Volume **4** (1) 2022 https://doi.org/10.5204/lthj.1583

Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers?

Josephine Helen Dwan
UNSW Canberra, Australia
Tamsin Phillipa Paige
Deakin University, Australia
Rob McLaughlin
University of Wollongong, Australia

Abstract

Understanding the descriptors attached to cyber operations and cyber actors is crucial to communicating the nature of these entities and the influence they wield in cyberspace. Given the ever-increasing threat that corporations, governments, and the everyday consumer face from these entities, it is paramount that respondents evaluate and apply the most appropriate descriptors when communicating about such incidents. In this paper, we discuss whether a 'privateer' analogy has relevance in this space given the current state of cyber-actor behaviour and the increase in the number of governments relying on external experts to design, construct, and execute cyber-disruption operations.

In determining the appropriateness of the 'privateer' analogy, we explore the following questions:

- What types of labels are available for this private actor-perpetrated, but state-purposed cyber-operational conduct?
- Based on a brief history of privateering, how and why might privateering be an appropriate analogy?
- Given the strict legal paradigmatic constraints surrounding the availability of the concept and the availability of modern Law of Armed Combat (LoAC) concepts to cover the practice, how and why is privateering not an appropriate analogy?

Ultimately, we conclude that the applicability of the 'privateering' analogy in the context of cyber operations is dubious. It appears that international law has developed beyond the need (and desire) for privateers and privateering operations. In this discussion, we consider legal and regulatory alternatives for responding to cyber behaviour that may still resemble privateering under effective (and much more current) international law.

Keywords: International law; cyber proxies; cyber operation; law of armed combat; privateer; privateering.

I. Introduction

The activities of state-sponsored hackers, who operate with a 'for-profit' motivation and engage in a form of cyber disruption designed to gain an advantage (intelligence, security or propaganda) for a sponsor, are no secret. One of the earliest known international cyber-espionage incidents can be traced to1986 when German hackers searched through thousands of United States (US) computer files and sold the stolen materials to the *Komitet Gosudarstvennoy Bezopasnosti*. (KGB)[1] Five (West) German nationals were ultimately convicted in the now unified state's first computer-hacker trial for selling information to the Soviet Union, having used nothing more than a commercial home computer and a telephone. The group's activities had been discovered by a California-based systems administrator at the computer centre for the Lawrence Berkley Laboratory (LBL).

[1] Reuters, "2 W. Germans Get Suspended Terms as Computer Spies."

Ultimately, the installation of a honeypot[2] was used to trap and ensnare the hackers. At the time, this type of remote hacking was entirely new and not fully understood by the law enforcement authorities tasked with collecting evidence and initiating a criminal prosecution against the hackers. It took significant effort by the LBL to obtain the cooperation of the Federal Bureau of Investigations (FBI) and the German government to identify and prosecute the hackers. However, Chief Judge Leopold Spiller handed down a lenient sentence due in part to the fact that "[I]t could not be proven that substantial damage had been done to the Federal Republic (West Germany) nor its [North Atlantic Treaty Organization] NATO partners".[3]

More recently, on 22 July 2020, officials from the US accused China of sponsoring criminal hackers who were targeting biotechnology firms around the world working on various Coronavirus Disease 2019 (COVID-19) vaccines and treatments.[4] The US Justice Department charged two former engineering students with hacking various companies engaged in high-technology manufacturing, pharmaceuticals and gaming software development, and with targeting dissidents, clergy, and human rights activists in the US, China, and Hong Kong. It is alleged that the defendants instigated cyber operations for their own profit but also for the Chinese Ministry of State Security, a civilian spy agency responsible for counterintelligence, foreign intelligence, and domestic political security. This incident marks the first time that the US has charged suspected Chinese hackers with working both to enrich themselves and as cyber agents of a foreign government, something that prosecutors characterised as a "blended threat" '.[5] Another recent accusation of cyber interference—this time emanating from Russia—also concerned COVID-19 research. On 17 July 2020, security officials in the US, Britain, and Canada accused hackers linked to a Russian intelligence service of trying to steal information from researchers working to produce COVID-19 vaccines.[6] The hackers belong to a unit known across the web as 'APT29', 'the Dukes', or 'Cozy Bear', who operate as one of the two Russian spy groups alleged to have penetrated the US Democratic Party's computers in the lead up to the 2016 presidential election.

Each of these incidents highlights the long-standing but growing tensions emanating from state-facilitated, sponsored or endorsed 'private' cyber operations. There are myriad other examples of cyber conflict facilitated by such cyber proxies, dating back to the very earliest days of the Internet,[7] and given that the global rates of cybercrime are increasing year upon year, there are clear indications that malicious conduct through the use of Internet-based services will become the norm for both global organised crime and state-sanctioned grey and black cyber operations.[8] However, uncertainty remains as to the categorisation and concept definition, particularly with respect to the oft-used term 'cyber proxy' and who, if anyone, would then appropriately fall within this definition in terms of modern cyber operations. The question raised in this paper is whether incidents such as these demonstrate the utility of a 'privateer' analogy to cyber-disruption operations and 'cyber proxy' definitions. Given the growth of such incidents, an assessment of the applicability of historical international law concepts, such as 'privateer', to modern cross-state cyber-incidents may prove useful in understanding the implications and validity of the re-purposing of such legal terms of art. Thus, the question of whether state-sponsored hackers are modern-day privateers is important at this time, especially given that the 'private' actors fundamental to the incidents noted above were 'permitted' to act in in these ways to further the interests of a particular state, while also securing profit or compensation for their efforts. On the surface, there appears to be a strong case for applying the 'privateer' analogy to modern hackers, but as this paper discusses, the idea of a return to lawful privateering operations is one that international law has strongly resisted since the 1856 Declaration of Paris.[9]

One reason why the privateer analogy is so seductive to cyber-espionage and cyber-disruption activities is that private activity with public and diplomatic consequences is not a new phenomenon. The activities of such state-sponsored hackers (which should be distinguished from hacking collectives that operate more directly as agents of the state) are reminiscent and, as a number of scholars and analysts have observed,[10] reflective of the activities of privateers prior to the 1856 Declaration of Paris that banned this practice. The similarities lay in the fact that these hackers: (1) target states as directed and authorised by their sponsor state (under a 'letter of marque'); (2) focus on creating disruption but also take from these acts some form of profit ('prize'); (3) concentrate on 'soft targets' ('merchant vessels'); and (4) operate with a high degree of autonomy (as an adjunct to, but not part of, the state's military forces).

[2] A computer security mechanism data that appears to be a legitimate part of a site and contain information or a resource of value to attackers but is actually isolated and monitored and enables the attackers to be blocked or analysed.
[3] Associated Press, "Hackers Found Guilty of Selling Computer Codes."
[4] Nakashima, "U.S. Accuses China of Sponsoring Criminal Hackers."
[5] Nakashima, "U.S. Accuses China of Sponsoring Criminal Hackers."
[6] ABC/Wires, "UK Accuses Russia of 'Despicable' Hacking Attacks."
[7] Reuters, "2 W. Germans Get Suspended Terms as Computer Spies."
[8] Morgan, "2019 Official Annual Cybercrime Report."
[9] Paris Declaration Respecting Maritime Law.
[10] Egloff, "Cybersecurity and the Age of Privateering," 231–247.

In this paper, we seek to assess the utility and viability of the privateering analogy for emerging and escalating private cyber actions with public and international security consequences. As will become evident, it is our conclusion that the application of this analogy is dubious in the modern age, particularly given the strong condemnation of privateering and piracy in general under international law. In addition, there are still unsettled opacities in cyber operation related definitions, and it is likely that a cyber-privateering analogy will further muddy the already murky waters in this area. The assessment conducted and the conclusions reached leverage a historical contextual analysis that uses both modern and historical resources to describe the relevant definitions for our analogy and employs the history of privateering to highlight why the analogy is so attractive. This contextualisation is then contrasted with an analysis of the Law of Armed Combat (LoAC) and wider international law developments to conclude why—in spite of its attractive nature— the analogy is ultimately unhelpful.

II. Cyber Proxies: Some Initial Thoughts About Labels …

The rise of the Internet has brought with it a significant shift in the way in which governments interact with each other in and via the cyber domain. Originating from a military project, the Internet has evolved into a key facilitator of modern global communication. After an initial lack of interest, a shift occurred when the technology emerged from academic institutes and became commercialised in the mid-1990s.[11] Within a very short period, governments around the world realised the Internet's potential as not only a global communication network but also a source of intelligence and a platform of coercion with almost unlimited reach and range. Because of its origins as an academic project, many early examples of malicious cyber activities facilitated by the Internet have been attributed to non-state actors, and early cases, such as that of the Morris Worm, were the product of private citizen endeavours.[12]

More recently there has been a significant shift in the attribution of similar cyber-espionage incidents to state-backed cyber actors, particularly since late 2010, when the public became aware of the high-level cyber-intelligence operation at the Natanz nuclear enrichment facility in Iran that purportedly involved US and Israeli developed malware.[13] As a result of this incident, governments and citizens are now acutely aware of the reality of ongoing high-level cyber-military operations, and the international community has since come to terms with the reality that cyber proxies are embedded within the Internet-facilitated communication systems on which the world currently depends. 'Cyber proxies' can thus be broadly understood as intermediaries who conduct or directly contribute to an offensive or targeted cyber action (usually across communication channels facilitated by Internet connections) that are knowingly enabled (whether actively or passively) by a beneficiary state.[14] However, as will be explored further in this section, definitions of cyber proxies, cyber actors and everything in between remain contentious, and there has been some confusion regarding the applicability of historical terms, such as 'pirate', 'privateer', or 'mercenary' to cyberspace activities. As will be reiterated throughout this paper, the inclusion of the term 'cyber privateer' in these spaces is actually detrimental, due in part to the oversaturation of the characterisation concepts already present in discussions of cyberspace.

A. The Challenge of Characterising Linkage

As mentioned above, the definitional approach to cyber proxies is admittedly broad, but it seeks to capture the varying and complex relationships that cyber proxies can share with their beneficiaries and sponsors. It is for this reason that this term will be used throughout this paper. Concern about the use of cyber proxies by states appears to stem from, among other things, the sense that (as with other more traditional and kinetic forms of proxy activity) cyber proxies present 'escalatory risks' to international peace and security.[15] However, this risk of escalation is in many ways beholden to the threshold issue of attribution or adoption and thus the character of any relationship. Cyber-proxy relationships can include 'active' arrangements whereby the proxies operate under the 'effective control' of a state and more relaxed relationships whereby the proxies receive support indirectly when a government is aware of but chooses to ignore (and thus, in terms of immunity from local jurisdiction, to facilitate) their activity.[16] Cyber proxy relationships may also include 'passive' situations in which a state repeatedly and consistently turns a blind eye to malicious activities against external targets. In such circumstances, the state may even claim that it is unwilling or unable to stop such proxy activities, which may contextually imply tacit support for the actions.[17] Other

[11] Maurer, Cyber Mercenaries.
[12] Thompson, "The Morris Worm."
[13] Kerr, "The Stuxnet Computer Worm."
[14] Maurer, "Cyber Proxies and Their Implications."
[15] Sheldon, Civil Military Integration and Cybersecurity.
[16] Maurer, Cyber Mercenaries.
[17] This is, of course, a legally crowded concept encompassing a wide range of both general and bespoke thresholds and indicia of control, attribution and adoption (across bodies of law encompassing state responsibility, the LoAC and the *jus ad bellum*) and significant debates around criteria, such as unwilling or unable (including the Bethlehem principles in the Americal Journal of International Law (AJIL)).

approaches seek to label such proxies as 'cyber mercenaries';[18] however, as mentioned above, the application of analogous terms to cyberspace activities can create confusion among observers and decision makers in these spaces. This has been an issue in discussions about cyberspace for some time, and it is unlikely (given the complexity of modern cyber operations) to be resolved any time soon, let alone in this contribution to the debate. Other approaches to defining and characterising cyber proxies, such as the LoAC, privilege the perpetrator-conflict-victim nexus, and yet other definitional approaches hinge on whether the actions of the cyber actors in question are motivated by profit.[19] It is this type of profit-centric behaviour that is often referenced in comparisons with traditional privateering and is the behaviour of focus in this analysis.

B. Why Linkage is a Key Concern and a Key Challenge

As a statement of general principle, public international law (PIL) is concerned with the characterisation and regulation of conduct between states. As a result, PIL tends to concentrate on the conduct of the 'state' and of state agents as opposed to private actors. However, this body of law (e.g., as encapsulated in the law of state responsibility) also recognises that non-state actors can effectively become state agents or that their conduct can be adopted by a state in such a way as to create attribution and perhaps responsibility for that state. This relationship is sometimes more readily identifiable where the benefit to the sponsor or harm to the target is significant and identifiable,[20] but it is (ultimately) more beholden to the indicia of a link than to the scale of effects. This is evident across a wide range of relationships between states and 'private' actors in the military, intelligence, and security domain, where solving the legal challenge of defining the relationship between the sponsor and the perpetrator of the act is often key to defining and characterising the legal nature of the act itself.

Private-security contractors are one example of this trend (usually from the delegation of cybersecurity services under sponsor-agent relationships between private entities and governments) and are a group from which definitional challenges, such as the use of the term 'cyber-privateer', can emerge. This growing reliance of states on private cybersecurity firms is particularly evident in the US, the United Kingdom, and other European and NATO countries and highlights the growing global tendency of states to leverage and in some cases rely upon private agents to facilitate and respond to cyber threats.[21] As early as 2003, *The Professional journal of the United States Army* argued that the US military should 'hire specialised [private military contractors] for specific offensive information campaigns, providing a surge capacity instead of attempting to maintain limited-use, cutting-edge skills in the regular force, far removed from its core activity'.[22] In fact, the idea of using private agents in response to cyber threats has even attracted arguments in favour of re-introducing privateering and 'letter of marque' arrangements in US cyber-military strategies.[23]

Commentators have argued that there are two main reasons for this growing trend. First, the traditional 'pure-play' defence contractors have been expanding their activities to include cybersecurity and cyber-espionage services and thus to gain a profitable share of what is a growing market.[24] Second, smaller boutique firms and start-ups have either become established contractors or have been bought by larger companies (e.g., HC Gary, QuesTech Inc, Immunity and Hacking Team) and as a result have significantly expanded their technical and operational capabilities. The types of services these companies now offer include "intelligence and operations, counterintelligence, information operations and cyber-warfare' and 'cyber forensics, exploitation, SIGINT and cyber operations support"'.[25] These service descriptions are admittedly vague, but they clearly indicate the expanding professionalisation and privatisation of cybersecurity actors beyond state military and security forces, while also highlighting the global pool of private, non-state talent governments can access when selecting cyber actors for both general services and specific operations. Additionally, some commentary argues that the introduction of cyber proxies as a solution to cyberattack threats could supplement the market failures afflicting, specifically, the US. This argument relies on the assumption that a military or government is experiencing a shortage of security measures and personnel adept at countering cyber threats, especially where these threats target private companies or citizens.[26] The argument follows that while militaries or governments are enacting change to be able to handle cyber threats themselves, the use of cyber proxies through contracts or prize law may provide a suitable alternative while countermeasures are sourced.

[18] Cruz, "Cyber Mercenaries."
[19] Cruz, "Cyber Mercenaries," 2–3.
[20] Maurer, "Cyber Power."
[21] Maurer, "Cyber Proxies on a Tight Leash."
[22] Singer, Corporate Warriors.
[23] Garrett, "Taming the Wild Wild Web."
[24] Maurer, "Cyber Proxies on a Tight Leash."
[25] Maurer, "Cyber Proxies on a Tight Leash."
[26] Garrett, "Taming the Wild Wild Web."

C. Public-Private Cyber-Operational Partnerships?

As cybersecurity displays a range of inherent differences to traditional physical security as a service offered by private operators, it is also more amenable to a private-public partnership in some ways than more 'kinetically focused' forms of operational support. Unlike many forms of kinetic offence and defence, cybersecurity practices and tools existed in the private market and were being deployed long before states and governments began to consider cyberspace a viable domain for military operations.[27] Over time and with the growth of the Internet and the development of the 'Third Wave' of technology, a preference for the privatisation of certain government functions and the emergence of the 'new public management' movement extended to cybersecurity markets.[28] Cyber operations also have the added bonus of having a much lower barrier to entry. Conventional weaponry usually requires substantial investment and manufacturing capabilities. Conversely, the development of malware for cyber operations is comparatively cheap and generally much easier to source. Consequently, the 2013 and 2015 United Nations Group of Government Experts (UNGGE) meeting records include direct references to the use of cyber proxies by international governments; however, both the UNGGE 2013 and 2015 panels failed to provide any succinct definition as to which state actors can and cannot be considered 'cyber proxies' for the purposes of international law.[29] The 2013 and 2015 UNGGE panels both advocated for a safely broad definition of cyber proxies as 'individuals, groups, or organisations, including criminal organisations [that act on behalf of states] in the conduct of malicious ICT actions'.[30]

D. Proxies or Criminals? Proxies and Criminals?

The stereotype of the cyber criminal as a 'counterculture' individual who works alone and exists on the fringes of society is neither flattering nor particularly accurate. Modern cyber criminals are generally financially motivated, highly organised groups who operate with the goal of acquiring the highest possible return for the least amount of effort.[31] The repertoire of cyber-criminal activity, ranging from extortion and fraud to outright theft, is in many ways enhanced by the cyber domain and allows criminals to leverage the remoteness, anonymity, and the high level of connectivity that the modern Internet facilitates.[32] However, what differentiates a regular cyber criminal from a cyber proxy is the dual motivations for their operations of profit and a national effect. Cyber proxies are either directly or indirectly (though the latter is more common) associated with a state and may receive instructions or tools and recommendations from their sponsoring state. Conversely, cyber criminals operate independently (and often in opposition to the law enforcement structures of the state) with a central goal of generating a profit via malicious means.[33] Of course, the very notion of 'profit' in the cyber world is often diverse and many steps may be required to produce a tangible, usable 'currency' or tradable goods or services. This indirect means of generating a profit often requires conduct that is more complicated than traditional 'physical' crimes of theft and fraud. This is an important observation, as it frames the modern cybercrime landscape in which cyber proxies and cyber criminals all operate in close proximity and often with similar tools and methods. General private cyber actors use similar (if not entirely identical) disruption techniques. Consequently, a mere change in nomenclature and sponsor can often differentiate a possible cyber proxy from a cyber criminal, largely because the tools, methods and generated effects are often the same between these actors. However, this does not mean that a subtle difference in motivation and thus potentially status as a state-affiliated actor is irrelevant. It is not. Indeed, it is this subtle difference that speaks very directly to the ways in which international law can attempt to define the character of cyber proxies, attribute their conduct, and manage and mitigate their effects. This brings us to the enduring but misplaced attraction to the privateering analogy.

III. The Privateering Analogy

Considerations of piracy and privateering give rise to images of European colonial expansion, the Caribbean and the golden age of piracy from the mid-16th to late-17th century; however, as a legal concept, privateering first took shape in the Mediterranean, predominantly at the hands of the Barbary corsairs, and it is this concept that informs our modern understanding of a 'privateer'. The Barbary corsairs ran what was effectively a protection racket on the Mediterranean shipping lanes,[34] whereby states paid tribute in exchange for safe passage; however, the corsairs themselves were acting under the commission

[27] Maurer, "Cyber Proxies on a Tight Leash."
[28] Moe, "The Quasi Government."
[29] United Nations, "Developments in the Field of Information and Telecommunications;" Secretary-General and Security, "Group of Governmental Experts."
[30] United Nations, "Developments in the Field of Information and Telecommunications;" Secretary-General and Security, "Group of Governmental Experts;" Maurer, "Proxies and Cyberspace."
[31] Shoemaker, "Criminal Profiling and Cyber Criminal Investigations."
[32] Gonzalez, "Cases without Borders;" Nawang, "Combating Anonymous Offenders in the Cyberspace."
[33] Maurer, "Cyber Proxies: An Introduction."
[34] Kraska, Contemporary Maritime Piracy International Law, 22; Benton, A Search for Sovereignty, 125–26.

of the Barbary States and Ottoman Empire.[35] The Barbary States and their privateers were able to continue this conduct for a long period for two reasons. First, the European powers of the time used the Barbary States' protection racket as *de-facto* privateers in the Mediterranean theatre. They achieved this by paying the necessary tributes for the safe passage on their own ships and cargo while allowing the raiding to continue rather than engaging in a multilateral maritime action to suppress this raiding. The intention behind this conduct was the hope that by paying tribute, their own vessels would be safe from attack but the vessels of their competitors would be vulnerable.[36] Second, Gentili and Grotius argued that the term 'pirate' could not be legally attributed to a state, making their captures lawful acts of war.[37] The conduct of the Barbary States in the Mediterranean theatre was mirrored by the privateering conduct of the European states, first in the New World with Spanish colonial expansion and later in the Indian Ocean. The continued use of privateers throughout this entire era is reflective of the laissez-faire approach to mercantile trade at the time.[38]

The colonisation of the Americas began at the end of the 15th century with privateering following in its wake. The raiding of Spanish colonies and treasure ships by privateers mirrored the predatory nature of the Spanish conquests of the 'New World'.[39] Spain's predatory approach to expansion in the Americas is demonstrated by the following offer, made by the Governor of Cuba, to some adventurers who purportedly declined it:

> [We] purchased three ships … The third, a bark, [we] bought on credit from the Governor, Diego Velázquez, on the condition that all our soldiers should go in 3 vessels lying between Cuba and Honduras … And make war on the natives and load the vessel with Indians, as slaves, with which to pay him for his bark.[40]

This Spanish attitude towards the 'New World' set the tone for the 16th, 17th , and early 18th centuries in the Americas. Throughout the 16th century, privateers conducted maritime raids in the region (albeit very few operators were pirates) for which the primary target was Spanish treasure fleets.[41] This situation began to change at the end of the 16th century and through the early part of the 17th century and gave rise to the 'golden age of piracy' in the mid-17th century for two reasons. First, changes in Spanish convoy ships made the treasure fleets more difficult targets, as the raiders no longer possessed ships with greater speed and manoeuvrability.[42] Second, by the early part of the 17th century, the European states that were conducting raids on the Spanish had themselves established colonies in the Americas.[43] These colonies initially served as bases for the privateers, but as legitimate trade developed, the issuing of commissions diminished.

Even before Gentili, Grotius and Coke explored the law defining the crime of piracy and the existence of pirate states, the punishment for piracy was execution.[44] The possession of a valid commission was the difference between summary execution as a criminal and prisoner-of-war treatment as an agent of the state. This was clearly demonstrated in 1582 when a French raiding party was captured after five days of combat and could not provide evidence of a commission, resulting in the summary execution of almost 400 combatants.[45] The reasons for the lack of a commission are not clear, but it was obvious that the executed men were acting on behalf of the French Crown.[46]

With the decline of Spanish prominence in the Americas during the mid-17th century in favour of the French and English, and increased trade from the region, pirates rather than privateers conducted the majority of raiding.[47] States responded by selectively enforcing this raiding for several reasons. Perhaps the most overlooked reason is that, on the whole, the colonies in the 'New World' benefited from both the privateering and pirate activities.[48] Another reason was that the majority of colonial powers lacked the naval resources that would be required to engage in consistent and effective counter piracy activities.[49] It is for these reasons that the parallel with the modern-day conundrum of how to deal with hackers that take the form of cyber

[35] Little, Pirate Hunting, 205–7.

[36] Little, Pirate Hunting, 205–7.
[37] Grotius, *De Jure Belli Ac Pacis Libri Tres*, 631, 637; Rubin, The Law of Piracy, 20–21.
[38] Anderson, "Piracy and World History," 187.
[39] Kraska, Contemporary Maritime Piracy International Law, 27; Latimer, Buccaneers of the Caribbean, 3–4; Little, Pirate Hunting, 133.
[40] Taylor in Little, Pirate Hunting, 133–134.
[41] Kraska, Contemporary Maritime Piracy International Law, 28–30; Little, Pirate Hunting, 133–46.
[42] Little, Pirate Hunting, 144.
[43] Little, Pirate Hunting, 134.
[44] Queen Elizabeth I, "A Proclamation Agaynst the Maintenaunce of Pirates."
[45] Little, Pirate Hunting, 150.
[46] Little, Pirate Hunting, 150.
[47] Kraska, Contemporary Maritime Piracy International Law, 30; Lane, Blood and Silver, 201–2; Little, Pirate Hunting, 154.
[48] Benton, "Legal Spaces of Empire," 717–18.
[49] Little, Pirate Hunting, 171.

criminals is so seductive. The final, and possibly most significant reason, is that the European powers issued many privateering commissions during times of war to bolster their naval presence, only to revoke them once peace had been re-established. This led to a revolving door between privateering and piracy whereby privateers simply engaged in piracy during peace time[50]—today's privateer was tomorrow's pirate, and the following day's privateer.

From the mid-17th century until shortly after the enactment of the Treaties of Utrecht in 1713,[51] piracy and privateering was rife in the Caribbean theatre[52] with Port Royal and Tortuga serving as the most common havens.[53] Counter piracy in this time was reactionary and generally only engaged in when the privateer or pirate ceased to be useful or had become more of a hindrance than an asset.[54] Again, this occurred because of a lack of sufficient resources and assets to engage in consistent, effective, and sustained counter piracy operations. The Peace of Utrecht led to an upsurge in pirate activity in the Caribbean, as large numbers of privateers found themselves without sponsors, but simply continued to engage in the same conduct.[55] This in turn led to a surge of counter piracy activity by the British Royal Navy, resulting in mass hangings in the Atlantic ports throughout the 1720s[56] but not in a sustained manner sufficient to meaningfully end piracy.[57]

From this time onwards, piracy and privateering moved away from the Americas and into the Indian Ocean and East Indies. The reasons posited for this shift are varied, suggestions include that it was more profitable in the Caribbean to financially support legitimate trade than piratical activity,[58] which led to a lack of safe anchorages for pirates,[59] that the trade routes of the East Indies yielded greater prizes, and thus became the focal point,[60] and that the increase in prominence of the East India Company attracted raiders away from the Caribbean theatre.[61] Regardless, piracy in the Indian Ocean and East Indies appears to be very similar to that of the Americas.[62] The 19th century brought an end to privateering in policy circa 1801[63] and in law in 1856.[64]

The shift away from sanctioned privateering and high levels of tolerated piracy began with the US conflicts with the Barbary States that commenced in 1801. Weariness with the requirement to pay tribute to the various Barbary principalities as part of their protection racket over the Mediterranean and North African shipping lanes drove the resulting series of military actions against Tripoli and Derne.[65] Kraska argues that these engagements against the Barbary States by the US served to end the Barbary privateering predation in the Mediterranean as European powers began to follow America's lead on how to deal with the North African corsairs.[66] However, some arguments suggest that it was not until the French conquest and colonisation of Algeria in 1830 that the Barbary corsairs ceased to be a threat on the Mediterranean and North African sea routes.[67]

Concurrent with the Barbary Coast wars, the rise of professional navies throughout the Napoleonic wars at the beginning of the 19th century led to a decline in the number of commissions being issued for privateering,[68] which in turn led to a drop in autonomous pirates. By the end of the Napoleonic wars, the British Royal Navy had reached a high point of strength and

[50] Anderson, "Piracy and World History," 184; Benton, "Legal Spaces of Empire," 706–707; Kraska, Contemporary Maritime Piracy International Law, 28–30; Little, Pirate Hunting, 156; Puchala, "Of Pirates and Terrorists," 5.
[51] This treaty series served to end the Spanish Succession Wars. Sofka, "The Eighteenth Century International System," 150.
[52] Anderson, "Piracy and World History," 193; Kraska, Contemporary Maritime Piracy International Law, 30; Lane, Blood and Silver, 201; Puchala, "Of Pirates and Terrorists," 8.
[53] Kraska, Contemporary Maritime Piracy International Law, 30; Lane, Blood and Silver, 102, 105; Latimer, Buccaneers of the Caribbean, 135, 151.
[54] Little, Pirate Hunting, 153.
[55] Benton, "Legal Spaces of Empire," 719; Benton, A Search for Sovereignty, 149–50; Little, Pirate Hunting, 156.
[56] Benton, "Legal Spaces of Empire," 719.
[57] Benton, A Search for Sovereignty, 150.
[58] Anderson, "Piracy and World History," 185; Benton, "Legal Spaces of Empire," 720–21; Lane, Blood and Silver, 167–68; Paige, "The Impact and Effectiveness of UNCLOS," 117.
[59] Little, Pirate Hunting, 199.
[60] Kraska, Contemporary Maritime Piracy International Law, 31.
[61] Puchala, "Of Pirates and Terrorists," 8.
[62] Risso, "Cross-Cultural Perceptions of Piracy", 302–9.
[63] Rubin, The Law of Piracy, 216.
[64] Paris Declaration Respecting Maritime Law Art 1; Lemnitzer, Power, Law and the End of Privateering, 191.
[65] Kraska, Contemporary Maritime Piracy International Law, 25–26; Little, Pirate Hunting, 219–220. It is also arguable that this activity drove the formation of the US Navy and Marines.
[66] Kraska, Contemporary Maritime Piracy International Law, 26–27.
[67] Little, Pirate Hunting, 220; Puchala, "Of Pirates and Terrorists," 17–19.
[68] Kraska, Contemporary Maritime Piracy International Law, 31; Little, Pirate Hunting, 227.

ubiquity, but was no longer fighting a conflict, which created sufficient spare capacity to enforce *Pax Britannica*.[69] This led to the British Royal Navy engaging in unilateral antislavery and antipiracy actions globally in defence of international shipping and commerce.[70] During this period, the British treated international law more like guidelines than actual rules, as best demonstrated by their practice in counter piracy operations.[71] Further, this period in which British naval dominance ended piracy is significant because of the way in which it blurred British Imperial Law with international law,[72] something that has had an indelible impact on the formation and interpretation of modern international law.

The primary tactic used by the British Royal Navy was the blockading of pirate friendly ports,[73] as safe anchorage was key to successful piracy.[74] This tactic, combined with the manpower of the large professional navy, had the effect of ending piracy in the Americas and off the African coast by 1828[75] and globally by circa 1830[76] (although there were minor upsurges in the East Indies through the 1830s and 1840s).[77] The significance of this tactic in ending piracy, which also ended privateering, was that it was grounded in a material change in circumstances; that is, the growth of the British Royal Navy, in both size and professionalism, and the lack of any war in which to engage enabled it to attain global maritime dominance. Consequently, the British had the capacity to engage in the effective blanket suppression of piracy, the motivation to do so (to ensure that their large standing professional navy did not become listless and unruly), and no longer had the need to maintain access to fractious mercenaries of questionable value to bulk out their standing forces should another war eventuate.

It is in this history of the rise and fall of privateering as an accepted practice of states that we find our analogy to the modern conundrum of cyber hackers and the management of this criminal nuisance by states. What the history of piracy and privateering demonstrates is that where there is a crime with a relatively low entry threshold (joining a pirate crew was not exactly a difficult endeavour, nor was commandeering a vessel from a port)[78] and states lack the capacity to engage in any meaningful suppression mechanisms, states will instead manage the problem by attempting to direct it at their enemies. This observation, in the modern context, is once again reflected in commentary surrounding the use of prize law as an incentive in cyberspace and demonstrates that the idea of managing a criminal nuisance problem with re-direction is not new.[79] The primary purpose of the use of these original high-sea privateers was the control and effective taxing of crime that the states lacked capacity to suppress as demonstrated by the British's blanket suppression as soon as they had the capacity to do so. The secondary benefit was the way in which this control of the crime allowed states to bulk out their military assets in times of conflict. The general philosophy of managing piracy through privateering was essentially, "if you're going to have crime, it might as well be organized crime".[80]

Our previous discussion of cybercrime highlights the same problem we have historically observed in piracy; that is, widespread criminal activity that has a low entry threshold for the perpetrators, who operate in fora that are difficult to survey and difficult to police. The Internet operates in a similar manner to the high seas during European colonial expansion in that no state has the capacity to effectively suppress this widespread criminal activity. Our discussion of cybercrime and cyber-disruption has also highlighted activities that states are already engaging with these actors in the same way in which they engaged with privateers (i.e., by tolerating their criminal activity because they can aim that activity at their adversaries and competitors). The primary benefit of this approach is not the damage that is being done to a state's enemies by these raiders; rather, it is the fact that these raiders are not inflicting damage on the sponsoring state. Further, should these privateers engage in activity the state is no longer willing to tolerate (for political or practical reasons) their ties to the state make them easier to track down and punish than if they were truly independent criminal opportunists.[81] The question then becomes how the privateering relationship between states and hackers can be regulated in a modern legal framework. This is of crucial importance given that before the banning of privateering in 1856, the raiding activity that privateers engaged in was considered a valid use of force.

[69] Kraska, Contemporary Maritime Piracy International Law, 31; Puchala, "Of Pirates and Terrorists," 10–11.
[70] Anderson, "Piracy and World History," 189; Hunter, Policing the Seas, 73; Rubin, The Law of Piracy, 202–203.
[71] See generally, Serhassan (Pirates), 166 English Reports; The Madgellan Pirates, 164 English Reports.
[72] Paige, "Piracy and Universal Jurisdiction," 139; Rubin, The Law of Piracy, 201; Kraska, Contemporary Maritime Piracy International Law, 105.
[73] Hunter, Policing the Seas, 83, 85; Little, Pirate Hunting, 225.
[74] Puchala, "Of Pirates and Terrorists," 6–7.
[75] Hunter, Policing the Seas, 86.
[76] Kraska, Contemporary Maritime Piracy International Law, 31; Little, Pirate Hunting, 199.
[77] Hunter, Policing the Seas, 86.
[78] See, for example, *United States v. Tully et al.*, 28 F.Cas.
[79] Garrett, "Taming the Wild Wild Web."
[80] Pratchett, Men at Arms, 19.
[81] For historical evidence of how this was used to deal with pirates/privateers who had ceased to be sufficiently controllable see: *Rex v. Kidd*, 14 The Howell State Trials.

The purpose of the privateering analogy is not necessarily to make an attribution of state-sponsored cybercrime easier to identify.—When engaging in raiding, privateers still 'flew the black' and only produced their 'letters of marque' if they were captured. Similarly, hackers still engage in measures to obfuscate their identity but have the capacity to produce their state of affiliation should they be caught, thus attributing their activities to the state in question rather than themselves and escaping personal criminal liability. The benefit of our analogy is the way in which it incentivises cyber criminals to work with and stay engaged with their sponsor state, making them easier to track and capture should they go rogue because of the legal cover the term 'privateer' can provide. However, as the next section discusses, the strength of this analogy presents its own challenges within the current structure of international law and may only serve to further confuse an area overflowing with varying (and sometimes contradictory) definitions for the multitude of cyber actors currently operating around the world.

IV. The Challenges Inherent in the Analogy: Context and Alternative Concepts

A. Context

The first suite of challenges that confront the use of the admittedly quite attractive privateering analogy for cyber-proxy operations is that it does not really provide any benefit in terms of an operative legal assessment. This is because privateering is prohibited in international law. As far as international law is concerned, this is clearly the most important fact in favour of forgoing the 'privateer' analogy in the context of cyber proxies and cyber operations. Despite some states, such as the US, holding out against the *1856 Paris Declaration* for some time (it should be noted that privateering was used extensively by the Confederacy during the US Civil War),[82] the prohibition had become widely accepted by the early part of the 20th century.[83] The negotiation of the naval conventions at The Hague in 1907 routinely evidenced a broad consensus regarding the desirability of preventing any potential resurrection of lawful privateering. This desire to ensure no resurrection extends to 'privateer' behaviour and privateer status, and is unlikely to garner much support from modern states, whose histories detail the significant drawbacks of allowing privateers to operate on the high seas or elsewhere. Further, the definition of 'warship' subsequently settled in articles 1–4 of the *1907 Hague VII* (and now replicated in article 29 of the1982 LOSC) was in part designed specifically to safeguard against any such outcome.[84] These articles again emphasise the reluctance of states to allow any resurgence of pirates and privateers and should serve as a legal (and historical) reminder as to why these behaviours were so strongly outlawed.

The second suite of challenges that radically limits the potential utility of the privateering analogy for cyber-proxy operations carried out by private actors is that privateering was only ever available as a legal characterisation of conduct when its parent body of law (i.e., the Law of War) was applicable to a situation. Thus, privateering was only a 'thing' (in a legal sense) when a state of war existed between the relevant states, and the Law of War was in operation as the assessment paradigm. To put it another way, outside state-against-state war, privateering was still piracy. The only exception to this was the situation of recognised belligerency, when the rebel group in a civil war was formally recognised, for the purposes of the application of the Law of War only, as a belligerent party in what was then regarded as a state-against-state war for the purposes of the application of the Law of War. In such situations, before privateering was outlawed generally, both sides (i.e., the state and its adversary, the belligerent-status rebel group) could employ privateers.[85]

This raises a particularly significant issue for any use of the privateering analogy today, as the reorganisation of the Law of War into the LoAC in 1949 altered the rules around the *de jure* application of the applicable *jus in bello*; that is, the advent of the new concept of non-international armed conflict (NIAC) in common article (CA) 3 of the *1949 Geneva Conventions* and the re-classification of 'war' between states as international armed conflict (CA2)[86] created new thresholds for the application of the LoAC. This is significant because the post-1949 orthodoxy maintains that unless the specific CA2 or CA3 threshold is

[82] See, for example, Letter from the Duke of Newcastle to Governor Hincks (Windward Islands) and Relayed to Other Colonial Governors (November 30, 1861) (in response to a request for instructions regarding 'the course which should be taken by the British authorities in regard to privateers carrying the flag of the so-styled Confederate States... '); Lord McNair, "Legal Advice of Harding, Atherton, and Palmer to Earl Russell", 369–60; Bernard, A Historical Account of the Neutrality of Great Britain during the American Civil War, 173–86.

[83] This view is not universally acknowledged, and there are contra-indications even post 1907; for example, Brown Scott, The Hague Peace Conferences of 1899 and 1907: A Series of Lectures Delivered before the Johns Hopkins University in the Year 1908, 222–23; Schwartz, "U.S. Privateering is Legal" 146:4

[84] See Hague Conference Records 1907 at 805–807 (discussing the arguments from the Mexican delegation); Hague Conference Records 1907 at 749–752 (discussing the arguments from the Brazilian delegation).

[85] See generally, McLaughlin, Recognition of Belligerency.

[86] Being articles 2 and 3 common to the four *Geneva Conventions* of 1949.

crossed (even noting the quite low level of the CA2 threshold in particular),[87] then the LoAC as a body of law is irrelevant (standfast a few enduring obligations such as the CA1 duty to 'respect and ensure respect' for the *1949 Geneva Conventions* and the *1977 Additional Protocol I* article 36 obligation to conduct legal reviews of new means and methods of warfare). This threshold makes the applicability of the LoAC much more 'factual' and public, and marks a clear point of transition at which the LoAC becomes relevant. Thus, any discussion of the relevance of privateering is legally otiose unless and until the modern paradigmatically applicable parent body of the LoAC is itself applicable *de jure*.

Further, because the concept of privateering was only ever available in situations in which the Law of War was more broadly applicable (i.e., in conflicts between states or between a state and a recognised belligerent-status rebel group), if privateering were available as a characterisation today, it would only be available in the contexts characterised in the post-1949 LoAC as international armed conflicts. Thus, privateering is of little to no utility as a legal characterisation in the vast bulk of recent conflicts, being (as they are) non-international armed conflicts (a legal concept that did not exist before 1949). This observation is echoed in similar work, particularly that of Egloff, who discussed the applicability of the privateer analogy to the cyber realm.[88] Similarly, there is no longer a comparable dominant power that can control cyberspace to the same degree as Britain once did on the high seas during the mid-19th century.[89] Consequently, in the majority of situations in which private cyber actors are engaged in pursuing state-sanctioned outcomes, including 'active measures' (espionage, data theft, and other state-sanctioned cybercrime), the very label of 'privateer' (if it were even any longer a beneficial consequence-carrying characterisation) is paradigmatically inappropriate and legally irrelevant, as such situations are not governed by the LoAC applicable in international armed conflict (IAC).

B. Alternative Concepts

The second reason the privateer/cyber-proxy analogy is likely of little practical utility today is that the modern LoAC has generated a range of alternative characterisations and legal labels for the types of conduct (e.g., private but state-sanctioned) that cyber proxies engage in during armed conflict. Coupled with the oversaturation of definitions for cyber actors already, this contributes to the argument that the introduction of a cyber-privateer definition would likely further confuse an already complicated discussion. Given that there are existing terms under the established LoAC, the practicality of re-introducing a privateer analogy for the cyber realm is dubious. Of these terms, the key replacement concept or status is that of a 'civilian taking a direct part in hostilities'[90] as (quite thinly) encapsulated in the *1977 Additional Protocols*.[91] The debate concerning the indicia for the temporal envelope of and parameters around this concept (i.e., what acts represent direct participation in hostilities [DPHs] [and when] and what acts do not) continues, and this paper is not the place to rehash those debates.[92] However, two observations are relevant for the purposes of this paper.

The first observation is that regardless of the debates surrounding the indicia, temporal limitations, and act parameters, there is no debate as to the consequences that accrue for a person being categorised as a civilian taking a direct part in hostilities—they

[87] See, inter alia, the classic statement in the *1949 Geneva* Convention I Commentary of 1952 (by Pictet): 'It makes no difference how long the conflict lasts, or how much slaughter takes place. The respect due to human personality is not measured by the number of victims. Nor, incidentally, does the application of the Convention necessarily involve the intervention of cumbrous machinery. It all depends on circumstances. If there is only a single wounded person as a result of the conflict, the Convention will have been applied as soon as he has been collected and tended, the provisions of Article 12 observed in his case, and his identity notified to the Power on which he depends. All that can be done by anyone: it is merely a case of taking the trouble to save a human life!' 32–33 (https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=02A56E8C272389A9C12563CD0041FAB4).

[88] Egloff, "Cybersecurity and Non-State Actors."

[89] Egloff argues that despite the clear superiority of the US in other realms of power, in cyberspace, it is more equal to other powers, such as China and Russia, than in any other domain.

[90] Note that the concept of 'organised armed group' may also be applicable; however, for the purposes of focusing on the consequence for the individual cyber-proxy operator, we have concentrated on CDPH. Of course, it must be recalled that while the indicia of membership and temporal liability to attack for an OAG fighter differs from those relevant to CDPH, the consequence of the status (for the time in which it is applicable) is the same (i.e., liability to attack and no claim to combatant immunity if captured).

[91] Article 51(3) of the *Additional Protocol I* 1977 states, "1. The civilian population and individual civilians shall enjoy general protection against dangers arising from military operations. To give effect to this protection, the following rules, which are additional to other applicable rules of international law, shall be observed in all circumstances… 3. Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities." Article 13(3) of the *Additional Protocol II* 1977 states, "1. The civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations. To give effect to this protection, the following rules shall be observed in all circumstances. 2. The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited. 3. Civilians shall enjoy the protection afforded by this Part, unless and for such time as they take a direct part in hostilities."

[92] ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities; Watkin, "Opportunity Lost," 641; Schmitt, "Deconstructing Direct Participation in Hostilities," 697; Boothby, "And for Such Time As," 741.

lose their civilian immunity from being made the target of attack for as long as they are engaged in an act of DPH.[93] For example, a private cyber operator or actor whose conduct amounts to DPH becomes a targetable individual under the LoAC for the duration of that act of DPH. Further, upon capture by the adversary, that private cyber operator cannot claim the right to be treated as a prisoner of war (PoW) or seek the application of combatant immunity (i.e., that a PoW cannot be prosecuted for conduct that was in accordance with the LoAC). This liability assumes civilian DPH status and persists regardless of any claim to have been engaged in state-sanctioned operations (unless evidence can be provided of formal militia or similar status).[94]

The second observation is that this concept clearly can be and has been assessed as applicable to the conduct of private cyber operators engaged in state-sanctioned operations. In terms of international armed conflict, the clearest example is the Georgia-Russia war of 2008, during which private cyber proxies were variously directed and enabled by Russia in operations against Georgian public and private actors and objects.[95] Similarly, if the current conflict in Ukraine is considered an IAC between Ukraine and Russia, then individual private actors (such as hackers within the Internet Research Agency[96]) might become civilians engaged in acts of DPH. This is certainly the view of the *Tallinn Manual 2.0*[97] and is a conclusion that extends not just to IAC, but also to NIAC. In this second observation, there are two further subsidiary reasons as to why the concept of privateering in the modern LoAC terms is of minimal utility when thinking about cyber proxies.

First, privateering is only a valid legal concept in relation to what today would be classified as IAC or as a specific type of NIAC in which the LoAC applicable to IAC applies by virtue of article 1(4) of *Additional Protocol I* and—if recognition of belligerency persists as an operative legal doctrine—those NIACs in which this status has been recognised.[98] However, in the vast majority of NIACs, within which the status and consequences of civilian DPH continues to apply, the concept of privateering would be paradigmatically irrelevant.

Second, even in IAC situations where the analogy to privateering might be thought to retain some force, the trajectory of the law since 1949 is clearly to the effect that unless the private cyber operator is incorporated within the state's combatant forces in a manner indicated within and permissible under the *1949 Geneva Conventions* or *1977 Additional Protocol I*, then the conduct of that individual is DPH (leaving aside the organised armed group characterisation for the purposes of analysis). There is no scope in the concept of DPH for a modern equivalent of a 'letter of marque' that would immunise the private actor from criminal liability if captured.

V. Conclusion

There is no denying that the Internet has revolutionised the way in which people communicate across the globe. We are now able to connect with nearly anyone in any place, at anytime, anywhere around the world. However, the Internet has also revolutionised the way in which espionage and state disruption operations are organised and executed. The 2020 to 2021 period will go down in history as the years in which the COVID-19 outbreak changed the world, but this period will also be remembered for the massive increase in the number of reported cyber incidents between major world powers, cyber-specialist organisations and the everyday consumers who were caught in the middle.[99]

Understanding the nature and legal personality of cyber threats has become paramount to preventing, responding and, as discussed in this paper, constructing law for both current and future responses to cyberattacks. In this paper, we answered the question of whether our current understanding of cyber actors shows the utility of the 'privateer' analogy in cyber-disruption operations, given that some cyber actors have been 'permitted' to act in certain ways to satisfy the interests of a particular state while also securing profit or compensation for themselves. In answering this question, we have built upon established definitions of 'cyber mercenaries' and 'cyber proxies' who, more broadly, conduct or directly contribute to offensive or targeted cyberattacks while knowingly being enabled by a beneficiary state. Similar to cyber proxies and cyber mercenaries, the differentiation in our analogy lies in the already established definition of 'privateer' and what constitutes 'privateering' behaviour under established international law. We argued that the benefit of this analogy is in understanding the ways in which

[93] McLaughlin, "Organised Armed Groups and Direct Participation in Hostilities", Chapter 17.
[94] See 1949 *Geneva Convention III*, article 4(A); Additional Protocol I 1977, articles 43–44.
[95] Gotsiridze, "The Cyber Dimension of the 2008 Russia-Georgia War"; Shakarian, "The 2008 Russian Cyber-Campaign Against Georgia" 66-67; White, "Understanding Cyberwarfare," 5–10.
[96] Bugorkova, "Ukraine Conflict."
[97] Schmitt (ed), "Tallinn Manual 2.0," 428–432.
[98] For debates on the recognition of belligerency and the issues surrounding its application to the LoAC see McLaughlin, Recognition of Belligerency
[99] Purtill, "Why Online Hackers Are after COVID Vaccine Scientists;" Beatty, "The Increase in Ransomware Attacks during the COVID-19 Pandemic;" Marsh, "Aussies Lost More than $176 Million to Scams."

cyber criminals are incentivised to work and stay engaged with their sponsor state because of the legal cover it can provide them, while acknowledging that this approach also identifies the 'privateer' purpose (from the sponsoring state's perspective) of making these actors easier to track and capture should they go rogue.

Thus, while the term 'cyber privateer' represents a tempting analogy for the current environment of largely state-backed cyber operations, it is unfortunately not supported by current international law and nor is it ever likely to be. This is because privateering is prohibited by international law. In fact, it is prohibited so much so that international law expresses a consensus as to the desirability of preventing any potential resurrection of lawful privateering behaviour. Privateering itself was only available as an operative a legal term when the parent body of law was applicable, and given this parent body of law requires a state of war to exist, privateering behaviour, cyber or otherwise, would be characterised as criminal behaviour and would be dealt with under relevant sanctions. Indeed, it is unlikely that cyber-privateering behaviour or cyber privateers themselves will ever become a viable definitional subset of cyber actors given the current state of the international law and the fact that privateering itself is barely distinguishable from piracy except under very specific circumstances.

In determining the applicability of the 'privateering' label to current cyber-proxy behaviour and in determining its weak applicability, we also offered alternative concepts to this analogy. We argued that introducing yet another 'cyber' label to cyber actors has limited utility and may only serve to confuse a discussion already overpopulated with cyber-centric definitions. Further, the LoAC offers a range of alternative characterisations and labels for the types of conduct in which cyber proxies engage, the most relevant of which is that of a 'civilian taking a direct part in hostilities'. As discussed, this area of law is deeply developed and the consequences of such activities are well established in the LoAC whether they concern cyber activities or otherwise. It would thus appear that international law is already well equipped to deal with the possibility of cyber actors engaging in privateering-like activities and while they could not be described as privateers, such activities could be dealt with by reference to the alredy established and currently operative rules without the need to introduce a new cyber-actor category.

The benefit of our discussion is thus threefold. First, we provided a succinct summary of the current definitions of various cyber actors, specifically those involved in state-sponsored, -endorsed or -enabled cyber operations. Second, we provided a description of a cyber privateer and placed that description within a historically relevant understanding of privateers and privateering behaviour. Third and finally, we demonstrated why the cyber-privateer analogy is ineffective today. As a means of understanding relationships and motives, the privateer/cyber-proxy analogy may have some utility but as a means of operative legal characterisation, it is of no current value.

Acknowledgements

This work was supported by the Cyber Security Research Centre Limited, whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

Bibliography

ABC/Wires. "UK Accuses Russia of 'Despicable' Hacking Attacks on COVID-19 Researchers." *ABC News*, July 16, 2020. https://www.abc.net.au/news/2020-07-17/coronavirus-uk--accuses-russia-hacking-attacks-covid-19-research/12464958

Anderson, J. L. "Piracy and World History: An Economic Perspective on Maritime Predation." *Journal of World History* 6, no 2 (1995): 175–199.

Associated Press. "Hackers Found Guilty of Selling Computer Codes." *New Straits Times*, February 17, 1990.

Beatty, David R. and Michael Parent. "The Increase in Ransomware Attacks during the COVID-19 Pandemic May Lead to a New Internet." *The Conversation*, June 16, 2021. http://theconversation.com/the-increase-in-ransomware-attacks-during-the-covid-19-pandemic-may-lead-to-a-new-internet-162490

Benton, Lauren. "Legal Spaces of Empire: Piracy and the Origins of Ocean Regionalism." *Comparative Studies in Society and History* 47, no 4 (2005): 700–724. https://doi.org/10.1017/S0010417505000320

Benton, Lauren A. *A Search for Sovereignty: Law and Geography in European Empires, 1400–1900*. Cambridge: Cambridge University Press, 2010.

Bernard, Mountague. *A Historical Account of the Neutrality of Great Britain During the American Civil War*. London: Longmans, 1870.

Bugorkova Olga, "Ukraine Conflict: Inside Russia's 'Kremlin troll army'", *BBC*, 19 March, 2015, https://www.bbc.com/news/world-europe-31962644

Cruz, José Arimatéia da and Stephanie Pedron. "Cyber Mercenaries: A New Threat to National Security." *International Social Science Review (Online)* 96, no 2 (2020): 1–33.

Egloff, Florian J. "Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates." PhD Thesis, University of Oxford, 2018. https://ora.ox.ac.uk/objects/uuid:77eb9bad-ca00-48b3-abcf-d284c6d27571

Garrett, Nathaniel. "Taming the Wild Wild Web: Twenty-First Century Prize Law and Privateers as a Solution to Combating Cyber-Attacks." *University of Cincinnati Law Review* 81, no 2 (2012): 683–707.

Gonzalez, Jason P., Matthew A. S. Esworthy and Neal J. Gauger. "Cases without Borders: The Challenge of International Cybercrime Investigations." *Criminal Justice* 30, no 4 (2016): 15–18.

Gotsiridze, "The Cyber Dimension of the 2008 Russia-Georgia War", *Cyber Security Studies & Education Centre*, 6 August, 2021, https://www.linkedin.com/pulse/cyber-dimension-2008-russia-georgia-war-andro-gotsiridze

Grotius, Hugo. *De Jure Belli Ac Pacis Libri Tres*. Translated by Francis W. Kelsey, Arthur E. R. Boak, Henry A. Sanders, Jesse S. Reeve, and Herbert F. Wright. Washington, D.C.: Carnegie Institution of Washington, 1925.

Hunter, Mark C. *Policing the Seas: Anglo-American Relations and the Equatorial Atlantic, 1819–1865.* St. John's, Nfld: International Maritime Economic History Association, 2008.

International Committee of the Red Cross. *The Geneva Conventions of August 12, 1949*. Geneva: International Committee of the Red Cross, 1983.

International Committee of the Red Cross. *Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land*. The Hague, 18 October 1907

Kerr, Paul K., John Rollins, and Catherine A. Theohary. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* CRS Report No. R41524. Washington, D.C.: Congressional Research Service, 2010. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf

Kraska, James. *Contemporary Maritime Piracy International Law, Strategy, and Diplomacy at Sea*. Santa Barbara, Calif.: Praeger, 2011.

Lane, Kris E. *Blood and Silver: A History of Piracy in the Caribbean and Central America*. Oxford: Signal, 1999.

Latimer, Jon. *Buccaneers of the Caribbean: How Piracy Forged an Empire*. Cambridge, Mass: Harvard University Press, 2009.

Lemnitzer, Jan. *Power, Law and the End of Privateering*. Basingstoke: Palgrave Macmillan, 2014.

Little, Benerson. *Pirate Hunting the Fight against Pirates, Privateers, and Sea Raiders from Antiquity to the Present.* Washington, D.C.: Potomac Books, 2010.

Lord McNair, "Legal Advice of Harding, Atherton, and Palmer to Earl Russell", 5 October, 1861, *in 2 International Law Opinions* 369-60

Marsh, Stuart. "Aussies Lost More than $176 Million to Scams during the Height of the COVID-19 Pandemic." *9 News*, January 18, 2021. https://www.9news.com.au/national/australia-covid-news-aussies-lost-millions-to-scams-during-global-pandemic/10554bc5-9627-4644-8a97-deccc8ad2382

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018.

———. "Cyber Power: Geopolitics and Human Rights." In *Cyber Mercenaries: The State, Hackers, and Power*, 50–68. Cambridge: Cambridge University Press, 2018.

———. "Cyber Proxies: An Introduction." In *Cyber Mercenaries: The State, Hackers, and Power*, 3–28. Cambridge: Cambridge University Press, 2018. https://doi.org/10.1017/9781316422724.002

———. "Cyber Proxies and Their Implications for Liberal Democracies." *The Washington Quarterly* 41, no 2 (2018): 171–88.

———. "Cyber Proxies on a Tight Leash: The United States." In *Cyber Mercenaries: The State, Hackers, and Power*, 71–80. Cambridge: Cambridge University Press, 2018. https://doi.org/10.1017/9781316422724.005

———. "Proxies' and Cyberspace." *Journal of Conflict and Security Law* 21, no 3 (2016): 383–403. https://doi.org/10.1093/jcsl/krw015

Moe, Ronald C. and Kevin R. Kosar. *The Quasi Government: Hybrid Organizations with Both Government and Private Sector Legal Characteristics.* CRS Report No. RL30533. Washington, D.C.: Congressional Research Service, 2011. https://sgp.fas.org/crs/misc/RL30533.pdf

Morgan, Steve. "2019 Official Annual Cybercrime Report." Cyber Security Ventures, 2019.

Nakashima, Ellen and Devlin Barrett. "U.S. Accuses China of Sponsoring Criminal Hackers Targeting Coronavirus Vaccine Research." *Washington Post*, July 21, 2020. Accessed July 22, 2020. https://www.washingtonpost.com/national-security/us-china-covid-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0_story.html

Nawang, Nazli Iamail. "Combating Anonymous Offenders in the Cyberspace: An Overview of the Legal Approach in Malaysia." IEEEXplore, 2017. https://ieeexplore.ieee.org/document/7905255

Paige, Tamsin. "Piracy and Universal Jurisdiction." *Macquarie Law Journal* 12 (2013): 131–154.

Paige, Tamsin Phillipa. "The Impact and Effectiveness of UNCLOS on Counter-Piracy Operations." *Journal of Conflict and Security Law* 22, no 1 (2017): 97–123. https://doi.org/10.1093/jcsl/krv028

Paris Declaration Respecting Maritime Law (1856).

Pratchett, Terry. *Men at Arms: A Discworld Novel*. London: Corgi Books, 1994.

Puchala, Donald J. "Of Pirates and Terrorists: What Experience and History Teach." *Contemporary Security Policy* 26, no 1 (April 2005): 1–24. https://doi.org/10.1080/13523260500116059

Purtill, James. "Why Online Hackers Are After COVID Vaccine Scientists," *ABC News*, December 14, 2020. https://www.abc.net.au/news/science/2020-12-15/covid-19-coronavirus-the-hackers-targeting-vaccine-researchers/12974504

Queen Elizabeth I. "A Proclamation Agaynst the Maintenaunce of Pirates," August 3, 1569. https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/709/proclamation.pdf?sequence=1

Reuters. "2 W. Germans Get Suspended Terms as Computer Spies." *Los Angeles Times*, February 16, 1990, sec. L.A. Times Archives. http://articles.latimes.com/1990-02-16/news/mn-667_1_computer-wizards

Risso, Patricia. "Cross-Cultural Perceptions of Piracy: Maritime Violence in the Western Indian Ocean and Persian Gulf Region during a Long Eighteenth Century." *Journal of World History* 12, no 2 (2001): 293–319.

Rubin, Alfred P. *The Law of Piracy*. Newport, Rhode Island: Naval War College Press, 1988.

Schmitt, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Second edition. New York, NY: Cambridge University Press, 2017.

Schwartz, "U.S. Privateering is Legal", *US Naval Institute*, April, 2020, https://www.usni.org/magazines/proceedings/2020/april/us-privateering-legal

Scott, James Brown. *The Hague Peace Conferences of 1899 and 1907: A Series of Lectures Delivered before the Johns Hopkins University in the Year of 1908*. New York: Garland Pub, 1972.

Secretary-General, United Nations, and United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015. https://digitallibrary.un.org/record/799853

Serhassan (Pirates), 166 English Reports 788 (1845).

Shakarian, Paulo. 'The 2008 Russian Cyber Campaign Against Georgia'. Military Review 91, no 6 (2011): 63

Sheldon, Robert, and Joe McReynolds. *Civil Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias.* New York, NY: Oxford University Press, 2015.

Shoemaker, Daniel and Daniel B. Kennedy. "Criminal Profiling and Cyber Criminal Investigations." In *Crimes of the Internet*. Prentice Hall, 2009.

Singer, Peter Warren. *Corporate Warriors: The Rise of the Privatized Military Industry*. Updated ed. Ithaca, N.Y.: Ithaca, N.Y.: Cornell University Press, 2008.

Sofka, James R. "The Eighteenth Century International System: Parity or Primacy?" *Review of International Studies* 27 (2001): 147–63. https://doi.org/10.1017/S0260210501008063

The Madgellan Pirates, 164 English Reports 47 (The High Court of Admiralty 1853).

Thompson, Jon. "The Morris Worm." *Personal Computer World*, 2009.

United Nations. "Developments in the Field of Information and Telecommunications in the Context of International Security." *United Nations Disarmament Yearbook 2013: Part I*. United Nations, 2014. https://www.un-ilibrary.org/content/books/9789210566018s003-c048

United States v. Tully et al., 28 F.Cas. 226 (Circuit Court, D. Massachusetts 1812).

White, Sarah, "Understanding Cyberwarfare: Lessons from the Russia-Georgia war", *Modern War Institute*, 20 March, 2018, https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/

Primary Legal Material

Rex v. Kidd, 14 The Howell State Trials 147 (The Old Bailey 1701).