New Pirates, Old Solutions: An 18th Century Approach to Cybercrime

AUTHOR
Filip Norén

ABSTRACT
Various authors on cybersecurity have compared cyberspace to the high seas and suggested that states should contract privateers, in the form of private corporations or individuals, in order to bolster their defensive and offensive capabilities in cyberspace. This conceptual paper explores the high seas-cyberspace analogy and evaluates the extent to which it can strategically inform the battle against cybercrime. It is argued that the historical battle against piracy, characterized by its emphasis on legal frameworks, the removal of market support structures, and states’ use of privateers, offers limited lessons with regard to cybercrime. The analogy suggests that strategies against cybercrime should stress the usefulness of existing legal structures and earmark additional resources for them, while also prioritizing the establishing of specialized cybercrime courts and the hiring of former cybercriminals. Moreover, the comparison between piracy and cybercrime suggests that cybercrime should be treated as a socio-economic problem, while the historical use of privateers can be reimagined as cyber-privateering to potentially construct a new model of cyberdeterrence.

Correspondence Address
Filip Norén, MSc Student, University of Leiden, Netherlands.
Email: n.f.noren@umail.leidenuniv.nl

INTRODUCTION
At a glance, the high seas and the Internet seem to have little in common, perhaps except the fact that the Internet works through undersea cables. However, they share significantly more since both domains are vast and partially ungoverned, yet critical for trade and communication. Many cybersecurity issues come with a high seas counterpart. Singer and Friedman, in their book Cybersecurity and Cyberwar: What Everyone Needs to Know, suggest that the way in which piracy and privateering were managed historically “provides an instructive parallel to explore for cybersecurity today” (2014, p. 178).

This paper uses Singer and Friedman’s mention as its foundation, exploring in the first section various aspects of the analogy. Most literature that uses it focuses on privateeering as a means to bridge public-private divides, whereas this paper targets piracy and cybercrime. In the second section, the measures that were key in ending the so-called Golden Age of Piracy will be examined through a limited historical investigation. In the third section, the two preceding sections are tied together to identify strategic aspects in which the present-day battle against cybercrime can be bolstered by insights from the fight against piracy. As such, this is a conceptual paper that explores the extent to which the successful battle against piracy on the high seas might be translated into the 21st century to combat cybercrime.

THE HIGH SEAS-CYBERSPACE ANALOGY

Pirates and Privateers - Then and Now
It is customary by now for authors on cybersecurity to bring up increased engagement with, and by, the private sector as a solution to cyberinsecurity (Singer and Friedman, 2014).1 In

1 Regardless of an author’s specific purpose, be it financial cybercrime, cyberwarfare, cyberdefense, and so on, they tend to recommend “better” leveraging of private sector knowledge for public gain. See, for...
doing so, they are typically concerned with avoiding a ‘Wild West’ of cyberattacks, a scenario that is colorfully captured in the free-for-all that sometimes characterized the Golden Age of Piracy (Garrett, 2013). Given the centrality to the analogy of private actors, it is necessary to delineate what privateers were in the historical, seaborne sense. Privateers commonly were “private actors using their own resources and ships to attack merchant shipping” and relied on ‘letters of marque and reprisal’ for doing so (Spearin, 2014, p. 99). Other scholars define privateering simply as “state-sanctioned piracy” (Boot, 2009, p. 96). Indeed, as we will see in section two, “privateering did not differ from piracy in the substantive nature of the conduct, but only in the attendant formalities” (Kontorovich, 2004, p. 214).

Singer and Friedman point to the similarities between privateers and ‘patriotic hackers’ (Singer and Friedman, p. 177; see also pp. 110-114). Both groups are licensed, explicitly or tacitly, to act on behalf of the state without being a formal part of it. Privateers can also be analogous to private cybersecurity actors contracted by state agencies, such as America’s National Security Agency (NSA), to bolster cyber (military) forces. In other words, cyber-privateers collectively represent both state-sanctioned pirates and patriotic hackers. Like privateers at sea, much of the value of ‘cyber-privateers’ rests with the difficulty of successful attribution, the identification of the source or organizer behind an attack. The port blockades that pirates and privateers operated effectively correspond to DDoS attacks. Similarly, acts of theft and hijacking essentially correspond to today’s data breaches affecting corporations and individuals.

Lastly, both the privateers and pirates of old and today’s cyber criminals attack economic infrastructure and military assets (Singer and Friedman, 2014, p.177). For instance, hackers hijacked online client operations at Banrisul, a major Brazilian bank, in 2017, stealing clients’ credentials (Lynch, 2017). By contrast, direct attacks by state actors on economic and military assets are not covered by the analogy herein. An example for comparison is the 2007 Operation Orchard, during which Israeli state forces cyber-neutralized Syria’s air defenses while fighter jets decimated a Syrian nuclear facility (Makovsky, 2017).

The Cyber-Privateering Debate

Aside from Singer and Friedman, the concept of privateers in cyberspace is the subject of a limited literature. The term “cyber-privateering” may have originated with a 2015 report on how the US government could empower financial institutions in “the private sector—and even private individuals—to pursue economic warfare on its behalf” (Zarate, p.24). In the US, some suggest that the solution to the problem of cyberattacks can be found in Article I, Section VIII of the Constitution: the Congressional power to grant letters of marque and reprisal (Garrett, 2013; Zarate, 2015; Mazanec and Thayer, 2015; Egloff, 2017). While these authors mainly envision a cyber-privateering regime that bestows private actors with more powerful means of defending themselves in collaboration with governments, others argue that they should be allowed to offer and employ offensive capabilities, including those that governments are currently lacking (CCHS, 2016). Offensive cyber capabilities are often considered the most extreme on a ‘sliding scale’ of active cyber defense, or ACD, measures (Hoffman and Levite, 2017).

Combining rhetoric of more active measures and the high seas-cyberspace analogy, Jeremy and Ariel Rabkin argue that the analogy’s merit lie in the grey zone between tension and war: “Cyber conflict should be open—as naval war has been—to hostile measures short of war, to attacks on enemy commerce, to contributions from private auxiliaries” (2013, p. 197).  

4 Rosenzweig (2014) constructs a useful typology concerning the effects of, and the degree to which, measures affect external networks.

5 This is how Russia and China exploit the concept of grey areas of conflict, as they do not see the typically Western, binary understanding of conflict as either a state of peace or a state of war. See, for instance, Neither War nor Peace: The Uses of Constructive Ambiguity, The Economist (2018).
A particular topic related to the cyber-privateering debate that has received scholarly attention lately is cyber deterrence. Some, such as Zarate, argue that more systematic use of private actors working “in concert with the government” would create a new level of cyber deterrence (2015, p.25). Private actors possess a majority of the knowledge needed to dependably identify attackers and move from attribution to retribution. The latter corresponds to the more extreme measures within the above-mentioned ACD spectrum. However, Singer and Friedman join others in pointing out that the difficulty in attribution of cyber attacks is a central reason that prevents the direct application of deterrence theory in cyberspace (2014, pp. 136-137; Mazanec and Thayer, 2015). Others have raised the concern that cyber deterrence may not work as well as nuclear deterrence (Libicki, 2009). Overall, there is a lack of empirical evidence on the prevalence of ACDs and the effectiveness of cyber deterrence (Hoffman and Levite, 2017).6

In sum, scholars have employed the high seas-cyberspace analogy to describe an ecosystem in which states are in need of added capabilities as they interact to varying extents as allies and enemies with private actors. This paper, by contrast, maintains a narrower focus on the usefulness of the high seas-cyberspace analogy at the strategic level against (mainly non-state) cyber criminals.

HOW PIRATES WERE DEFEATED ON THE HIGH SEAS

Outlined below in their respective sections are the boundaries of the so-called Golden Age of Piracy as discussed in the literature and two major themes of anti-piracy measures: the shutting down of markets and support structures, and the commissioning of privateers to directly target pirates as a complement to state navies.

The Golden Age of Piracy from an Academic Perspective

The concept of a ‘Golden Age of Piracy’ is contested by historians in terms of its boundaries in time and space, yet it is useful in understanding the ecosystem in which pirates and privateers were most active. The first systematic use of the term appears to be from 1897, when historian John Fiske held that it “may be said to have extended from about 1650 to about 1720” (1897, p. 338). While Fiske refers to the greater West Indies and the US Eastern Seaboard, Konstam and Cordinally limit their definition to the Caribbean “…from 1714 until 1722, so the true Golden Age cannot even be called a ‘golden decade.’” (2005, p. 98). Tellingly, several scholars have revised their definitions at least twice (cf. Rediker, 1981; 2004; Cordinally, 1994; Konstam and Cordinally, 2005).

For the purposes of this paper, it is sufficient to note a convergence around Fiske’s boundaries as they reappear in more recent works (Botting, 1978; Cordinally, 1994; Rediker, 2004).7 Since Britain was the major geopolitical power of this era, most examples and references will be made to it, although other powers feature as well.

Shutting down markets and support structures

The first key theme of counter-piracy success in the past was the shutting down of safe havens by cleaning up markets and removing support structures. The first component of this strategy was the clean-up of incompetent or corrupt officials from positions of power. Two British examples are Governor Nicholas Trott of the Bahamas, deposed in 1696, and Governor Benjamin Fletcher of New York, removed the following year (Boot, p. 98). Another tool was the recruiting of former troublemakers to secure competent leadership. The ‘revolving door’ between the public and private domains is not a recent phenomenon, in spite of the contemporary woes (Stephenson, 2014). The case of Sir Henry Morgan serves as an example; his activities as a privateer led to his arrest by the British Crown, yet this experience also saw him knighted and sent to Port Royal, Jamaica, as Lt. Governor.8 He helped the city shed its status as a sanctuary for pirates and their trade, defending it against raids by pirates and French privateers. Similarly, despite the strict legal regime of the Netherlands during the Golden Age, numerous Dutch seamen

---

6 To the extent that such evidence exists, it is probably to be found in the grey literature.

7 Rediker’s most recent, and most complex, definition of the Golden Age of Piracy consists of three temporal subdivisions, or “generations”: the buccaneers of 1650–1680, the Indian Ocean pirates of the 1690s, and the pirates of 1716–1726 (2004, p. 8).

8 A non-British example: “The French privateer Jean Bart was so effective in attacking Dutch shipping in the late seventeenth century that King Louis XIV ennobled him and gave him a captain's commission in the French navy” (Boot, p. 98).
charged with piracy were “rehabilitated to serve the state” (Lunsford, 2005, p. 141).

The second component in the clean-up of power and trading structures was to more firmly establish the rule of law. Authors belonging to a certain strand in the study of history or international law ascribe the decline of piracy to the use of universal jurisdiction for prosecuting pirates (Bassiouni, 2001; Jarvis, 2006). Courts and commentators have “misinterpreted jurisdiction [over piracy] as based upon universality” because of rhetoric that branded pirates as the enemy of mankind (Garrod, 2014, p. 202). “Rather, pirates were the enemies of the State that labelled them as such” (Ibid.). Benton clarifies that “even when the discourse labelling pirates as the enemies of all mankind emerged in full voice, the mechanisms for controlling piracy under the law remained those of municipal law” (Benton, 2011, p. 239).

Rather than universal jurisdiction, the critical legal reform was to geographically extend the reach of municipal law to piracy-infested areas. In 1700, Britain’s Parliament provided for Vice-Admiralty courts consisting of seven ‘commissioners,’ typically naval officers as opposed to regular judges. These courts helped speed up prosecutions by convening far afield (Boot, p. 99). Numerous European maritime powers followed suit, implementing decentralization models that enabled their anti-piracy campaigns (Ritchie, 1986; Benton, 2011, p.232). As they did so, these powers called upon “the principle of universal jurisdiction over piracy as a tool for advancing political interests or imperial expansion,” not in its (dubious) legal sense (Kempe, 2010, p. 371; also, see Garrod, 2014).

At the receiving end of this invigorated legal regime, it is necessary to acknowledge a more sinister account of history. Rediker surveys primary sources to show how “the Atlantic Empires, led by Britain, organized an international campaign of terror to eradicate piracy, using the gallows in highly public displays of power” (2004, p. 10). While the maltreatment that sailors suffered at the murderous hands of captains of contemporary ships probably contributed to their decisions to become pirates (Ritchie, 1986; Rediker, 2004, p. 17), Rediker excessively victimizes the pirates as revolutionaries in legitimate pursuit of an egalitarian community. Rather than primarily being casualties of social class and the mercantilist state, pirates suffered a heavy-handed response because the nascent international (colonial) system depended increasingly on transoceanic trade. The 173 peace treaty at Utrecht caused thousands of unemployed sailors to look for work as pirates. Albeit despicable in humanitarian terms, the crackdown corresponds to the perceived level of threat that pirates posed to core state interests.

**Enlisting Privateers to Support State Navies**

The growing dependence among European maritime powers on protected shipping routes to distant parts of their overseas empires resulted in the increased use of, and regulation of, privateers. For instance, the Dutch developed a sophisticated regulatory system for privateers that severely punished violators (Lunsford, 2005). Similarly, the British practiced judicial specialization for privateers, much like in the case of pirates, by setting up specialized prize courts for captured booty (Richard, 2010). The seriousness of this effort was perhaps felt more than anyone by Captain Kidd, who was hanged after seizing vessels in violation of his privateer commission (Ibid.).

As the practice of privateering matured, states increased their use of privateers for the specific task of pirate-hunting. For instance, the Bahamas was a pirate rendezvous in 1718, despite being a British colony. Woodes Rogers, a British privateer, was commissioned to reinstate government control, successfully expelling the pirates and fending off the Spanish Navy (Woodard, 2007). In another instance of ‘the revolving door,’ Rogers was subsequently appointed Governor of the Bahamas and proceeded to disperse many a Caribbean pirate by, in turn, commissioning privateers (Ibid., pp. 284-5).

However, the role of privateers in ending the Golden Age of Piracy is often downplayed by authors arguing that states could not develop international norms against piracy and suppress it until privateering was delegitimized (Thomson,

---

9 See also Kontorovich (2004).

10 For a more detailed account, see Benton (2009).

11 Rediker (2004) has illuminating accounts on the particular role of the slave trade in transatlantic commerce as well as in piracy, both of which lie outside the scope of the present argument.

12 The scale of the unemployment among sailors was extensive. For instance, the British Royal Navy reduced its number of sailors by over 36,000 over a period of two years (Rediker, 2004, p. 23).
Golden Age Piracy ended a century before privateering was abandoned in the 1856 Paris Declaration Respecting Maritime Law, at least in the West. In the words of Richard, “piracy suppression had less to do with delegitimizing privateering and more to do with establishing the rule of law” (2010, pp. 436-7). Towards this end, privateers were not alone, but rather complemented regular state navies; “together they effectively hunted down pirates” (Ibid.).

APPLYING 18TH CENTURY LESSONS TO 21ST CENTURY PROBLEMS

As previously outlined, most authors employ the high seas-cyberspace analogy to argue for issuing letters of marque in order for private entities to defend themselves against cyberthieves. This section aims to apply the strategic lessons from the fight against piracy to the cybercriminal realm such that governments and corporations alike can achieve greater deterrence and chances of prosecution. While authors have created various typologies of cybercrime, there is no universal definition (Chang and Grabosky, 2014). The definition used here is “criminal offences specifically related to computers and telecommunications, or crimes that have taken place within cyberspace” (Ibid., pp. 322-3).

Shutting down cyber safe havens

Akin to Golden Age pirates, cybercriminals rely on cryptomarkets to trade technical tools or services needed for cyber attacks, as well as products derived from the ‘loot.’ The ubiquitous example is the Silk Road, the largest Dark Web market until it was dismantled in 2013, offering cybercrime-as-a-service, credentials, stolen identities, as well as drugs and weapons, etc. Whereas piracy was relatively limited, although with far-reaching political-economic consequences, it is difficult to estimate the extent of cryptomarkets. Pirates themselves estimated that the all-time peak in their global number was 2,400 aboard 30 ships in 1716 (Rediker, 2004, p. 29). A 2014 study suggests the Silk Road was just the tip of the iceberg (Martin, 2013), while a 2016 study using a near-identical definition of cryptomarkets found that “about 20 cryptomarkets [were] active” (Broséus et al., p. 11). The issue is that it is difficult to estimate how much trading is done on the Deep Web. It is probably substantial, but the impact is softened since access is limited for all but the highly skilled.

In addition to markets, cybercriminals rely on disreputable Internet Service Providers, or ISPs, for access to basic Internet infrastructure. The term bulletproof hosting (BPH) captures how these providers enable their customers’ dubious or illicit activities, sometimes due to incompetence or ethical stances, but mainly for profit. To illustrate the impact of BPH, consider the Rustock botnet. “At its peak, it was blamed for about 60 percent of the spam sent daily” (Bright, 2011). Its takedown, called Operation b107, was led by Microsoft and involved US federal law enforcement agencies, cybersecurity company FireEye, and the Dutch and Chinese governments (Ibid.). The importance of reducing the number of BPH providers is impossible to overstate as many cybercriminals would not be able to operate without them (Goncharov, 2015). That is because they constitute hideouts, much like physical ports

13 “Piracy did reemerge in the early nineteenth century as a result of privateers, notionally supporting independence movements, going rogue... The pirate crews, however, were not limited to privateersmen. Former naval personnel, sailors, fishermen, slaves, and criminals all joined pirate companies” Peter Earle (2006), The Pirate Wars, (St. Martin's Griffin), p. 211, quoted in Richard, 2010, p. 437.

14 As also argued in more detail by Cordingly (1995, p. 222).

15 The term ‘cryptomarket’ originated as a colloquial online term, but has also been adopted by academia and refers to “an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities” (Martin, 2013, p. 356). Not all transactions on cryptomarkets are illegal.
did for Caribbean pirates before they were brought under imperial control.

The historical analogy, as seen in Section 3.2, suggests that governments should impose stricter regulatory control over cryptomarkets and hosting structures, while also recruiting former cybercriminals. It also suggests executing substantial numbers of cybercriminals. Naturally, we can dismiss the latter as morally outdated, not to mention operationally difficult.

Regarding stricter regulatory control, the Silk Road and Rustock takedowns exemplify how technical capability in law enforcement is less problematic than commonly imagined (Hayes et al., 2015). Contrary to claims that law enforcement agencies are ‘going dark’ in the face of technology, “law enforcement has much better and more effective surveillance capabilities now than it did [in the Internet’s youth]” (Abelson et al., 2015, p. 71). In cybercrime, governments’ problems remain close to those of ‘traditional’ crime, revolving around clashing national and international jurisdictions, hiring elite cyber forensics investigators, and being able to afford enough of them, according to Europol and Eurojust staff (Hayes et al., 2015).

The historic overseas extension of legal regimes such that prosecution could take place where piracy took place cannot be readily applied in cyberspace. Local laws at the national level are already the primary tools for enforcing the rule of law against cybercrime. However, the analogy suggests that the specialization of courts must be accelerated. Like the piracy courts of old, regular judges or juries could be replaced with persons holding deeper knowledge in cybersecurity and cybercrime, who are better suited to evaluate evidence.

Regarding jurisdictional issues in the international battle against cybercrime, the analogy is less instructive. Britain secured its position as the premier naval power at this time, unilaterally exerting state power as the piracy threat to trade started to outweigh the risk of conflict with (mainly) France, Spain and the Netherlands (Rediker, 2004). In cybercrime, some geopolitical dimensions apply given that BPH operators often choose political hotspots as shields against takedowns. For instance, most BPH operations on the Dark Web operate from Russia, Ukraine or Moldova (Mahjoub and Passwaters, 2017). For jurisdictional reasons, courts cannot touch such operations in unilateral moves similar to historical anti-piracy moves by the British. Also, operators commonly place different customers in different countries according to the type of content they offer (Mahjoub, 2017). These key challenges for governments in combating cybercrime operations can perhaps only be addressed with greater international cooperation, not legal specialization. Hence the piracy analogy fails to explain how a state can create incentives for another to mitigate cybercriminal operations in its territory.

The revolving door that propelled privateers Woodes Rogers and Sir Henry Morgan to governorships in the Caribbean translates into the hiring of cybersecurity professionals and even cybercriminals for high-ranking government jobs as investigators and administrators. Associated problems include cultural clashes with government bureaucracy, background checks that take years, and relatively low pay (Peterson,

introduced specialized cyber prosecution units, see Pisaric (2017). Malaysia is another example (Habibu, 2016). BPH providers also flourish in ostensibly cleaner jurisdictions. In terms of spam operations originating in their territories, the US and the UK combine to host as many as Russia and China combined because of loose laws, or loose enforcement thereof. See Spamhaus.org. Zarate (2015) proposes drawing inspiration from counterterrorism and anti-money-laundering efforts of the Financial Action Task Force in the cyber realm. If a cyber norms framework was created around the international financial system, ostracizing or barring States that fail to quash domestic actors launching cyberattacks on that system, those norms may be followed. That is because States and bankers would ultimately be guided by self-interest rather than “high-minded appeals to the law of armed conflict” (Zarate, 2015, p. 4).
The persuasive power of the ‘privilege of public service’ is questionable (Ibid.). Nevertheless, the analogy suggests that the urgency and amount of resources afforded to these recruitment efforts should increase significantly.

In sum, the high seas-cyberspace analogy is instructive for issues of court specialization, manpower, and the salience of ‘regular’ municipal law. It fails to contribute to jurisdictional issues, including how to investigate and prosecute more effectively given that the physical infrastructure of the Internet always lies within the national jurisdiction of some country.

**Expanding State Capabilities**

The dynamic of sailor unemployment and use of privateers by states in the Golden Age is illuminating for the cyber realm in several ways. Consider the overrepresentation of Russians in cybercrime. According to Galeotti, Russians account for 35 percent of global cybercrime revenue, but only one percent of the global ICT economy (2011). He attributes this to the fact that “a disproportionate number of Russians have world class math and computers skills, yet not the kind of jobs to use them legitimately” (Ibid.).

There is some empirical evidence to support a correlation between weak economic development and escalating levels of cybercrime (Kshetri, 2010; Ojedokun and Eraye, 2012; Odekshola and Adeta, 2013). Ilievski and Bernik synthesize the results of research on the connection between cybercrime and social-economic factors, finding three empirical studies that establish statistically significant correlations between social-economic characteristics, including unemployment, GDP per capita, and education, and perpetration of cybercrime, such as phishing and fraud (2016). As such, there is reason to believe that the historical case in which states provided fruitful employment for seamen can be instructive in the sense that expanding state cyber forces could reduce cybercrime.

If political or practical realities should preclude an expansion in states’ cyber forces, the Golden Age reliance by governments on privateers to supplement their capabilities can still inform the battle against cybercrime. After crafting detailed contracts - akin to letters of marque - specifying the enemy assets to be targeted, cybersecurity contractors could be permitted to attack or disrupt the (hostile) activities of another state, or actors believed to act as proxies of another state. Importantly, the contracted private companies already hold a majority of the cyber expertise available.

As opposed to the current ad hoc public-private organizational model, a more institutionalized cyber-privateering model has several substantial implications. First, it helps align various interests against cybercrime. By empowering private organizations to defend themselves against state and non-state cyber attackers to a greater degree, they help the state in protecting intellectual property and data privacy to the benefit of citizens broadly. Second, cyber-privateering projects state power to adversaries, boosting deterrence on account of the private sector’s superior cyber capabilities.

While Zarate expresses hope that a “doctrine of cyber deterrence may emerge in the context of the cyber-privateering model” (2015, p. 26), one must also consider the perils. Consider, for instance, a cyber-privateer firm that responds offensively to data breaches, but goes off script and starts attacking lawfully operated ISPs abroad, reminiscent of Captain Kidd’s last adventure. Such an instance poses critical political as well as regulatory risks to states, with outcomes that are difficult to survey. Again, since all physical components of the Internet’s infrastructure lie within national jurisdictions, an offensive operation by a cyber-privateer can have highly complex consequences as it likely would include servers across the globe (Libicki, 2009; New Pirates, Old Solutions
Mazanec & Thayer, 2015). Lastly, a complicating factor is how cyberdeterrence might be less effective than military deterrence. Whereas pirates (and privateers) faced retribution that often took the form of imprisonment or execution, cybercriminals are physically and legally protected to a greater degree. Arguably, for cyber-privateering to have a deterrent effect, it must be coupled with the legal specialization and strengthened human skills outline above.

In sum, the high seas-cyberspace analogy suggests that cybercrime should be treated as a socio-economic problem to a greater extent and indicates that increased hiring into state cyber forces may reduce cybercrime. Meanwhile, a cyber-privateering model promises to unlock cyber capabilities in pursuit of state interests, although its deterrent effect is unclear.

CONCLUSION

Cyberspace develops exponentially in terms of data and speed, while governments move “at a glacial pace, if that,” as Singer and Friedman accurately put it (p. 198). Given that the international community still does not fully understand high seas piracy, exemplified by recent experiences in the Gulf of Aden, it has arguably made significant progress regarding cybercrime. The Silk Road cryptomarket and the Rustock botnet, among many similar takedowns, illustrate that legal-technical and public-private cooperation, not to mention grand-scale international cooperation, are possible and do occur. The extent to which the cyber-piracy analogy can contribute strategically to greater numbers of such achievements is not clear-cut, however.

The high seas-cyberspace analogy does have some illuminous value to guide the future of cybersecurity. This is particularly true in understanding the salience of incentive structures that connect cybercrime, regulation, and private sector agency. Equally, the comparison is conceptually useful in understanding the limited reach of government power through law enforcement agencies. However, the comparison is not as powerful as Friedman and Singer appear to indicate in their 2014 book, which inspired the present inquiry.

The cyber-piracy analogy does little to offer new tools of coercion to be used against states that willfully harbor cybercriminals, such as Russia’s ‘patriotic hackers’ - the equivalent of loyal pirates. Whereas Britain was in a position to impose its will and gradually defeat widespread piracy practices (mainly in the Caribbean), no state has such geopolitical power or legal reach on the Internet. Likewise, the analogy fails to identify new incentive structures that can encourage states to impose their own existing laws to the detriment of domestic cybercriminals.

Nevertheless, the high seas-cyberspace analogy highlights a number of strategic areas where current public and private efforts against cybercrime must be expanded and reinforced. First, the Golden Age of Piracy suggests that the emphasis on enabling structures should be reinforced. The removal of cryptomarkets and bulletproof hosting services can be aided to an extent by the specialization of courts and the training of cyberforensics investigators and prosecutors, although the problem of physical jurisdictions remains. As such, the constraints on governments are often shared with age-old battle against ‘analogue’ crime. Second, the creation of organized cyber-privateering through a modern-day letter of marque is a complementary way of acquiring the human expertise needed. It may emulate a deterrent effect upon cybercriminals reminiscent of that of seaborne privateers upon pirates. Third, the analogy points to the need to treat cybercrime as a socio-economic problem. States can reduce the incentives for cybercrime by offering more fruitful employment for cyber-savvy individuals.

Ultimately, it is noteworthy that the Council of Europe’s Convention on Cybercrime, or the Budapest Convention as it is commonly known, arguably constitutes international cooperation in cybercrime prevention at a level to which 18th century counter-piracy cooperation never came close. Although the Convention is toothless in practice (Chang and Grabosky, 2014), this demonstrates a willingness to seek state-level dialogue. If combined with the revitalization of existing strategies against cybercrime, as suggested by the comparison between piracy and cybercrime, there emerges a promising formula for the battle against cybercrime.

BIBLIOGRAPHY


Rosenzweig, P. (2014). International Law and Private Actor Active Cyber Defensive


