Cyber Studies PROGRAMME

UNIVERSITY OF OXFORD

www.politics.ox.ac.uk/centre/cyber-studies-programme.html

Working Paper Series - No.1 March 2015

Cybersecurity and the Age of Privateering: A Historical Analogy

Florian Egloff

florian.egloff@cybersecurity.ox.ac.uk

Clarendon Scholar
DPhil Candidate in Cyber Security

Centre for Doctoral Training in Cyber Security and Department of Politics and International Relations, University of Oxford

Image Source: Samuel Scott, in David Cordingly, *Pirates, Terror on the High Seas: From the Caribbean to the South China Sea.* CC via Wikimedia Commons

Abstract

Policy literature on the insecurity of cyberspace frequently invokes comparisons to Cold War security strategy, thereby neglecting the fundamental differences between contemporary and Cold War security environments. This article develops an alternative viewpoint, exploring the analogy between cyberspace and another largely ungoverned space: the sea in the age of privateering. This comparison enables us to incorporate into cybersecurity thinking the complex interactions between state and non-state actors, including entities such as navies, mercantile companies, pirates, and privateers. The paper provides a short historical overview of privateering and cybersecurity and compares the two by identifying state actors, semi-state actors, and criminal actors in each historical context. The paper identifies the limitations of Cold War analogies and presents the analogy of privateering as a superior conceptual benchmark for future policy guidance on cybersecurity. The paper makes three main arguments. First, cyber actors are comparable to the actors of maritime warfare in the sixteenth and seventeenth centuries. Second, the militarisation of cyberspace resembles the situation in the sixteenth century, when states transitioned from a reliance on privateers to dependence on professional navies. Third, as with privateering, the use of non-state actors by states in cyberspace has produced unintended harmful consequences; the emergence of a regime against privateering provides potentially fruitful lessons for international cooperation and the management of these consequences.

European Union
European Social Fund

Investing in your future

This publication is funded by the European Social Fund and the Estonian Government

Introduction: Analogies in Cybersecurity Thinking

Cybersecurity is a classic "problem without passports."[1] Threats propagating through the transnational, globally interconnected cyberspace are difficult to manage with conventional state instruments. While "states are still struggling to understand and define their interests"[2] in the cyber domain, the academy grapples with interpreting and modelling this actor-rich and seemingly chaotic security environment.

The use of historical analogies can hinder or help this analytical task, with potentially profound implications for policy. For policymakers, the application of a misleading analogy in the analysis of security challenges can have disastrous consequences. For example, Yuen Foong Khong demonstrated how U.S. leaders' reliance on the analogy to the Korean War in the 1950s significantly shaped U.S. strategy in the Vietnam War—with significant consequences for human suffering.[3] Cognitive psychological research explains how practitioners use analogies to analyse situations that share a relational structure with a previously encountered problem.[4] The analogy in question often yields a specific set of policies associated with the resolution of the analogous problems. As David Bobrow puts it, "The choice of a metaphor carries with it practical implications about contents, causes, expectations, norms, and strategic choices."[5] In addition, in an analysis of the deliberations for a WMD-free zone in the Middle East, Gregoire Mallard highlights the constitutive purpose of analogies in the policymaking process.[6] Introducing the term "forward analogies," he shows how references to historical cases were used to constitute not only the Middle East as a region but also to shape a "common map of the future" with significant implications for regional policy.[7]

The choice of analogies, in short, shapes the way scholars and practitioners perceive problems of national and international security, sometimes with severe and negative policy implications. Therefore, it is vital to assess an analogy's potential implications for practice before applying it in the policymaking process.

A similar analogy-to-policy mechanism is at play in framing problems of cybersecurity. For instance, in framing the challenges of cybersecurity, Joseph Nye invokes the analogy of nuclear strategy, which involved a set of problems arising within the historical context of the Cold War.[8] To be sure, Nye's study is limited to the broad process of strategic adaptation to the nuclear revolution; it examines "meta-lessons" without drawing direct parallels between nuclear and cyber technologies. Nevertheless, other analysts and policymakers have been quick to apply specific Cold War analogies and strategies, such as classical deterrence, to the cyber realm.[9] The application of Cold War strategic concepts to cybersecurity analysis raises potentially grave problems. It introduces state-centric assumptions that govern much of existing international security studies theory but which hinder the interpretation of new forms of state and non-traditional agency that characterize cyber phenomena. Moreover, as David Betz and Tim Stevens explain, the current cybersecurity discourse invokes a "winner-takes-it-all modality that is neither desirable nor necessary in the current strategic reality."[10]

The analysis of cyber insecurity requires more appropriate historical analogies. Instead of focusing on state-centric analogies inherited from Cold War

[1] Kofi A. Annan, "Problems without Passports," *Foreign Policy*, No. 132 (September–October 2002), pp. 30–31.

[2] Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," in *Paper Series* (London: Global Commission on Internet Governance (CIGI) and Chatham House, 2014), p. 12.

[3] Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, N.J.: Princeton University Press, 1992).

[4] Dedre Gentner and Linsey A. Smith, "Analogical Learning and Reasoning," in Daniel Reisberg, ed., *The Oxford Handbook of Cognitive Psychology* (Oxford: Oxford University Press, 2013).

[5] Davis B. Bobrow, "Complex Insecurity: Implications of a Sobering Metaphor: 1996 Presidential Address," *International Studies Quarterly*, Vol. 40, No. 4 (1996), p. 436.

[6] Gregoire Mallard, "From Europe's Past to the Middle East's Future: The Constitutive Purpose of Forward Analogies," paper presented at the American Sociological Association Annual Meeting, New York, August 2013.

[7] Ibid., p. 8.

[8] Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol. 5, No. 4 (Winter 2011); ibid., "The Regime Complex for Managing Global Cyber Activities."

[9] Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat," Washington, D.C.: U.S. Department of Defense, 2013; Noa Shachtman and P. W. Singer, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive," Brookings Institution, Washington, D.C., 15 August 2011. http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman.

[10] David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue*, Vol. 44, No. 2 (April 2013), p. 147.

thinking, this article explores challenges arising from the murkiness of state–non-state distinctions in the age of privateering. The paper develops this historical analogy to capture problems of state action in a historically largely ungoverned space—the sea—in which quasi-state and non-state actors exerted significant influence on state interests and relations. The study examines actors with various degrees of state involvement in the ungoverned sea of previous centuries—navies, mercantile companies, pirates, and privateers—to draw lessons and insights for the analysis of contemporary problems of cyber insecurity.[11] It explores sets of relationships between rulers and "private" parties and assesses the development of state and non-state interaction. In doing so, the paper considers "the negative [and positive] influences that nonstate players may be able to exert on states and their relations with other states" in a way that re-examines traditional public-private distinctions.[12] As Krause and Milliken observed regarding armed "non-state" groups: "Many so-called 'non-state' armed groups are also deeply entangled with state power and state agents in complex ways. Thus, the label 'non-state' represents a barrier to understanding their multiple roles and functions."[13] The paper transcends this barrier by introducing more nuanced conceptual understandings between state and non-state actors.

The paper is organized into four sections. First, it outlines the history of both privateering and cybersecurity. Second, it compares the two themes by identifying similarities and dissimilarities in the roles of state actors, semi-state actors, and criminal actors, drawing on a variety of empirical events. Third, it explores the limitations of the privateering analogy as a conceptual benchmark. Last, the discussion extrapolates best practices for utilizing this analogy in the cybersecurity decisionmaking process.

A Brief History of Loosely Governed Spaces: The Sea and Cyberspace

This section provides a historical overview of two loosely governed spaces: the sea and cyberspace. Specifically, it examines the concurrent development of navies, mercantile companies, pirates, and privateers. It then discusses the much later emergence of cyberspace, with an emphasis on problems of cybersecurity. The analysis below will provide the historical context for a comparative conceptual framework of the sea and cyberspace.

From the Age of Privateering to Its Abolition: History of the Ungoverned Sea

The term "privateer" denotes a privately owned vessel that operates against an enemy with the licence or commission of the government in times of war.[14] In maritime history, "privateer" can also refer to the person who is engaged in privateering. The privateer differs from the pirate because the actions of the privateer are committed under the authority of a state. The use of privateers was part of established state practice between the thirteenth and nineteenth centuries. The practice ended with an international regime abolishing privateering in 1856.

The earliest references to privateering in England date back to the thirteenth century, when King Henry III ordered the men of the coastal towns (known as Cinque Ports) to "commit every possible injury to the French at

[11] Shachtman and Singer point out that the Cold War concepts used in cybersecurity are misleading; privateering, they argue, may offer a superior perspective. Existing scholarship on the lessons of privateering for cybersecurity faces shortcomings, however. It is underdeveloped, focuses too much on warfare, or centres on privateering as a policy option rather than assessing its potential for the re-examination of the public-private distinction. See P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York, N.Y.: Oxford University Press, 2014); Shachtman and Singer, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive"; Robert Axelrod, "A Repertory of Cyber Analogies," in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, Calif.: Naval Postgraduate School, 2014), http://hdl.handle.net/10945/40037; J. Laprise, "Cyber-Warfare Seen through a Mariner's Spyglass," *Technology and Society Magazine, IEEE*, Vol. 25, No. 3 (Fall 2006); M. Lesk, "Privateers in Cyberspace: Aargh!" *Security & Privacy, IEEE*, Vol. 11, No. 3 (May-June 2013).

[12] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol. 38, No. 2 (Fall 2013), p. 38; Michael C. Williams, "The Public, the Private and the Evolution of Security Studies," *Security Dialogue*, Vol. 41, No. 6 (December 2010).

[13] Keith Krause and Jennifer Milliken, "Introduction: The Challenge of Non-State Armed Groups," *Contemporary Security Policy*, Vol. 30, No. 2 (August 2009), p. 202.

[14] "Privateer," I. Dear and P. Kemp, eds., Vol. 2014, *The Oxford Companion to Ships and the Sea* (Oxford: Oxford University Press, 2006), http://www.oxfordreference.com/view/10.1093/acref/9780199205684.001.0001/acref-9780199205684-e-1884.

sea" in 1242.[15] The following year, Henry III offered the first privateering licences to "grieve" the Crown's enemies at sea and share half of the profits with His Majesty.[16]

Another practice was reprisal. During peacetime, *letters of marque* were issued to merchants who sought redress against a harm they suffered from foreigners on the high seas. A British merchant harmed by a French ship, for example, could obtain a *letter of marque* allowing him to attack any French ship until he found something of equal value to his loss.[17]

As merchant shipping increased, exploitation by state actors rose as well. When states were at war, privateers were used to disrupt shipping and gain income. Often sponsored by private capital, privateering was a lucrative undertaking. The Elizabethan Sea Dogs engaged the Spanish in the New World, raising large sums of money for both themselves and the Crown.[18] Problems arose when, after being knighted for his services to the court, the famous privateer Sir Walter Raleigh did not stop looting, even after the peace treaty between James I and His Most Catholic Majesty.[19] James I finally had Raleigh executed. This episode is a case in point for one of the problems that eventually led to the abolition of privateering, i.e. the difficulty of controlling privateers.

The longer wars lasted, the more privateering was professionalised and institutionalised. At the end of wars, privateers were either integrated into the navy or became active as pirates.[20] The line between privateering and pirating was often blurred, however. As Fernand Braudel noted, pirates could serve as a "substitute for declared war."[21]

During the late seventeenth century, French privateers (*corsairs* and *filibustiers*) became more active. While the English privateers were used as a tool of influence alongside the growing navy, the *corsairs* were used as a primary tool of naval warfare.[22] For France, they provided an ideal weapon against the English, who, comparatively, relied much more on foreign trade.[23] The French used the *guerre de course* against the English in the War of the Spanish Succession.[24]

Besides being attacked by French *corsairs*, piracy proved to be problematic for England. English pirates, for example, did not refrain from attacking ships of local rulers in the colonies.[25] In India, the Mogul asked the English East India Company for protection from English-speaking pirates. After attacks against the mercantile company, it raised its own demands in England for protection by the Royal Navy. This only caused pirates to sail on to the Bahamas, however. By the eighteenth and early nineteenth centuries the British state responded with a comprehensive set of policies, offering incentives to pirates, implementing legal reform in the colonies to prevent markets for pirated goods, and sending the Royal Navy to destroy pirates' home bases.[26] This differentiation of policies between piracy and privateering merits analysis in light of the increasing power of navies, the integration of privateering into naval war strategy, and the decreasing usefulness of pirates owing to their negative impact on

[15] Francis R. Stark, *The Abolition of Privateering and the Declaration of Paris* (New York: Columbia University, 1897), p. 52.

[16] Henry III, "Henry III, Patent 27, M.16," http://sdrc.lib.uiowa.edu/patentrolls/h3v3/body/Henry3vol3page0362.pdf.

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

[18] Kenneth R. Andrews, *Elizabethan Privateering; English Privateering During the Spanish War, 1585–1603* (Cambridge: Cambridge University Press, 1964).

[19] Stark, *The Abolition of Privateering and the Declaration of Paris*, p. 66.

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

[21] Fernand Braudel, *The Mediterranean and the Mediterranean World in the Age of Philip II*, 2 vols. (Berkeley, Calif.: University of California Press, 1995), p. 865.

[22] Anderson, *War and Society in Europe of the Old Regime, 1618–1789*, pp. 97–98, 147.

[23] Paul M. Kennedy, *The Rise and Fall of British Naval Mastery* (London: Penguin, 2004), p. 79. The degree of choice should not be overstated, however, as the French did not have the financial means to invest in a comparable navy. 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 Alejandro Colás and Bryan Mabee, eds., *Mercenaries, Pirates, Bandits and Empires: Private Violence in Historical Context* (London: C. Hurst and Co., 2010), pp. 60–62.

[24] Kennedy, *The Rise and Fall of British Naval Mastery*, pp. 84–85.

[25] Peter Earle, *The Pirate Wars* (London: Methuen, 2003); the following case is explained in Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*, p. 109.

[26] Kennedy, *The Rise and Fall of British Naval Mastery*, pp. 164–165, 71; Earle, *The Pirate Wars.*

trade.[27] Increasingly, "merchants laid down their weapons and accepted that the state would protect their business in exchange for regulating and taxing it. There would have been no 'suppression of piracy' without this change in relationship between merchant and the state."[28]

After a period of decline in English privateering in the early seventeenth century, it resurged in the eighteenth.[29] To incentivise privateers in the War of the Spanish Succession, Queen Anne passed an English Prize Act that allowed privateers to retain all profits and introduced a bounty for prisoners taken.[30] By 1744, George II pardoned prisoners who volunteered to serve as privateers.[31] In 1758, Britain introduced a policy that encouraged privateers to attack neutral ships trading French colonial goods (i.e., the Dutch).[32] This spurred so much interest in privateering that the maritime insurer Lloyd's filed a complaint with the English government.[33] The government responded by announcing a minimum vessel size, which raised the entry costs for active privateers.

British policy toward neutral ships was not well received by the Russians. In 1780, Catherine II reacted by enacting the Free Ships Free Goods policy, which allowed neutrals to trade with nations at war (excluding contraband), to denounce ineffective blockades, and to defend this policy by force if necessary.[34] Other neutrals agreed with Russia. The renewal of this agreement in 1800 led to a convention between England and Russia in 1801 in which Russia gave up the Free Ships Free Goods policy in return for immunity from search by privateers.[35]

By the end of the eighteenth century, it was mostly the United States (in the War for U.S. Independence) and France (in the French Revolutionary War and later in the Napoleonic Wars) that employed privateers against Britain. Thus, 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."[36]

For the duration of the Crimean War, France and Britain agreed to extend the Free Ships Free Goods policy to the neutral powers.[37] In 1854, the United States launched an offensive to persuade the European countries to settle this principle contractually. Britain, however, knowing that it would be difficult to revert to its former policy after the war, aimed for something in return: the abolition of privateering. The interest in this was both ideological and strategic.[38] Ideologically, some members of the liberal elite were appalled by this crude method of warfare. Strategically, Britain's naval commerce had become very large. In addition, the large merchant navy of the United States posed a risk even to the largest navy in the world. Considering the possible instability of the Anglo-French alliance, a U.S.-French alliance would have directly threatened Britain's survival. In contrast, the United States relied on being able to transform its merchant cruisers into weapons of warfare and lobbied for its own proposal in European capitals.[39]

Meeting for a settlement of the Crimean War in Paris in 1856, the Congress of Paris decided to resolve some other questions of concern. France seized the opportunity to press for establishment of the Free Ships Free Goods policy as international law, proposing to concede to the British demand to abolish privateering.[40] Both France and Britain had not engaged in privateering since the Napoleonic Wars, and besides Britain, France

[27] Bryan Mabee, "Pirates, Privateers and the Political Economy of Private Violence," *Global Change, Peace & Security*, Vol. 21, No. 2 (June 2009).

[28] Anne Pérotin-Dumon, "The Pirate and the Emperor: Power and the Law on the Seas, 1450–1850," in C. R. Pennell, ed., *Bandits at Sea: A Pirates Reader* (New York: New York University Press, 2001), p. 41.

[29] Maximilian Leeder, *Die Englische Kaperei Und Die Thätigkeit Der Admiralitäts-Gerichte* (Berlin: Berliner Buchdruckerei-Actien-Gesellschaft, 1882).

[30] Great Britain and John Raithby, *The Statutes Relating to the Admiralty, Navy, Shipping, and Navigation of the United Kingdom from 9 Hen. Iii to 3 Geo. Iv Inclusive: With Notes, Referring in Each Case to the Subsequent Statutes, and to the Decisions in the Courts of Admiralty, Common Law, and Equity, in England, and to the Scotch Law* (London: s.n., 1823), pp. 104–106.

[31] Leeder, *Die Englische Kaperei Und Die Thätigkeit Der Admiralitäts-Gerichte*, p. 10.

[32] Stark, *The Abolition of Privateering and the Declaration of Paris*, p. 74.

[33] Leeder, *Die Englische Kaperei Und Die Thätigkeit Der Admiralitäts-Gerichte*, p. 45.

[34] Paul Fauchille, *La Diplomatie Française Et La Ligue Des Neutres De 1780, 1776–1783*, Bibl. Internat et Diplomatique (Par.1893).

[35] Stark, *The Abolition of Privateering and the Declaration of Paris*, p. 82.

[36] Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*, p. 26.

[37] Great Britain, "British Declaration with Reference to Neutrals and Letters of Marque," in *British Foreign and State Papers* (London: HMSO, 1865).

[38] Jan Martin Lemnitzer, *Power, Law and the End of Privateering* (Basingstoke: Palgrave Macmillan, 2014), pp. 39–40.

[39] Ibid., pp. 48–51.

[40] Ibid., p. 70.

held the largest navy. As this policy option was evaluated in the context of a new U.S. proposal to protect private property at sea, Britain felt compelled to act. Prussia, having evaluated its policy options in an earlier U.S. proposal, was now ready to support the British proposal.

The declaration passed and it was agreed that it would be widely circulated so that as many powers as possible could comply with it. Most powers happily acceded because Britain, the predominant sea power, was finally ready to support a practice protecting neutral commerce. This agreement, however, left the United States out. Since there was a consensus among the parties of the declaration that no port could receive privateers, privateering was made practically impossible. A privateer would have to return to his home state in order to sell his prizes. During the U.S. Civil War, the northern states enquired about 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 justification to sign away rights for the other party.[41]

This discussion about the abolition of privateering, suppression of piracy, and the extinction of mercantile companies would not be complete without highlighting the concurrent development of the nation-state and the institution of territorial sovereignty. Sovereignty on the high seas is linked to a state's capacity to control (i.e., the development of navies).[42] The absence of a sovereign on the high seas is one of the preconditions for the presence of the types of actors that the following section will discuss. The state-making and war-making processes, which Charles Tilly aptly compared to organised crime, form the backstory to this discussion.[43] As we shall see, the growth of cyberspace and the absence of state control produced opportunities for private actors to exploit it.

The Origins and Development of Cyberspace

Compared to the history of privateering, the history of cyberspace and its security challenges is a short one. Cyberspace, and especially the Internet, expanded rapidly as a result of commercialisation and advances in personal computing. Early design choices did not prioritise confidentiality concerns; rather, they focused on the ability to connect. The rationale for this choice was to increase the network's survivability.

Different actors have shaped the trajectory of the development and the norms associated with cyberspace. Early proponents, mainly from the United States, focused on an open, unregulated network. With the expansion of the network, states started to realise the vulnerabilities that became apparent when analysing the relatively unchecked interconnectivity with the rest of the world. Alongside the increase of a technically literate user base, attacks arose. At first, Computer Emergency Response Teams (CERTs) were formed (e.g., Carnegie Mellon University's CERT in 1998) to respond to the technical challenges of the growing number of threats. CERTs started cooperating internationally by sharing data regarding vulnerabilities and attacks.[44] While performing the same basic defensive functions, however, the diversity of national political systems and practices created challenges to cooperation.[45]

States have reacted to these security challenges in different ways. The U.S. military has developed its policy of information warfare from the early 1990s into a fully operational cyber command structure (CYBERCOM). This was done not only to create information dominance in warfare, but also because of the realisation that the interconnectivity of critical infrastructures posed new risks to national security. Similarly, most advanced industrialised nations have tasked their defence and intelligence agencies with a large role in implementing their cybersecurity strategies.[46] Growing out of the capabilities of traditional signals intelligence, many states have teams working on ways to exploit cyberspace for their own interests. The use of private actors for this purpose is of particular importance in the analogy described below.

[41] Stark, *The Abolition of Privateering and the Declaration of Paris*, pp. 155–156.

[42] David J. Bederman, "The Sea," in Bardo Fassbender et al., eds., *The Oxford Handbook of the History of International Law*, *Oxford Handbooks* (Oxford: Oxford University Press, 2012).

[43] Charles Tilly, "War Making and State Making as Organized Crime," in Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol, eds., *Bringing the State Back In* (Cambridge: Cambridge University Press, 1985).

[44] ENISA, "Cert Cooperation and Its Further Facilitation by Relevant Stakeholders," in *Deliverable WP2006/5.1 (CERT-D3)* (Heraklion: ENISA, 2006).

[45] Nazli Choucri, Stuart Madnick, and Jeremy Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," *Information Technology for Development*, Vol. 20, No. 2 (October 2013), p. 106.

[46] Organisation for Economic Co-operation and Development (OECD), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy," in *OECD Digital Economy Papers* (Paris: OECD Publishing, 2012).

The Sea and Cyberspace: A Framework for Comparison

This section develops a comparative framework for the analogy between the loosely governed seas and cyberspace by exploring the relationships among state actors, semi-state actors, and criminal actors. Specifically, the framework elucidates the degree of closeness between non-state actors and governments (see Table 1).

Table 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
Semi-State Actors	Mercantile companies	Technology champions (e.g. Apple, Google, Huawei)
	Privateers	Patriotic hackers
		Some cyber criminal elements
Criminal Actors	Pirates	Cybercrime (incl. organised crime)

State Actors

In the state realm, the comparison between the two cases is closely linked to the development of naval warfare capacity over time. As described above, privateers were once the main actors in states' capacity for naval warfare. By the seventeenth century, however, states with ambitions for maritime influence needed professional navies. Spain, England, and the Netherlands invested in naval capabilities early on, while other powers (e.g., France) continued to rely on a combination of privateering and renting warships from other powers (e.g., the Netherlands). The growing state ambitions for public recruitment resulted in more regulated privateering. In order to prevent competition for personnel, for example, a quota of professional sailors for privateering ships was introduced. While privateering continued to be an effective auxiliary method to "grieve"[47] an enemy's commercial waterways, professional navies were able to perform more complicated and resource-intensive tasks, such as establishing blockades on enemies' ports.

In cyberspace, various efforts for public recruitment are underway. Since the 2000s, many states have invested in cyber defence, intelligence, and policing capabilities.[48] As with the development of navies, there are different ways in which cyber capacities have developed. Some states have invested in governmental capabilities, refraining from relying heavily on third-party support. There is, however, a range of cybersecurity contractor services that offer anything from intelligence and surveillance to offensive operational capabilities. The spectrum covers defence, intelligence, and policing tasks. States can use such services to jump-start their technical capabilities in the cyber realm. Expensive manpower developing "zero-day" exploits,[49] which enable offensive cyber capabilities, is outsourced to companies who act as middlemen in much the same way that privateers once did.[50]

Semi-State Actors

Mercantile companies performed semi-state functions. Primarily interested in unregulated profit-making, they operated with state consent, assuming sovereign-like functions abroad. The right to raise an army and to declare war illustrates this point clearly: "At the heart of these practices was the state-building process. To attain wealth and power promised by overseas expansion, states empowered nonstate actors to exercise violence,"[51] as the states' capabilities were insufficient or too constrained. The companies operated by their own international policies, made deals with other companies or states, or were at war with them, engaging in open warfare, piracy, and privateering, sometimes independently and against

[47] Henry III, "Henry III, Patent 27, M.16."

[48] See, e.g., Myriam Dunn Cavelty, "The Militarisation of Cyber Security as a Source of Global Tension," in Daniel Möckli, ed., *Strategic Trends 2012* (Zürich: Center for Security Studies, ETH Zurich, 2012).

[49] They are called zero-day exploits because they manipulate previously unknown vulnerabilities.

[50] Clay Wilson, "Cybersecurity and Cyber Weapons: Is Nonproliferation Possible?" in Maurizio Martellini, ed., *Cyber Security: Deterrence and IT Protection for Critical Infrastructures* (Cham: Springer, 2013), p. 20.

[51] Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*, p. 67.

the interests of their home states.[52]

For a long time, these companies ruled vast territories. It is important to highlight the political economy of mercantilism, in which the political and the economic were not functionally differentiated. John Anderson writes that "the term *mercantilist* reflects the symbiotic alliance between the state and the commercial interests in pursuit of power and wealth at the expense of other states."[53] The use of violence allowed mercantile companies to establish trade monopolies. There was no clear separation between the interests of the company and the interests of the state. In Britain, it was the growing political calculation to consolidate the sovereign functions in state rule that eventually rendered the company purely commercial.[54]

Arguably, there is no direct modern-day equivalent of the mercantile company. The closest modern counterparts are the technology champions and telecommunications providers of different countries, which hold large market and informational power in and between countries (for selected examples, see Table 2).

Table 2: Examples of Modern Companies Analogous to Mercantile Companies

Selected Countries	Contemporary Companies
China	Huawei, Lenovo, ZTE
France	Alcatel-Lucent, Orange
Germany	Deutsche Telecom
Japan	Sony
South Korea	Samsung
Spain	Telefónica
Taiwan	D-Link
United Kingdom	BT, Vodafone
United States	Apple, AT&T, Cisco, Google, Facebook, Juniper Networks, Level3, Microsoft, Verizon

The relationships between states and companies are usually kept secret. In the case of U.S. companies, however, the link was revealed by Edward Snowden's disclosures on National Security Agency (NSA) activities.[55] The most prominent example is a U.S. government program code-named PRISM, in which, by invoking FAA Section 702, the government compelled several telecommunications providers to cooperate with the government in collecting data on non-U.S. persons. Similar relationships exist elsewhere (e.g., France[56] and the United Kingdom[57]). The exact nature of voluntarily shared data between private corporations and state agencies is an important question for further research.[58]

States profit from the globalised, market-dominating nature of commercial enterprises in the information technology sector by gaining access to information. Another resemblance with mercantile companies occurs when companies are able to levy state resources for their own defence abroad. Google's actions in China in 2009 and 2010 are one example. When Google allegedly faced Chinese governmental intrusions against its network, U.S. officials became involved very quickly. Just as the English East India Company called on the Royal Navy, Google reached out to both the U.S. State Department and the NSA for help.[59]

A third resemblance between the multinational information technology companies and mercantile companies emerges from their interaction with different state actors. Multinational companies have a commercial incentive to offer their intelligence collection capabilities to more than just their "home" governments.[60] In the interest of selling their services to "foreign" governments, however, companies have to convince governmental buyers of the security of their products. From these dual objectives, incentives arise that are different from the "home" state's objectives. A multinational company will have a general

[52] Ibid., pp. 61–62.

[53] John L. Anderson, "Piracy and World History: An Economic Perspective on Maritime Predation," in C. R. Pennell, ed., *Bandits at Sea: A Pirates Reader* (New York: New York University Press, 2001), p. 91.

[54] Others went bankrupt, had their royal charters removed, or merged with other companies. See Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe.*

[55] See, e.g., http://leaksource.info/category/nsa-files/.

[56] Jacques Follorou, «Espionnage: Comment Orange Et Les Services Secrets Coopèrent,» *Le Monde,* 20 March 2014.

[57] James Ball, Luke Harding, and Juliette Garside, "BT and Vodafone among Telecoms Companies Passing Details to GCHQ," *Guardian,* 2 August 2013.

[58] With respect to Google and Microsoft, see Shoshanna Zuboff, "Dark Google," *Frankfurter Allgemeine Zeitung*, 30 April 2014.

[59] Joseph S. Nye, Jr., *The Future of Power*, 1st ed. (New York: PublicAffairs, 2011), pp. 128–130.

[60] Frederik Obermaier et al., "Der Lohn Der Lauscher," *Süddeutsche Zeitung*, 21 November 2014.

policy on how it interacts with governments. In addition, the legal domicile of the company exposes it directly to the legal policies of the respective country. Owing to the global nature of the company, however, operations may be influenced by any state that has sufficient leverage over the company's undertakings. The interaction between the two is another important area for further research.

Privateers were once the most prominent semi-state actors; in fact, privateering was sometimes referred to as "patriotic piracy."[61] As explained above, privateering was a legitimate method of warfare. Privateers were private individuals (e.g., merchants) who used private equipment, at their own risk, to fulfil the mercantilist state-sponsored goal of attacking enemy commerce. In return, they profited from the booty. The state benefited from this undertaking in two ways. First, privateering was a means of disrupting enemy commerce (and thus for the state's own merchants to profit). Second, it provided a good source of income for the state. In cyberspace there has been a similar development. Although not restricted to countries at war, attacks against foreign companies are regularly attributed to "patriotic hackers." Working in the political and economic interest of a country, patriotic hackers have been active in many highly visible cases—ranging from the attacks by Russian hackers on Estonia in 2007 and on Georgia in 2008, to the attacks by Chinese and U.S. hackers in 1999 and 2001, to those by Muslim and Israeli hackers (ongoing). Besides these highly visible, clearly politically motivated attacks, there are also private intelligence collection efforts.

The alignment of interests between hackers and governments is closer economically than politically. There are hackers who form part of governmental efforts to raise cyber capacity. Instead of recruiting personnel for governmental positions, governments rely on the support of private personnel in several countries, including China, Japan, Estonia, and Iran. Recent reports, however, have indicated a shift of groups formerly known to be engaged in political attacks toward more economic targets, focusing on economic espionage and intellectual property theft. The cultivation and utilisation of private talent for economic wealth transfer is the modern version of privateering.

In the case of Russia, 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 comes in several layers.[62] One example is discretionary enforcement based on the targets selected. Another is the way in which cyber criminals have become active in Russian political interests.[63] Empirical evidence, however, is usually incomplete and open to interpretation. For example, Deibert, Rohozinski, and Crete-Nishihata found no direct evidence linking the Russian government to the electronic attacks in Georgia in 2008,[64] but they have not ruled out the possibility that Russia quietly encouraged "malicious actions by seeding instructions on Russian hacker and nationalist forums and through other channels."[65] Tacit support can usually be inferred by the absence of cooperation between governments in the presence of a mutual legal assistance treaty (MLAT). For example, in the case of Estonia being attacked by patriotic hackers from Russian IP addresses,[66] the MLAT should have led to responsible state behaviour as expected by international law by, e.g., making forensic evidence available.[67]

Chinese hackers are also engaged in attacks against commerce. Their alignment with governmental interests is well-documented.[68] Hackers have been used regularly by government officials as an excuse to deny governmental

[61] James G. Lydon, *Pirates, Privateers, and Profits* (Upper Saddle River, N.J.: Gregg Press, 1970).

[62] See, e.g., Note of Warning in Kenneth Geers et al., "World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks," (Milpitas, Calif.: FireEye Inc., 2013), p. 4.

[63] Misha Glenny, *Darkmarket: Cyberthieves, Cybercops, and You*, 1st U.S. ed. (New York: Alfred A. Knopf, 2011); Christian Czosseck, "State Actors and Their Proxies in Cyberspace," in Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (Tallinn: NATO CCD COE, 2013).

[64] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue*, Vol. 43, No. 1 (February 2012).

[65] Ibid., p. 16.

[66] Depending on whether active Russian support or tacit support is assumed, the attacks on Estonia fit the privateering (active) or pirate (tacit) case better.

[67] In 2013, the UN Group of Governmental experts affirmed the applicability of international law in cyberspace. See Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report," (New York: United Nations, 2013).

[68] U.S.-China Economic and Security Review Commission, "Annual Report to Congress" (Washington, D.C.: U.S. Government Printing Office, 2009), pp. 167–184; Scott J. Henderson, *The Dark Visitor: Inside the World of Chinese Hackers* (Raleigh, N.C.: lulu.com, 2007).

involvement in attacks emanating from the Chinese network space.

Thus, companies, hacker groups, and some cyber criminals engage at their own risk to fulfil state-sponsored goals against the interests of other commercial and non-commercial entities. The profit motives for both the state and the hacker groups are sometimes different from those of the privateers. In cyberspace, states may profit indirectly by gaining the capabilities of criminal hacker groups in return for tolerating their criminal activity, whereas in the case of privateering, states directly encouraged the profit-generating criminal activity.

Criminal Actors

Privateers proved difficult to control. They would often resort to piracy, attacking not only enemies but also neutral ships. This led to acts of reprisal against commerce, which increased the need for protection and raised insurance rates for merchants. Some pirates, rejecting their home states' systems, formed pirate communities centred on their profession. Some states chose to pay off the pirates so that the pirates would attack the state's enemies instead. Pirates sold their goods in pirate markets, which provided cheap colonial goods to merchants. In this way, states that could avoid injury profited from the pirates. Pirates became a problem once their actions were attributed to their country of origin. In the case of England, this meant that other states would associate English pirates' actions with the English East India Company, which in turn requested protection by the Royal Navy.

While it was widely accepted that states would have to take control of piracy within their territorial waters, there emerged several approaches to dealing with piracy on the high seas. The Spanish approach was to extend territoriality and claim large parts of the high seas. This failed due to Spain's inability to enforce its claims. Another approach was to blame piracy on the home state of the pirate (e.g., England if the pirate spoke English). A third way was to treat pirates as stateless. This solution was finally accepted; it was viable only once states could define piracy, however. In order to do so, a clear distinction between state-supported and unsupported activity was required. This, in turn, was only possible with the delegitimisation of privateering.[69] As professional navies developed and privateering became more regulated, the difference between piracy and privateering became more formalised.[70]

In cyberspace, the criminal market has matured to the point that most parts of the criminal business process can be bought as services.[71] Products and services are marketed with testing possibilities, bulk order discounts, and customer service and support. Information technology has made this type of marketing easier because vendors can hide behind anonymous profiles. In addition, there is a market for customised cybercrimes. Targeted hacking-as-a-service, for example, can be bought in advance (e.g., one can order information about the accounts or intellectual property of a particular organisation). Intellectual property can sometimes be bought as a side product of an attack, but it is much more difficult to sell without a previously arranged buyer.[72] The collusion of some criminal organisations with the state as described above makes this activity potentially more feasible. Also, the market for information on zero-day vulnerabilities is highly professionalised.[73] This is due partly to the low legal risk of selling such information on the grey market and partly to the financially powerful buyers (public and private intelligence agencies, militaries, etc.).

There are some regional specialisations in cyber criminal underground markets. Latin America is most actively known for banking malware.[74] The Russian-speaking

[69] Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*, pp. 117–118.

[70] Mabee, "Pirates, Privateers and the Political Economy of Private Violence."

[71] Raj Samani and Francois Paget, «Cybercrime Exposed: Cybercrime-as-a-Service» (Santa Clara, Calif.: McAfee, 2003), http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf.

[72] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime. Tools and Stolen Data," Santa Monica, Calif.: RAND, 2014, p. 4.

[73] See, e.g., Symantec, "How the Elderwood Platform Is Fueling 2014's Zero-Day Attacks," Mountain View, Calif., 14 May 2014, http://www.symantec.com/connect/blogs/how-elderwood-platform-fueling-2014-s-zero-day-attacks.

[74] Gustavo Diniz et al., "A Fine Balance: Mapping Cyber (in) Security in Latin America," Igarape Institute and The SecDev Foundation, Rio de Janeiro, June 2012); Organisation of American States and Trend Micro, "Latin American and Caribbean Cybersecurity Trends and Government Responses," Trend Micro, Cupertino, Calif., 3 June 2014 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf; Trend Micro, "Brazil: Cybersecurity Challenges Faced by a Fast-Growing Market Economy" Trend Micro, Cupertino, Calif., 26 August 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-brazil.pdf.

underground (Russians, Romanians, Lithuanians, Ukrainians)[75] focuses mainly on attacking financial institutions, but also has a large malware community.[76] The Chinese have a large hacker community focusing on SIM card scams, online gaming fraud, and intellectual property theft.[77] Besides the well-known upfront payment scams, there are some reports from Western Africa about fraudsters leveraging the information left in hardware waste exported to the region.[78]

As in the case of privateering, the cyber criminal economy brings substantial revenue to a country. Profiting both in terms of financial and informational inflow, some states may have an interest in harbouring cyber criminals. If states are able to steer the target selection of cyber criminals, some state leaderships may come to the conclusion that (at least for a time) cybercrime is an acceptable evil. Unlike in the age of privateering, modern states do not have to fear reprisals against their companies, but corporations will have a strong interest in protecting their informational assets from theft. It is unclear how modern corporations will act to protect their assets. On ships, merchants would have armed their vessels. Whether the same will be true for cyber actors remains to be seen.[79]

Drawing from the privateering analogy, a clear distinction between state-supported and unsupported cyberattacks is required in order to form an effective international regime against cybercrime. The Budapest Convention on Cyber Crime and its fifty signatories provide a good starting point for such a regime. Police cooperation with the rest of the world remains limited, however. In its 2013 report on cybercrime, the United Nations Office on Drugs and Crime stated:

> Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments, a lack of response time obligation, a lack of agreement on permissible direct access to extraterritorial data, multiple informal law enforcement networks, and variance in cooperation safeguards, represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters.[80]

As long as the opportunity to use cyber criminals against other states and corporations remains a policy option, an international regime against cybercrime cannot be expected to function effectively. Like privateering, however, the adverse effects of the use of private actors can be seen in the cyber realm. Increasingly, China faces the costs of domestic cybercrime. Likewise, one can expect the Russian interest in cracking down on cybercrime to rise if domestic companies are attacked more frequently.

The Ungoverned Sea and Cyberspace: Limitations of the Analogy

There are differences between privateering and cybercrime that could weaken the analogy proposed in this article. For example, Nye argues that "the costs of developing multiple-carrier task forces and submarine fleets create enormous barriers to entry and make it still possible to speak of American naval dominance.... The barriers to entry in the cyber domain, however, are so low that nonstate actors and small states can play significant roles at low levels of cost."[81] On the ungoverned seas, however, unlike in the Cold War arms race, the cost of entry was not always prohibitive for non-state actors in maritime crime and warfare. Privateering was once a profession that small fishing boats as well as large vessels

[75] Ablon, Libicki, and Golay, "Markets for Cybercrime. Tools and Stolen Data," p. 6.

[76] Max Goncharov, "Russian Underground 101," Trend Micro, Cupertino, Calif., 20 October 2012, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.

[77] Ablon, Libicki, and Golay, "Markets for Cybercrime. Tools and Stolen Data," p. 7; Lion Gu, "The Mobile Cybercriminal Underground Market in China," Trend Micro, Cupertino, Calif., 3 March 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-mobile-cybercriminal-underground-market-in-china.pdf; Jianwei Zhuge, Liang Gu, and Haixin Duan, "Investigating China's Online Underground Economy," Institute on Global Conflict and Cooperation. University of California, San Diego, http://igcc.ucsd.edu/assets/001/503677.pdf.

[78] Camino Kavanagh, "Getting Smart and Scaling Up: Responding to the Impact of Organized Crime on Governance in Developing Countries," New York: Center on International Cooperation, NYU, 2013; Peter Klein, "Ghana: Digital Dumping Ground," Frontline, 13 January 2010, http://www.pbs.org/frontlineworld/stories/ghana804/video/video_index.html; Jason Warner, "Understanding Cyber-Crime in Ghana: A View from Below," *International Journal of Cyber Criminology*, Vol. 5, No. 1 (January-July 2011).

[79] Good reasons against such a policy are explained in Lesk, "Privateers in Cyberspace: Aargh!"

[80] United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime—Draft," (New York: United Nations, 2013), p. xxvi.

[81] Nye, *The Future of Power*, p. 124.

could practice. It even had to be regulated in order to restrict smaller ships from entering. Thus, the dimensions of the cost of entry, depending on which historical period one uses for comparison, may be less extreme than portrayed by Nye.

It is true that a growing number of small state and non-state actors can exploit cyberspace. While privateering and pirating were limited to actors with access to the sea, cybercrime can be pursued by any actor connected to the Internet. States and non-state actors can be active in a part of the world that is geographically remote from where they commit their crimes. This does not imply that physical geography does not matter. Having physical access to a large Internet exchange point (IXP) still gives a state a vector of influence and power. The interconnectivity of the network, however, decreases the importance of geography relative to the dynamics of the sea.

Another difference that may set the analysis askew is the attribution problem. With privateering and pirates, the difficulty of attribution could arise from several elements. First, a seaman would wonder whether the crew could be attributed to the flag being flown. Second, one could question whether the flag flown matched the papers produced by the crew. Finally, it was not always clear that the papers produced were valid. In the absence of national or international registers, verification was a difficult undertaking.

In cyberspace, attribution is also difficult.[82] There are multiple challenges. First, one would need to ascertain the association between an attack and a specific hacker group. This can sometimes be established based on mistakes made, or by the techniques, tactics, and procedures (TTPs) used, or by inference from the specific targets selected. Similar to flying a flag of a different country on a ship, however, attacks are sometimes staged using the TTPs of a different group in order to hide the identity of the attackers. Second, one would need to find the association between this group and a given state actor. This is much harder to prove. When cyberattacks are attributed to a specific government, the attribution represents a political judgment. The alleged involvement of the Russian government in the attacks on Estonia, for example, remains unproven. Rather, it is the lack of mutual legal assistance provided by Russia that signals its tacit support of these cyberspace activities. The major difference between the two types of attribution problems is that on the sea, the human attackers have to expose themselves to physical risks. Thus, when an attack fails and a ship can overcome the privateer by force, the attacker faces retribution. With cybercrime, this is not the case. Even if an attack could be successfully traced to individuals, they may have the protection of their home state. In both the maritime and cyber contexts, states found ways of using the domain to project power with little attribution. Yet, actions in these spaces also created negative effects on those states.

Regarding the comparison of mercantile companies and cyber companies, again the analogy is not a perfect match. Although private global companies are powerful stakeholders in cyberspace, they are also less attached to their "home" countries than mercantile companies were. The global, interconnected capitalist economy is built upon the distinction between public and private interests. As demonstrated in this article, however, with cybersecurity this distinction is blurred. The global nature of the international market environment forces multinational companies not only to cater to the needs of the home government, but also to explore other options. The implications are twofold. On the one hand, the company has to convince international stakeholders of its independence from the home government, which can be seen in the reactions of companies to the Snowden disclosures. On the other hand, other governments also demand access to the informational power the global company holds. The Vodafone lawful enforcement disclosure report, for example, shows the extent to which governments worldwide have relied on direct access to the company's data.[83]

Finally, cyberspace is different from the sea because its topography is artificial—hence it is malleable by human practice. Both technological and social changes manifest themselves in cyberspace. Introducing new security-oriented technical protocols, hardware, and software is a theoretical possibility. Recent research in networking has proposed models for new types of Internet routing; many of these proposals use security properties as guiding

[82] Clement Guitton and Elaine Korzak, "The Sophistication Criterion for Attribution," *RUSI Journal*, Vol. 158, No. 4 (August 2013).

[83] Vodafone, "Law Enforcement Disclosure Report" (London: Vodafone Group Plc, 2013-2014), http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html.

principles for their designs.[84] If implemented, they could contribute to a more secure environment, offering users a more explicit way of making decisions about whom to trust.

Conclusion: Implications for Policy

Having compared actors from the sea and cyberspace, a number of conclusions can be drawn. 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 conceptualisation of actors in cyberspace captures both the expansion of transnational non-state actor activity and the devolution of responsibilities and authority to private actors as referred to by Deibert and Rohozinski.[85]

Second, the militarisation of cyberspace resembles 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, state actors' cyber capacities are in their infancy. Militarisation could have positive consequences for a cybercrime regime, as it could be accompanied by a decreasing interest in the use of non-state actors. Just as France opted for a prolonged period of *guerre de course*, however, the decreasing interest in the use of non-state actors is not guaranteed.

Third, the analysis of the regime against privateering has shown that it can be traced back 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 behaviour in order to control these unintended consequences while preserving the positive effects of cyberspace is an open question. For example, U.S. norm-building efforts against cyber espionage for commercial advantage have been hampered by the disclosures of U.S. spying by the NSA.[86] Chinese Vice-Foreign Minister Li Baodong's remarks leave no room for interpretation:

> An individual country has exercised double standards on the cyber issue, drawn lines out of its selfish interests and concocted 'regulations' only applicable to other countries. We express strong concerns over this. Instead of reflecting on its behaviors that undermine the sovereignty of other countries and privacy of citizens, it has painted itself as a victim and made groundless accusations against or defamed other countries. This kind of hypocritical and hegemonic behaviors must be corrected.[87]

U.S. and Chinese espionage activities against commercial entities appear to be similar. While U.S. assurances that government intelligence is not passed on to companies may seem credible to a Western audience, from a Chinese perspective such assurances look hypocritical.[88] Clearly, the United States still holds that effective norms of cyber espionage require raising the cost of commercial espionage (e.g., FBI accusations of Chinese military officials). This is consistent with the reciprocal expulsion of staff of diplomatic missions for espionage during the Cold War.[89] As in the regime against privateering, however, a regime against commercial espionage may require a political deal. In light of the scale of espionage pursued by the so-called five-eyes community,[90] other countries are not likely to be willing to give up their espionage capabilities.

Finally, it is very unlikely that there will be a regime regulating the use of non-state actors anytime soon. Existing forums for cooperation will continue to exist and are likely to be expanded. As cybercrime becomes an increasing problem for all states, the scope for cooperation will increase, and the scope for collusion

[84] See, e.g., Xin Zhang et al., "Scion: Scalability, Control, and Isolation on Next-Generation Networks," paper presented at the 2011 IEEE Symposium on Security and Privacy (SP) in Oakland, Calif., 22–25 May 2011.

[85] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology*, Vol. 4, No. 1 (March 2010).

[86] David E. Sanger, "With Spy Charges, U.S. Draws a Line That Few Others Recognize," *New York Times*, 19 May 2014.

[87] Li Baodong, "Address by Vice Foreign Minister Li Baodong at the Opening Ceremony of the International Workshop on Information and Cyber Security," Ministry of Foreign Affairs of the People's Republic of China, 5 June 2014. http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1162458.shtml.

[88] David E. Sanger, "Fine Line Seen in U.S. Spying on Companies," *New York Times*, 20 May 2014.

[89] Nye, "The Regime Complex for Managing Global Cyber Activities," p. 10.

[90] The five-eyes community refers to the intelligence cooperation program between the United Kingdom, United States, Canada, Australia, and New Zealand.

between state and non-state actors is likely to decrease. States, however, are likely to continue to rely on their large technology champions to provide information and access. It remains to be seen whether the Snowden disclosures will have a long-term economic impact on U.S. technology firms. If so, we may expect greater political action from private industry against state exploitation of its resources. Further research should focus on the unintended consequences of state-sponsored and state-tolerated malicious activity as well as on possible avenues for cooperation to reduce those consequences.

About the Cyber Studies Programme

The Cyber Studies Programme seeks to create a new body of knowledge that clarifies the consequences of information technology for the structures and processes of political systems.

Our research mission is (a) to produce scholarly works that contribute to major academic debates and opinions; and (b) to apply these new understandings in the analysis of major policy problems affecting the security and welfare of states and citizens.

Our teaching mission is (a) to support, guide, and train students and researchers in Oxford and beyond in the work and methods of cyber studies within the subdisciplines of political science; and (b) to foster understanding across technical and non-technical communities to promote the development of this new field of study more broadly.

The Cyber Studies Programme is hosted by the Centre for International Studies in the Department of Politics and International Relations, University of Oxford.

Acknowledgements

The author thanks Lucas Kello, Neil MacFarlane, and Ian Brown for their excellent guidance and support in the preparation of this paper. The paper also profited from the comments of members of Oxford University's Changing Character of War Programme and the Centre for Doctoral Training in Cyber Security. Any errors in the work are the author's.

European Union
European Social Fund

Investing in your future

This publication is funded by the European Social Fund and the Estonian Government