> The seas around the world are, much like the cyber domain, not governed by one single nation. We have created maritime norms and have to do the same in the cyber space to ensure a flow of information and ideas.
>
> ADM. MIKE ROGERS

Between the thirteenth and mid-nineteenth centuries, privateering was an established state practice. Privateers (privately owned vessels that operated against an enemy with the license or commission of the government in times of war) would be used to attack the enemy's trade. In peacetime the practice of reprisal represented the means to seek redress against the harm suffered by another nation's ships at sea. A letter of marque allowed merchants to attack any ship of the offending nation until they found something of equal value to their loss.

Two months after the 2007 cyber attacks on the small Baltic country of Estonia, Defense Minister Jaak Aaviksoo used the analogy to privateering in a speech, pointing to the 1856 Declaration Respecting Maritime Law that abolished privateering.[1] He suggested that similar norms of the maritime environment were needed in cyberspace. At the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence in Estonia in 2015, Adm. Mike Rogers also referred to maritime norms when thinking about norm development for cyberspace. Policymakers' hopefulness about the analogy to the seas is understandable; maritime trade is relatively peaceful after all. However, the historical record indicates that such norms did not develop quickly nor was the process of attaining them a peaceful one. On the contrary, once a private system of force was created, states were not able to control the use of force completely. This chapter argues that the study of the historical evolution of the private system of force in maritime history offers important lessons for analyzing and shaping the evolution of cybersecurity. Scholars have used the analogy to privateering to recommend, or dismiss, the issuance of letters of marque to private companies in cyberspace.[2] At the same time, various experts have used the analogy to describe the collusion between attackers and states.[3] Thus, it may be important

to explore what can be learned from the rich history of privateering, in this instance mainly from British maritime history.[4]

A longitudinal view of history is necessary to understand the development of norms against privateering. Privateering evolved from an institution that profited merchants and the Crown to one posing a threat to English naval dominance. A similar struggle is taking place today in cybersecurity. Protection from threats propagating through cyberspace has been treated as a predominantly private undertaking. At the same time, non-state actors are exploiting the insecurities of cyberspace, with the potential disregard of state versus state normative frameworks. The institution of privateering can shed light on the aligned and conflicting incentives involved for both state and non-state parties, when defensive and offensive regimes are in place and where the responsibilities of both actors are blurred. Thus, the opportunities and risks of using privateers can be explained with the aid of historical examples, and the information can then be applied to the modern-day problems of the cyber realm.

The analogy is both historical and conceptual. It makes recourse to an older world in which states were weak players when it came to the exploitation of the seas. Conceptually, the analogy points to the differing degrees of involvement and control that states can have with actors who exploit largely ungoverned spaces, such as the cyber domain. By examining the historical trajectory of privateering, we can learn from the intended and unintended consequences that the presence of such actors produced.

The analogy can shed light on specific aspects of the cyber challenge. First, it gives an insight into a system in which lines between state and non-state actors are blurred. Next, it focuses on a key aspect of the mercantilist system—that is, the economic and political realms are not differentiated. Thus, it captures two of the most important peacetime cyber challenges—cybercrime and cyber-enabled economic espionage. Finally, the analogy improves the understanding of security dynamics in a system in which capabilities are distributed among various actors. The comparison to a time in which semi-state actors (such as privateers and mercantile companies) and non-state actors (such as pirates) were abundant provides key insights into the conflicting objectives between the competition for advantage and the stability of and reliance on a system of trade.

This chapter begins with a short history of privateering and identifies the analogies found in the cybersecurity challenges. It then unravels the similarities and differences, sets up conceptual frameworks, and points to policy implications. The chapter closes with identifying the advantages and disadvantages of the analogy to privateering.

Historical Background

In the fifteenth and sixteenth centuries, several developments concurrently led to an increase in European exploitation of the seas. Shipping technology advanced so that long-distance sailing and war-fighting possibilities became more viable. At

the same time a will to explore, proselytize, and conquer led seafarers into new territories.[5] Financed by investing parties who expected lucrative returns, and backed by their respective sovereigns to attack both locals and rivals, privateers represented the early means of colonial expansion. The era of the mercantile companies had begun. Mercantile companies operated by their own international policies. Merchants had to provide their own protection outside of territorial waters. They made deals with other companies or states, or were at war with them, and engaged in open warfare, piracy, and privateering, sometimes independently and against the interests of their home states.

In English history, privateering is best known through the acts of the Elizabethan sea dogs. The voyages of Sir John Hawkins, Sir Francis Drake, and Sir Walter Raleigh not only brought wealth to themselves and their investors but also inspired subsequent generations of English singers and playwrights. Besides their voyages against the Spanish in the New World, the English privateers formed a key part in the still fledgling Royal Navy. The English thus also used the skills and experience of the privateers, gained in attacking commerce abroad, for the defense of the home country.[6] For example, Sir Francis Drake and Sir John Hawkins served in the Royal Navy to fight against the Spanish Armada. Thus, privateering was used to augment national strength both militarily and through its cultural contribution to national identity.

Privateering also brought disadvantages. For one, it was a lucrative undertaking for the sailors. As a privateer also enjoyed better food and took a higher share in the prizes than he would in the Royal Navy, many of the ablest seamen served as privateers, not as sailors in the navy. Over time, the Royal Navy addressed the competition for skilled labor by forcing sailors to join the navy (impressment) and by improving working conditions on royal vessels.

The state also tried to regulate the number of sailors involved in privateering and the targets that would be attacked by issuing privateering licenses; however, effective control was not guaranteed. For example, after being knighted for his services to the court, the notorious privateer Raleigh did not stop looting, even after the peace treaty between James I and King Philip III of Spain.[7] Finally, James I had Raleigh executed. This episode illustrates one of the problems that eventually contributed to the abolition of privateering—that is, the difficulty of controlling privateers.[8] The longer wars lasted, the more privateering was professionalized and institutionalized. At the end of wars, privateers were integrated into the navy, worked on merchant ships, or became pirates.[9] The line between privateering and pirating was blurred. As Fernand Braudel noted, pirates could serve as a "substitute for declared war."[10]

Privateering as a strategy of war could distract from the more formal naval efforts of building a battle fleet. During the late seventeenth century, French privateers (corsairs and *filibustiers*) became increasingly active. While English privateers were used as a tool of influence alongside the growing navy, the corsairs were used as a primary tool of naval warfare (*guerre de course*).[11] For France they provided an ideal weapon against the English, who, comparatively, relied more on foreign trade.[12] However, this emphasis on the *guerre de course*, which

was supported by the profiting investment circles, shifted (limited) funds and efforts away from building a more formal naval capacity.[13]

By the end of the eighteenth century, mostly the United States (in the War for Independence) and France (in the French Revolutionary Wars and later in the Napoleonic Wars) employed privateers against Britain. Privateering had "evolved into a weapon of the weak against the strong." However, "it was invented and encouraged by the 'strong' states of Europe, whose naval power was largely an outgrowth of privateering."[14]

The Congress of Paris decided to abolish privateering at its meeting for a settlement of the Crimean War in 1856. In the deal Britain, the dominant sea power, committed to protect neutral commerce, and, in return, the other powers relinquished the right to privateering. The settlement also represented a move against the United States, which still relied on turning its large merchant cruisers into privateers in case of naval conflict.[15] When the declaration passed, it was widely circulated so that as many powers as possible would accede. The parties of the declaration agreed that no port could receive privateers. Thus, privateering was made practically impossible also for non-signatories of the agreement, as a privateer would have to return to his home state to sell his prizes. During the US Civil War, the Northern states considered signing the Declaration of Paris to prevent the Southern states from using privateers against commerce. At that time, though, the two parties were already in a state of belligerency, thereby losing the right of signing away rights for the other party.[16] Hence, the United States never acceded to the declaration.

The Cyber Analogy

Looking at more recent technological development, the invention of the World Wide Web and the subsequent commercialization and expansion of cyberspace have rendered societies increasingly dependent on networked functionalities. Similar to the sailors' early expansionary years of activity on the seas, the users of cyberspace are largely left to protect themselves. Absent a state capacity providing redress, users must rely on their own abilities to withstand threats propagating through cyberspace. In such an environment, defensive and offensive skills are sought by a variety of actors. Just as mercantile companies could not rely on the Royal Navy to protect their trade and hence armed their merchant navy and sometimes sought protection from private men-of-war, large companies today seek to attract some of the most skilled cybersecurity experts.

Thus, a policy debate has arisen about the extent to which companies can protect themselves against state-directed attacks and about whether private actors should be engaged in hacking back.[17] Whether a private company can defend itself from a state-directed attack depends on the intent and capacity of the attacking state and the defensive capabilities of the company. If a company with a high cybersecurity maturity is a generic target, then it may be able to dissuade an attacker by making itself a hard target. However, when private companies are the direct target of a motivated, well-resourced state attacker, their

defensive capabilities will not deter the attacker. Companies need additional backup capabilities, which are traditionally reserved for states. The debate on hacking back often fails to explain what the aims of such an action might be for a private company. Is it to impose costs on the attacker? Is it to help determine the attribution of the attack to a particular actor? Is it to research the motivation of the attack? Given the uncertainty about the ramifications of any offensive or retaliatory actions against an attacker, it is unclear to what extent private actors would deem such actions to be in their interests. Nevertheless, the US government dissuades corporate hacking back by claiming it is illegal under the Computer Fraud and Abuse Act and by highlighting the danger of escalation against unknown adversaries.[18]

Many states are currently building their capacities to conduct offensive and defensive cyber operations. The growing state capacities in defending against and carrying out cyber attacks may be augmented by the experience of private actors. The interests of skilled personnel and governments can overlap in various ways. First, instead of recruiting personnel for governmental positions, governments rely on the support of private personnel in several countries. Countries depend on a form of national service (e.g., formalized cyber militias), the use of contractors to buy key capacities (e.g., zero-day exploits), or the use of a range of services offered in the cyber criminal underground as part of the tool set for state exploitation of the cyber realm.

Second, there is the phenomenon of so-called patriotic hackers. Working in the political and economic interests of a country, patriotic hackers have been active in many highly visible cases ranging from the Russian hackers' attacks on Estonia in 2007 and on Georgia in 2008 to the Chinese and US hackers' attacks after the Chinese Embassy's bombing in 1999 and the Hainan spy plane incident in 2001.

Third, and less evident than the highly visible and clearly politically motivated attacks, groups have also mounted criminal intelligence-collection efforts.[19] For example, allegations have been made of close alignment between Russian and eastern European cyber criminal networks and Russian state interests. The influence and direction of criminal activity are multilayered, ranging from discretionary enforcement based on the targets selected to the way in which cyber criminals have become active in Russian political interests.[20] Empirical evidence, however, is usually incomplete and open to interpretation. For example, Ronald Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata found no direct evidence linking the Russian government to the electronic attacks in Georgia in 2008, but they did not rule out the possibility that Russia quietly encouraged "malicious actions by seeding instructions on Russian hacker and nationalist forums and through other channels."[21] Tacit support can be inferred when governments do not cooperate and prosecute identified criminals in the presence of a mutual legal assistance treaty.

Reports also indicate an increase in attacks toward economic targets, focusing on economic espionage and intellectual property theft. The cultivation and utilization of private talent to effect economic wealth transfer comes closest to a

modern version of privateering. Thus, at their own risk, companies, hacker groups, and some cyber criminals engage to fulfill state-sponsored goals against the interests of other commercial and noncommercial entities. The profit motives for both the state and hacker groups can differ from those of privateers. In cyberspace, states may profit indirectly by gaining plausible deniability for their own activities by hiding behind criminal hacker groups in return for tolerating their criminal activity, whereas in the case of privateering, states directly encouraged the profit-generating criminal activity.

Similarity of Regulatory Challenges

Having identified the analogical structure of the two domains, the focus now shifts to the similarities of the challenges states have faced on the sea and in cyberspace. Neither domain was controllable by a single actor, skills for deploying force mainly rested with semi-state actors, and the state alone lacked the capability or will to protect private entities. A broad range of actors was engaged in exploiting the new possibilities offered by transoceanic trade, with some having more legitimacy than others. As trade on the sea and dependence on cyberspace increased, the respective attack surfaces increased also. Therefore, states built dedicated capabilities to project force through navies and their cyber equivalents. These capabilities, however, had to coexist and compete with their private equivalents.

In the maritime space, one important factor for a navy's mobilization potential was the total number of its able seamen. Thus, countries with larger merchant fleets could draw on a larger number of able seamen. Wartime demand usually exceeded peacetime supply.[22] As a conflict began, therefore, the speed of mobilization determined who could project naval power quickly. For example, the French "système des classes . . . could recruit men up to a certain level of manpower, faster than the British practice of bounties backed by the press"; hence, France had an advantage at the beginning of the mobilization.[23] However, due to the larger number of total able seamen, the British would enjoy an advantage in the later stages of mobilization.

At this time, how this issue applies to cyber capacities is unclear. The focus on human capital is analogous, for cyber capacities are predominantly reflected in skilled manpower; however, it is not clear which specific skills a cyber operator would need to be considered a quickly mobilized capacity (in analogy to the able seamen). One reason is that offensive and defensive skills may be more distinguishable in cybersecurity than they were in naval warfare. Hence, while one can assume that a country with a large information technology sector would have an advantage in recruiting people with the necessary skills, the time lags and transformation potentials remain unexplored.

Unintended consequences of using privateers continued to create difficulties for the states that employed them, thus leading states to regulate the practice over time. As states build their own cyber capacities, their acceptance of the unintended consequences of private activities (be they commercial or

criminal) may decrease. As all states grow more dependent on cyberspace, a window of opportunity for some agreement and cooperation in the cybercriminal space may arise. However, as the history of piracy has shown, the levels of protection for cybercriminals may ebb and flow along with the political tensions of the time.

On the seas, the involvement of private force continued to play a role up to the early nineteenth century. Privateering was abolished only when the dominant naval force, Britain, decided that, due to its reliance on global trade, maintaining the option of private attacks against commerce was strategically and ideologically against its interests.[24] This deal did not include the United States, a rising power that was more reliant on its merchant cruisers in wartime. However, in return for the smaller powers' agreement, the dominant sea power struck a deal whereby it committed to a more protected space for neutral trade.

The cybersecurity space is far removed from any international legal agreement settling cyber conflict. While the analogy would suggest that states learn from unintended consequences over time, they do so slowly. Thus, for some years, cyberspace may stay a relatively chaotic environment with an abundance of players present. If there is to be some sort of agreement, the analogy indicates that it does not necessarily have to include all the major powers. Leaving out one and building an effective regime constraining the usefulness of cyber attacks may suffice.

In 2015 Presidents Xi Jinping and Barack Obama agreed that their respective governments would not engage or knowingly support commercial espionage.[25] Commercial espionage was undertaken by different hackers, including some from the People's Liberation Army (PLA). Curtailing commercial espionage would then hurt the hackers' private income. Thus, given the regional power structure in the PLA, even if Xi wanted to halt this practice, he would likely face resistance.[26] As this practice has persisted for a number of years, the livelihoods and constituencies connected to the income streams need to be considered. There are strong similarities to stopping piracy, which involved a balancing act between building an alternative future for pirate communities and curbing their resistance. One theory holds that China will increasingly crack down on the work of freelancers while at the same time professionalizing the operational security of the state-conducted commercial espionage. This would mirror the British policies of the 1750s that raised the entry barriers for privateers and rendered the practice more regulated.

Differences between the Oceanic and Cyber Challenges

Having discussed the similarities between the two security spaces, we now address their differences. First, the pace of technological innovation seems faster in cyberspace than in shipbuilding. This observation has to be analyzed in conjunction with the more rapid diffusion of information and knowledge in the contemporary age. While the advancement in shipbuilding (e.g., the dreadnaught) gave the English an advantage for many years, a new cyber capability,

once discovered, may be repurposed by many actors within a very short time frame.[27]

Second, on the seas, human attackers expose themselves to physical risks. When an attack fails, the privateers face retribution. With remote attacks through cyberspace, this is not the case. Even if an attack is successfully traced to the responsible individuals, they may have the protection of their home state and may therefore be unreachable for prosecution.[28] This difference increases the prospects of the problem being more persistent in cybersecurity than on the seas.

Third, cyberspace widely differs from the sea because its topography is artificial; hence, it is malleable by human practice. Both technological and social changes manifest themselves in cyberspace and can change the "environment" in many, not always predictable, ways. Introducing new security-oriented technical protocols, hardware, and software for defensive purposes is a theoretical possibility. Research in networking has proposed models for new types of Internet routing; many of these proposals use security properties as guiding principles for their designs.[29] If implemented, they could contribute to a more secure environment, offering users a more explicit way of making decisions about whom to trust.

However, its malleability also means that the characteristics of cyberspace will significantly change over the coming years too. As the next two billion human users and twenty billion devices come online, the degree with which one can compare the maritime and cyber domains may change. Meanwhile, as the connectivity of societies deepens, access to security and surveillance technologies also spreads. This has already led to a balancing of the playing field in that surveillance technologies become more readily available to countries with traditionally more limited signals intelligence capabilities. Furthermore, this market is not limited to state actors, as non-state actors use some of the same technologies for defensive and offensive purposes.

Even though in many ways the cybersecurity environment seems far removed from the naval field, a lesson can still be learned. When operating in an actor-rich environment, states will not be able to control the use of cyber attacks completely. Once a system of private force is created, the institutional legacy carries forward. What state actors can do is manage the incentives, both for domestic and international actors, for using cyber attacks.

Conceptualizing the Range of Non-state and State Actors

Stepping back from the specific comparison of privateering and cybersecurity, a conceptual framework of a range of actors can capture the full potential of the analogy to the sea. In this framework, the navy, mercantile companies, privateers, and pirates are categorized according to their level of cooperation with state actors (see table 14.1).

In cyberspace, to be considered a state actor, an entity must be part of the state's organs or in direct support thereof. They are distinguished from semi-state actors that are in a close relationship with the state and sometimes advance

Table 14.1. Comparison between actors on the sea and in cyberspace

Actor type	Sea	Cyberspace
State actors	Navy (including mercenaries)	Cyber armies, intelligence, police forces, contractors, offensive security providers
Semi-state actors	Mercantile companies	Technology champions, major telecommunications companies, security vendors
	Privateers	Patriotic hackers Some cybercriminal elements
Non-state actors	Pirates	Hackers, cybercriminal elements (including organized crime)

state interests but are not organizationally integrated in state functions. Non-state actors have interests that lie outside the formal activities of a state and might reject the state's authority to govern their activities. Nevertheless, non-state actors may sometimes be in complicated relationships with states, reciprocally enabling the pursuit of respective interests. Simplifying the different relationships into three categories sufficiently captures the intuition that while some actors might be officially non-state actors, they are deeply entangled with states.[30] Overall, only those actors that directly interfere with another group's or individual's security interests are in scope.

This conceptual framework enables the analysis of different actors in cyberspace, highlighting how they are connected to the state. Importantly, the concepts do not carry an inherent moral value. The concepts of the navy, mercantile company, privateer, and pirate are understood to be by themselves morally empty. This reflects a historical understanding of them: some viewed privateers as heroes; others thought of them as criminals.

This conceptual framework enables multiple new types of analyses. It facilitates the tracing of state and semi-/non-state capabilities for deploying insecurity over time. This, along with a historical explanation of how it came about (including incentives, feedback loops, and normative changes), gives rise to a holistic analysis of the cybersecurity space. For example, figure 14.1 maps the state, semi-state, and non-state capabilities present in the international system over time and provides a richer understanding of the evolutionary development of the security dynamics. As the contemporary era witnesses a transfer from the high semi-state/non-state and low state capability quadrant to the high state and high semi-state/non-state capability quadrant, more conflicts between the different types of actors are to be anticipated. For example, as states build dedicated capabilities, they decrease their dependence on semi-state actors. This shift could be associated with a consolidation of activity in which a state cracks down on previously tolerated or sanctioned activity. One example might be China's arrest of cyber criminals after signing the Obama-Xi agreement.[31]

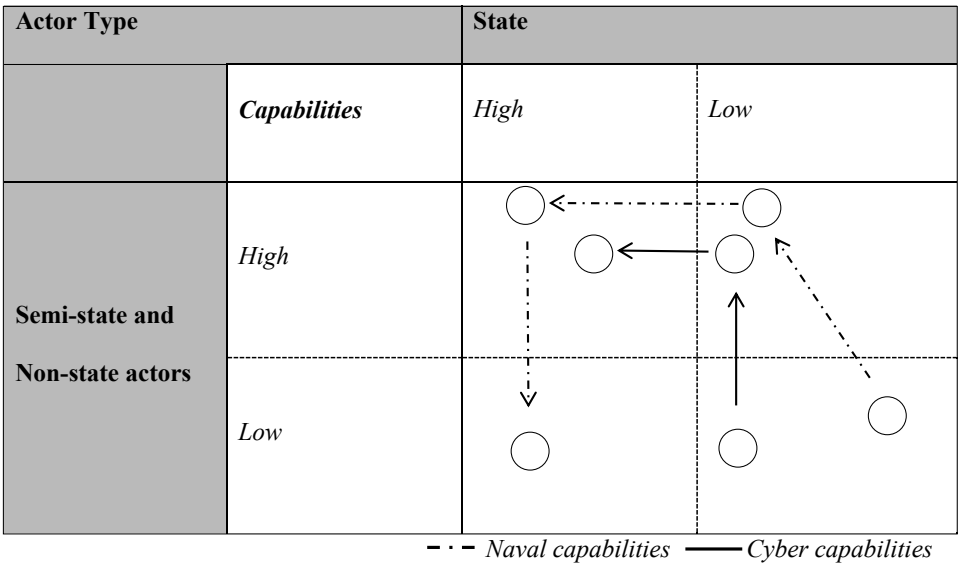


Figure 14.1. State and semi-/non-state capabilities on the sea and in cyberspace over time

In a second step, the state proximity framework categories can be used to analyze the interactions between state, semi-state, and non-state actors. Lucas Kello argues that while competition between states exists, cyber insecurity has also accentuated a new state of nature involving non-state actors.[32] This global state of nature can be analyzed using the state, semi-state, and non-state framework, both for where the actors' interests collide and for where they converge. Regarding collision, the question to ask is, where is a respective actor considered the attacker and where is it the target? (See figure 14.2.)

Mapping some of the most prolific cyber attacks onto the categories identified reveals a clearer picture of the complexity of responding to cyber attacks. Each category of constellations involves different challenges for the attacked party. The framework presented reduces complexity to aid policymakers in anticipating different constellations of attackers and defenders. For example, with this framework, governments could have anticipated the Sony Pictures Entertainment and Sands Casino scenarios and considered possible policy responses. Privateering cases suggest that when the attacker has a special relationship to a state, rather than going after the attackers through the criminal prosecution system, the state must address the situation politically. For example, in the case of the attacks against the Sands Casino, allegedly conducted by hackers connected to the Iranian government, the prosecution of cybercriminals only through the legal system would not have been a fruitful response. The attack against a private corporation in this case took on a new form of signaling discontent.[33] As such, the response must address both the criminal as well as the political aspects of the actions, using the full range of policy options available.[34]

		TARGETS		
	Actor Type	***State***	***Semi-state***	***Non-state***
ATTACKERS	***State***	Stuxnet GhostNet	US → Huawei China → Google, Lockheed (e.g. Titan Rain, Operation Aurora)	PLA → Tibetan activists (GhostNet) North Korea → Sony Pictures
	Semi-state	Patriotic hackers → Estonia Iranian "hackers" → Saudi (Shamoon)		Russian "hackers" → JPMorgan Chase Iran → Sands Casino Cybercrime
	Non-state	ISIS → US Strategic Command	ISIS → AP Hacker → HackingTeam & Gamma International	Cybercrime Anonymous → Scientology Ashley Madison
	Unknown			Advanced persistent threat → German steel factory

Figure 14.2. Collision of interests between state, semi-state, and non-state actors

The framework enables the development of a better-prepared response to the next novel situation that policymakers and business leaders may encounter. It also helps the analyst to categorize the different reactions so as to keep an overview of how attacks are being treated. Thus, the semi-state category allows for a more adequate capturing of the politicized activities below the threshold of war.

When considering where the interests of the different actors converge, the question to ask is, who is seeking assistance and who is providing it? (See figure 14.3.)

		SUPPLY OF COOPERATION		
	Actor Types	***State***	***Semi-state***	***Non-state***
DEMAND FOR COOPERATION	***State***	Five Eyes	US ↔ companies in PRISM program China ↔ Huawei Russia ↔ Patriotic hackers?	Iran ↔ hackers Russia ↔ cybercrime US ↔ Hector Monsegur (Sabu)
	Semi-state	Google ↔ US (Operation Aurora) UK ↔ Huawei		
	Non-state	Sony Pictures ↔ US Cybercrime ↔ Russia		WikiLeaks ↔ Anonymous

Figure 14.3. Convergence of interests between state, semi-state, and non-state actors

Mapping some of the prolific cooperation cases onto the matrix shows various constellations that would be missed if one focused on only state-level capabilities. For example, the cooperation between technology or telecommunications service providers and states is an area that requires careful research. When US telecom providers cooperate with the US government to facilitate intelligence collection, it can violate the privacy guarantees given to the customers.[35] Similarly, the cooperation between hackers or cyber criminals and states is of interest. Examples are the aforementioned alignment of cyber criminals with Russian interests or the use of convicted hackers as informants to coordinate cyber attacks as in the case of the Federal Bureau of Investigation and Hector Xavier Monsegur (Sabu).[36]

Akin to the collision model, some of the constellations can be analyzed with the analogy to the sea. Analogizing the category of semi-state actors, or privateers and mercantile companies, and the non-state category, or the experience with pirates, allows for a richer understanding of the political and security dynamics at play in each case. In both models, constellations indicate the presence of dynamics not only of an old state-versus-state type of interaction but also of a new type of state of nature, one involving state, semi-state, and non-state actors. Through these models, the analogy can provide context and reduce complexity. It can aid policymakers in developing a strategic vision of a desirable state for the domain, including their abilities and constraints to shape the emerging normative framework.

Conclusion

The analogy to privateering has elucidated some cybersecurity challenges. Learning from four hundred years of history allows for a rich understanding of the forces giving rise to the multiplicity of actors shaping the institution of privateering and eventually leading to its abolishment. Similarly, the forces enabling and constraining the different types of actors that are active in the cybersecurity space can be identified. First, actors in cyberspace have similar proximity to the state as the mercantile companies, pirates, and privateers did in the sixteenth and seventeenth centuries. This conceptualization of actors in cyberspace captures both the expansion of transnational non-state actor activity and the devolution of responsibilities and authority to private actors.[37] The frameworks of analysis including state, semi-state, and non-state actors can reduce complexity and aid the development of a strategic vision for the domain.

Second, the levels of state capacity in cybersecurity resemble the situation in the sixteenth century, when some states transitioned from the use of privateers to professional navies. In naval warfare, this transition reduced the interest in the use of non-state actors. Judging by this process, the cyber capacities of state actors are in their infancy. The increasing dependence on cyberspace of all societies and the growth in state capability could have positive consequences for a cybercrime regime, as it could be accompanied by a decreasing interest in the

use of non-state actors. However, the declining interest in the use of non-state actors is not guaranteed. Some states may still opt for a *guerre de course*.

Third, the analysis of the regime against privateering has shown that it can be traced to unintended consequences of state-sponsored and state-tolerated non-state violence, coupled with a growth of commercial opportunities for sailors. Similarly, in cyberspace one might expect unintended consequences to increase over time. Whether states will be able to coordinate their behavior to control these unintended consequences while preserving the positive effects of cyberspace remains an open question.

An awareness of the advantages and disadvantages of specific analogies is vital. It is important to clarify the type of knowledge an analogy can facilitate and where an analogy may mislead. The analogy to privateering is helpful because of the temporal distance between the two spaces, the possibility that this analogy invites long-term perspectives, and the fact that the policy innovations to redress the problems of privateering can be instructive in dealing with the cyber domain.

A comparison to a time that has long passed has a pragmatic and an analytical benefit. The pragmatic benefit is that it can depoliticize the debate and thereby focus the attention on the analytical problem at hand. The analytical benefit lies primarily in the integration of different actor types in a security space, where states are just starting to build capacities to project force.

The analogy reveals the long-term evolution of security dynamics in a space that becomes more important to the stakeholders over time. An ecosystem of security actors does not change quickly; rather, it evolves. Unintended consequences, feedback loops, and conflicting objectives influence how actors' policies change with time. In addition, the concurrent growing importance of the domain to all the actors raises the stakes and creates incentives to stabilize the domain. However, the decreasing interest in the use of non-state actors is not guaranteed.

There are some insights for more imminent policies. Particularly, the challenges in recruitment—both for states and non-state actors—can be better understood with the aid of the analogy. The analogy suggests that competition for skilled personnel is persistent and influences the way a formal state capacity can be developed. The analogy offers some appreciation for the various ways in which states have tried to work with skilled personnel (be it militias, volunteers, public-private partnerships, contractors, or army personnel). Linked to this aspect is the risk of policymakers profiting financially from cybersecurity policies. It is important to understand why some governments seem to enable economic and commercial espionage. Also, the job prospects of policymakers once they leave governmental employment have to be carefully evaluated. Parties that invested in privateering may shed some light on how governments are persuaded to sanction policies from which both officials and private corporations can profit. For example, critics of privateering argued that commerce raiding diluted the state's efforts to build an effective state-owned warfare capability.

The privateering analogy poses hazards too. Among them are the risks of further militarizing the discourse on cybersecurity, of advocating empire, and of assuming that history will predict the future.

The analogy considers cyberspace in relation to another relatively aggressive and militarized discourse. Civilian analogies may be more productive in creating opportunities for dialogue and cooperative solutions. Thus, other, more peaceful analogies could be more desirable in the context of a multilateral forum when looking to reshape the perception of the cybersecurity problem and to extend the possible range of solutions.

The analogy could be read as advocating empire, with all its oppressive and dominating aspects, as a solution to the security problems of cyberspace. After all, when privateering was abolished in 1856, the Royal Navy was the unchecked predominant naval power. The British had a very strong position from which to influence norm development, as they could assert those norms by force. It is not clear whether it would be desirable or feasible for any single power in the twenty-first century to reform the international cyber domain as Britain did the maritime domain centuries ago. Unlike the maritime case, where order was imposed by a Western power, in the cyber era China and perhaps others with different historical, cultural, and political predilections will be influential players.

Although this analogy can be used as a productive tool to enhance current thinking about cybersecurity, the general caveat that historical experience cannot guarantee a parallel course of events today must not be neglected. Just as past policymakers made decisions in the face of uncertainty, knowledge of the past should not lead the scholar into the misguided belief that history will repeat itself. While considering the lessons from the analogy to privateering, policies for the twenty-first century must take into account the idiosyncrasies of today's political landscape. The twenty-first century does offer some new opportunities, which policymakers can and should embrace. Higher degrees of international integration broaden the space for a cooperative solution between different stakeholders. Thus, as the Royal Navy guaranteed a principle of free trade in the past, a large group of stakeholders today is engaged in trying to make cyberspace a more open, transparent, interoperable, and inclusive environment.

Notes

Extracts of this chapter have previously appeared in Florian Egloff, "Cybersecurity and the Age of Privateering: A Historical Analogy," University of Oxford Cyber Studies Working Papers, no. 1 (Oxford: University of Oxford, 2015), http://www.politics.ox.ac.uk/materials/centres/cyber-studies/Working_Paper_No.1_Egloff.pdf. The publication is funded by the European Social Fund and the Estonian government. Printed with the permission of the Oxford Cyber Studies Programme. The author thanks the book editors, the participants of the author workshop in December 2015, and the Oxford Cyber Studies Working Group for their constructive feedback and comments.

Epigraph: Mike Rogers, "The Importance of Partnership in Cyberspace," keynote speech presented at the CYCON: International Conference on Cyber Conflict, Tallinn, Estonia, May 27, 2015.

1. Jaak Aaviksoo, "Cyber Defense: The Unnoticed Third World War," speech presented at the Twenty-Fourth International Workshop of the Series on Global Security, Paris, June 2007.

2. For an example discussing such a policy, see Michael Lesk, "Privateers in Cyberspace: Aargh!," *IEEE Security & Privacy* 11, no. 3 (2013). For an example of recommending the private sector in the United States should be given letters of marque, analogizing the privateers as a solution to the pirate problem, see Michael Tanji, "Buccaneer.Com: Infosec Privateering as a Solution to Cyberspace Threats," *Journal of Cyber Conflict Studies* 1, no. 1 (2007).

3. See Stewart Baker, Rafal Rohozinski, and Nigel Inkster in US Congress, Senate, Committee on Homeland Security and Governmental Affairs, 111th Cong., 1st sess., "Cyber Security: Developing a National Strategy" (Washington, DC: US Government Printing Office, 2009) (S. Hrg. 111–724); US Congress, US-China Economic and Security Review Commission, 111th Cong., 1st sess., "2009 Report to Congress" (Washington, DC: US Government Printing Office, 2009); and Peter Apps, "Analysis: Agreement Seen Distant at London Cyber Conference," Reuters, October 26, 2011.

4. Some scholarship on the lessons of privateering for cybersecurity exists, but it is underdeveloped, focuses predominantly on warfare, or centers on privateering as a policy option rather than assessing its potential for the reexamination of the public-private distinction. See J. Laprise, "Cyber-Warfare Seen through a Mariner's Spyglass," *IEEE Technology and Society Magazine* 25, no. 3 (2006); Peter W. Singer and Noah Shachtman, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive" (Washington, DC: Brookings Institution Press, August 15, 2011), https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive/; Thomas Dullien, "Piracy, Privateering . . . and the Creation of a New Navy," keynote speech presented at the SOURCE Conference, Dublin, May 2013; B. Nathaniel Garrett, "Taming the Wild Wild Web: Twenty-First Century Prize Law and Privateers as a Solution to Combating Cyber-Attacks," *University of Cincinnati Law Review* 81, no. 2 (2013); and Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014).

5. Paul M. Kennedy, *The Rise and Fall of British Naval Mastery* (London: Penguin, 2004).

6. However, this entailed significant risks. As Paul Kennedy points out, the privateers were "prone to alter carefully formulated plans in favour of rash enterprises and all too easily tempted by the prospect of plunder and glory into forgetting the national strategy." As an example, he points to Sir Francis Drake's abandoning the chase of the Armada to attack the *Rosario*. Ibid., 38.

7. Francis R. Stark, *The Abolition of Privateering and the Declaration of Paris* (New York: Columbia University, 1897), 66.

8. Another famous example is Captain Kidd, who was hired to go after French vessels and pirates but was eventually hanged for piracy. While some debate whether Kidd actually committed piracy or acted as a privateer, his actions upset some powerful interests and resulted in his execution.

9. Matthew S. Anderson, *War and Society in Europe of the Old Regime, 1618–1789* (Stroud: Sutton, 1998), 57; Michael Arthur Lewis, *The History of the British Navy* (Harmondsworth: Penguin Books, 1957), 74–75; and Stark, *Abolition of Privateering*, 97.

10. Fernand Braudel, *The Mediterranean and the Mediterranean World in the Age of Philip II* (Berkeley: University of California Press, 1995), 2:865.

11. Anderson, *War and Society*, 97–98, 147.

12. Kennedy, *Rise and Fall*, 79.

13. The degree of choice should not be overstated, however, as the French did not have the financial means to invest in a navy comparable with the British. In addition, there was much enthusiasm for privateering. For more details, see Halvard Leira and Benjamin de Carvalho, "Privateers of the North Sea: At Worlds End—French Privateers in Norwegian Waters," in *Mercenaries, Pirates, Bandits and Empires: Private Violence in Historical Context*, ed. Alejandro Colás and Bryan Mabee (London: C. Hurst, 2010), 60–62.

14. Janice E. Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*, Princeton Studies in International History and Politics (Princeton: Princeton University Press, 1994), 26.

15. Jan Martin Lemnitzer, *Power, Law and the End of Privateering* (Basingstoke: Palgrave Macmillan, 2014), 48–51.

16. Stark, *Abolition of Privateering*, 155–56.

17. See, for example, Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," *Stanford Journal of International Law* 103 (2014); Lucas Kello, "Private-Sector Cyberweapons: Strategic and Other Consequences," June 15, 2016, http://dx.doi.org/10.2139/ssrn.2836196. See also Florian Egloff, "Cyber Privateering: A Risky Policy Choice for the United States," Lawfare, November 17, 2016, https://www.lawfareblog.com/cyber-privateering-risky-policy-choice-united-states.

18. Leslie R. Caldwell, "Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Georgetown Cybersecurity Law Institute," Department of Justice News, Washington, DC, May 20, 2015, https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-georgetown-cybersecurity. For information about how the United States tries to boost cooperation with industry, see Department of Homeland Security, "Enhanced Cybersecurity Services (ECS)," Department of Homeland Security, accessed March 19, 2016, https://www.dhs.gov/enhanced-cybersecurity-services. For the background history of the precursor to the ECS program, see Milton Mueller and Andreas Kuehn, "Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change," paper presented at the Twelfth Workshop on the Economics of Information Security, Washington, DC, 2013.

19. See, for example, the investigation into a strain of the GameOver Zeus banking Trojan, which was configured to also collect security-related documents in Georgia, Turkey, and Ukraine pertaining to Russia's involvement in the conflict: Michael Sandee, "Gameover Zeus: Backgrounds on the Badguys and the Backends" (Delft: Fox-IT InTELL, 2015). For recent evidence of collaboration between Russia's FSB and cyber criminals, see "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," Department of Justice News, Washington, DC, March 15, 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

20. Indications for this are criminal sites, which exclude content that "can adversely affect the Russian Federation, the Ukraine, and Belorussia." Example is from Max Goncharov, "Criminal Hideouts for Lease: Bulletproof Hosting Services" (Los Angeles: Trend Micro, 2015).

21. Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue* 43, no. 1 (2012): 16.

22. Nicholas Rodger, "Mobilizing Seapower in the Eighteenth Century," in *Essays in Naval History, from Medieval to Modern*, ed. N. A. M. Rodger (Farnham: Ashgate Publishing, 2009), 4.

23. Ibid., 5.

24. Lemnitzer, *Power, Law*, 39–40.

25. Barack Obama and Xi Jinping, "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," White House, September 15, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

26. James A. Lewis, "Moving Forward with the Obama-Xi Cybersecurity Agreement" (Washington, DC: Center for Strategic & International Studies, October 21, 2015), https://www.csis.org/analysis/moving-forward-obama-xi-cybersecurity-agreement.

27. See, for example, the diffusion of techniques employed in the Stuxnet attack.

28. One way the United States tried to overcome this was by issuing bounties—unsuccessfully in the case of the Zeus author Evgeniy Mikhailovich Bogachev (FBI, "Evgeniy Mikhailovich Bogachev," Most Wanted List, https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev) and successfully in the case of the Sasser worm author, Sven Jaschan.

29. Xin Zhang et al., "SCION: Scalability, Control, and Isolation on Next-Generation Networks," paper presented at the IEEE Symposium on Security and Privacy (SP), Oakland, California, May 22–25, 2011.

30. A good heuristic for adjudicating state responsibility regarding actors operating from a state's territory is the ten-point "Spectrum of State Responsibility" developed in Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Issue Brief (Washington, DC: Atlantic Council, 2011).

31. Adam Segal, "The Top Five Cyber Policy Developments of 2015: United States–China Cyber Agreement," Net Politics (Washington, DC: Council on Foreign Relations, January 4, 2016), http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/.

32. Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013).

33. This ties in with the signaling function privateering took in the mid-seventeenth century as argued by Gijs Rommelse in "Privateering as a Language of International Politics: English and French Privateering against the Dutch Republic, 1655–1665," *Journal for Maritime Research* 17, no. 2 (2015).

34. Not much is known about the actual US response in the Sands Casino case. However, in the attacks against Sony Pictures Entertainment, the United States publicly attributed the attacks to North Korea and imposed sanctions.

35. Julia Angwin et al., "AT&T Helped U.S. Spy on Internet on a Vast Scale," *New York Times*, August 15, 2015.

36. Mark Mazzetti, "F.B.I. Informant Is Tied to Cyberattacks Abroad," *New York Times*, April 23, 2014.

37. Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010).