European Journal of International Security (2020), **5**, 233–254
doi:10.1017/eis.2020.6

RESEARCH ARTICLE

From defence to offence: The ethics of private cybersecurity

James Pattison*

University of Manchester
*Corresponding author. Email: james.pattison@manchester.ac.uk

(Received 16 July 2019; revised 17 February 2020; accepted 7 April 2020)

Abstract

The cyber realm is increasingly vital to national security, but much of cybersecurity is provided privately. Private firms provide a range of roles, from purely defensive operations to more controversial ones, such as active-cyber defense (ACD) and 'hacking back'. As with the outsourcing of traditional military and security services to private military and security companies (PMSCs), the reliance on private firms raises the ethical question of to what extent the private sector should be involved in providing security services. In this article, I consider this question. I argue that a moderately restrictive approach should be adopted, which holds that private firms can justifiably launch some cybersecurity services – defensive measures – but are not permitted to perform others – offensive measures.

Keywords: Cybersecurity; Just War Theory; Private Cyber Firms; Private Security and Military Companies; The Ethics of Cybersecurity

Introduction

The cyber realm is increasingly vital to national security, but much of cybersecurity is provided privately. Private cybersecurity firms perform a range of roles, from purely defensive operations to several more controversial ones, where firms engage in offensive operations to infiltrate, disrupt, and destroy the systems of actual or potential aggressors. As with the outsourcing of traditional military and security services to private military and security companies (PMSCs), the reliance on private firms (including PMSCs) to provide cybersecurity raises the ethical question of to what extent the private sector should be involved in providing security services.

This article considers this question. As we will see, there are various responses. On the one hand, it might seem that many of the ethical problems of relying on PMSCs to provide traditional security and military services, such as those experienced in Iraq and Afghanistan, also apply to the cybersecurity sector. Accordingly, private firms, including PMSCs, should be precluded from engaging in cybersecurity. I will call this the 'Highly Restrictive Approach': private firms should not be tasked with ensuring *any* cybersecurity services. On the other hand, it might seem that private firms are morally permitted to protect their own assets and so can hire PMSCs and other cybersecurity firms to assist them in doing so. I will call this the 'Permissive Approach': firms are allowed to engage in *all* cybersecurity operations. There is also a *via media* between these two positions, which I defend, at least at the non-ideal level. I call this the 'Moderately Restrictive Approach'. This holds that private firms can justifiably launch *some* cybersecurity services – *defensive* measures – but are not permitted to perform others – *offensive* measures.

The article will proceed as follows. Section 1 delineates in more detail private cybersecurity. Section 2 considers the ethical case for cybersecurity firms engaging in defensive operations, which are often seen as unproblematic. I argue that private defensive cybersecurity raises a series of ethical challenges but is currently permissible given the infeasibility of a public monopoly. This repudiates the Highly Restrictive Approach. I then consider (in section 2) whether it is morally permissible for private cybersecurity firms to engage in offensive operations, which would be mandated by the Permissive Approach. I argue that they should not be and, in doing so, defend the Moderately Restrictive Approach.

With regard to methodology, to clarify and evaluate the central issues for the ethics of private cybersecurity, and to develop its central claims, this article will use reflective equilibrium. This is the predominant meta-ethical method in contemporary analytic political philosophy and works by attempting to achieve coherence between our general moral principles and considered moral convictions about particular instances, in this case about private cybersecurity.[1] In doing so, the article will consider accounts of the ethics of private cyber operations that are idealised (that is, the Permissive Approach), and therefore more akin to what John Rawls calls 'ideal theory', as well as accounts of the ethics of private cybersecurity operations that are more 'non-ideal' (that is, the Moderately Restrictive Approach), and are very clearly part of what Rawls calls 'non-ideal theory'.[2] Whereas ideal theory focuses on theorising on the assumptions that there is compliance with the ideal moral principles and that there are favourable circumstances, non-ideal theory is relevant for when the world is messier, including when there is significant non-compliance and highly unfavourable circumstances.[3] By also considering more non-ideal approaches, this article is similar in approach to Jonathan Wolff's recent model of 'engaged' normative theorising and Joseph Carens's account of ideal and non-ideal theorising about migration.[4] It also accords with Chris Brown's call for normative International Relations (IR) to be more attuned to and engaged with empirical realities, rather than being overly idealised.[5]

In developing its account of the ethics of private cybersecurity, the article will draw upon literatures on the ethics of privatisation in general, the ethical challenges posed by PMSCs, and the ethics of cyber operations, and the normative considerations highlighted by these literatures. It will also, to some extent, draw on just war theory, but do so only *indirectly*. To explicate, one approach to the ethics of cyber operations would be to apply the standard list of just war criteria (for example, the six principles of *jus ad bellum*) to cyber operations. I do not do this since it is debatable whether, in general, cyber operations should be subject to the same ethical restrictions as regular warfare.[6] Much depends on the magnitude of the likely harms of cyber conflict (such as

[1] Sem De Maagt, 'Reflective equilibrium and moral objectivity', *Inquiry*, 60:5 (2017), pp. 443–65 (p. 463); Norman Daniels, 'Reflective equilibrium', in Edward Zalta (ed.), *Stanford Encyclopaedia of Philosophy* (winter 2016), available at: {plato.stanford.edu/entries/reflective-equilibrium/}; John Rawls, *A Theory of Justice* (rev. edn, Oxford: Oxford University Press, 1999).

[2] Rawls, *A Theory of Justice*.

[3] All of the ethics of cybersecurity might be viewed as part of non-ideal theory, to the extent that it is concerned with potential circumstances of noncompliance (for example, cyberattacks by hackers), which prompt the need for cybersecurity in the first place. Notwithstanding, there are, in general, different degrees of 'ideality' – how much a non-ideal theory reflects the lack of compliance and of favourable circumstances. More idealised accounts of the ethics of private cybersecurity largely assume compliance and favourable circumstances (apart from the need for cybersecurity in the first place), whereas more non-idealised accounts focus on significant noncompliance and unfavourable circumstances. See, further, James Pattison, 'The case for the non-ideal morality of war: Beyond revisionism versus traditionalism in just war theory', *Political Theory*, 46:2 (2018), pp. 242–68.

[4] Joseph Carens, 'Realistic and idealistic approaches to the ethics of migration', *International Migration Review*, 30:1 (1996), pp. 156–70; Jonathan Wolff, 'Method in philosophy and public policy: Applied philosophy versus engaged philosophy', in Annabelle Lever and Andrei Poama (eds), *The Routledge Handbook of Ethics and Public Policy* (London: Routledge, 2018), pp. 13–24.

[5] Chris Brown, 'International Relations and international politics theory', in Chris Brown and Robyn Eckersley (eds), *The Oxford Handbook of International Political Theory* (Oxford: Oxford University Press, 2018), pp. 48–59.

[6] See Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (eds), *Binary Bullets: The Ethics of Cyberwarfare* (New York: Oxford University Press, 2016); Randall R. Dipert, 'Distinctive ethical issues of cyberwarfare', in Allhoff, Henschke, and Strawser (eds), *Binary Bullets*, pp. 56–73; Luciano Floridi and Mariarosaria Taddeo (eds), *The Ethics of Information Warfare* (Dordrecht: Springer, 2014); Patrick Lin, Fritz Allhoff, and Keith Abney, 'Is warfare the right frame for the cyber

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

whether cyber attacks and responses to them might lead to several civilian deaths), but it seems unlikely that they will be as harmful as warfare.[7] Thus, the straightforward application of the just war theory framework, developed to govern war where the harms are typically very grave, seems questionable. Instead, the article will draw upon *underlying notions* that are central to 'revisionist' just war theory, especially the notions of liability, necessity, and proportionality.[8] Revisionist accounts of just war theory hold that the principles that should govern warfare are not *sui generis*, but instead are congruent with the rest of moral and political philosophy including, we can add here, the ethics of cyber operations. There is nothing special, on revisionist accounts, about the fact that these principles govern warfare; they also govern other domains. This article uses notions from revisionist accounts because they are some of the most philosophically developed concepts that we currently possess for thinking about ethical questions in international politics. Thus, to avoid misunderstanding, this article uses just war theory (and particularly revisionist just war theory) because it offers a sophisticated account of ethical questions in international politics, not because I claim that cyber operations are akin to war.

I focus on both the 'deeper' and 'contingent' ethical problems raised by private cybersecurity. In the context of private security, there are three types of more fundamental or 'deeper' normative objections. First, an objection may be deeper in the sense that it is *unique* to private actors. That is, it applies to private actors but not to public ones. Second, an objection may be deeper in the sense that it is *necessary* since it applies to all *private* actors (and perhaps to some public ones as well). Third, an objection may be deeper in the sense that it applies even *if firms were effectively regulated by a feasible system of national or international regulation*. In the security sector, it is difficult – and often impossible – to find unique or necessary features of private actors, given the range of private and public actors, and the fact that certain public actors can somewhat – and increasingly – resemble private ones.[9] I focus instead predominantly on the third sense of a deeper problem, that is, issues that would apply even if private cyber security firms were effectively regulated. I also consider the contingent problems raised by private cybersecurity.[10]

All told, the main contribution that this article provides is a systematic assessment of the ethics of private cybersecurity. As far as I am aware, this article offers the first detailed account of this issue. Although there has been a burgeoning literature on the ethics of cyberwarfare, this has been largely statist in focus, often drawing heavily on the state-centric frameworks of just war theory.[11]

debate?', in Floridi and Taddeo (eds), *The Ethics of Information Warfare*, pp. 39–59. See also Steven Lee, 'The ethics of cyberattack', in Floridi and Taddeo (eds), *The Ethics of Information Warfare*, pp. 105–122; Matt Sleat, 'Just cyber war? *Casus Belli*, information ethics, and the human perspective', *Review of International Studies*, 44:2 (2017), pp. 324–42.

[7] Dipert, 'Distinctive ethical issues of cyberwarfare'.

[8] The seminal account is Jeff McMahan, *Killing in War* (Oxford: Clarendon Press, 2009).

[9] See, more generally, John Gardner, 'The evil of privatisation', *Social Science Research Network* (2014), available at: {//papers.ssrn.com/sol3/papers.cfm?abstract_id=2460655}; James Pattison, *The Morality of Private War: The Challenge of Private Military and Security Companies* (Oxford: Oxford University Press, 2014); and Debra Satz, 'Some (largely) ignored problems with privatization', in Jack Knight and Melissa Schwartzberg (eds), *NOMOS LX: Privatization* (New York: New York University Press, 2019), pp. 9–29.

[10] It is also worth noting that the public/private distinction is used in myriad ways. It can be socially constructed by powerful actors and blur. See Jeff Weintraub, 'The theory and politics of the public/private distinction', in Jeff Weintraub and Krisham Kumar (eds), *Public and Private in Thought and Practice: Perspectives on the Grand Dichotomy* (Chicago: University of Chicago Press, 1997), pp. 1–42; Patricia Owens, 'Distinctions, distinctions: "Public" and "private" force?', *International Affairs*, 84:5 (2008), pp. 977–90; Deborah Avant and Virginia Haufler, 'Public-private interactions and practices of security', in Alexandra Gheciu and William C. Wohlforth (eds), *The Oxford Handbook of International Security* (Oxford: Oxford University Press, 2018), pp. 350–64. Indeed, it may be more judicious for work on private security to focus on commercial security actors rather than purely the public/private distinction. Notwithstanding, I will use 'public' and 'private' in this article in order to be congruent with the widespread use of these terms in the literature on cybersecurity and on PMSCs. See, further, Anna Leander, *Commercialising Security in Europe: Political Consequences for Peace Operations* (New York: Routledge, 2013).

[11] For instance, Christopher J. Eberle, 'Just war and cyberwar', *Journal of Military Ethics*, 21:1 (2013), pp. 54–67; Lee, 'The ethics of cyberattack'; Brian Orend, 'Fog in the fifth dimension: The ethics of cyber-war', in Floridi and Taddeo (eds), *The Ethics of Information Warfare*, pp. 3–24; Sleat, 'Just cyber war?'.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

As such, it has overlooked in large part the hugely significant – and indeed *central* – role of the private sector in cybersecurity. For instance, Matt Sleat argues that just cause for responding to a cyberattack comprises attacks on critical infrastructure. This immediately raises questions about the private sector, given that (as I discuss below) most of the critical infrastructure of major Western powers is in the hands of the private sector, and the private sector has been largely entrusted with defending it. Should the private sector therefore engage in defensive and even offensive measures to defend critical infrastructure? Similarly, although there is an extensive literature on the ethics of private firms performing traditional security functions (that is, PMSCs and mercenaries), this has not yet been extended to the cyber sector.[12] This is despite the huge and growing importance of cybersecurity globally. The conclusion of this article will draw out the broader significance of the analysis for the ethics of the privatisation of force and just war theory.

Two clarifications are necessary. First, I will adopt a broad definition of cybersecurity. I follow Myriam Dunn Cavelty in viewing it as a 'multifaceted set of technologies, processes and practices designed to protect networks, computers, programs, and data from attack, damage or unauthorized access, in accordance with the common information security goals: the protection of confidentiality, integrity and availability of information'.[13]

Second, I will draw on the ethical issues raised by PMSCs providing kinetic services to help inform the analysis. This is because there are certain similarities between the PMSC sector and private cybersecurity. According to Jesse McMurdo, private cybersecurity firms 'are the PMCs of cyberspace'.[14] As he notes, '[i]nstead of deploying armed guards and armored vehicles, [they] deploy sophisticated programs and capable cybersecurity specialists.'[15] More specifically, it seems appropriate to draw *some* insights from PMSCs providing kinetic services since both private cybersecurity firms and PMSCs are: (1) private firms offering (2) security services; (3) often operating across state borders; (4) sometimes in semi-governed or ungoverned spaces; and (5) sometimes with specialised needs of clients.[16] It is important here to highlight that PMSCs provide services beyond armed security protection, including outside of the war context, such as the maintenance of equipment, training, and logistics, in a seemingly similar manner to the variety of services offered by private cybersecurity firms (which help, for instance, to fix technical errors and to manage software updates). That said, we should be very cautious in drawing strong analogies between the ethics of private cybersecurity and the ethics of private military force. In general, the heavy reliance on analogies between the physical and cyber realms (for example, about deterrence) can be misleading, given the differences between the two realms.[17] Indeed, as we will see, there are significant differences between private cybersecurity and the private military and

[12] For instance, Deane-Peter Baker, *Just Warriors, Inc.*: *The Ethics of Privatized Force* (London: Continuum, 2011); William Feldman, *Privatizing War: A Moral Theory* (London: Routledge, 2016); Pattison, *The Morality of War*.

[13] Myriam Dunn Cavelty, 'Cyber-security and private actors', in Rita Abrahamsen and Anna Leander (eds), *Routledge Handbook of Private Security Studies* (London: Routledge, 2015), pp. 89–99 (p. 89). I define a cyber-attack as an attempt to harm or infiltrate another computer network. Sometimes a distinction is drawn between a cyberattack (said to be undertaken for political purposes) and cybercrime (undertaken for criminal purposes). Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, 'The law of cyber-attack', *California Law Review*, 100:4 (2012), pp. 817–85 (pp. 830–3). But this requires identifying the attacker and their goals, which can be very tricky given the notorious difficulties of attribution. It can also be misleading since attackers can have multiple and complex objectives. Also note that cyberattacks can be undertaken by both states and non-state actors and that there is not a sharp distinction between a cyberattack and cyberespionage (the latter is one form of cyberattack).

[14] Jesse Jacob McMurdo, 'Cybersecurity firms – cyber mercenaries?', *Homeland and National Security Law Review*, 4:1 (2016), pp. 35–78 (p. 67).

[15] Ibid., p. 68.

[16] Wyatt Hoffman and Steven Nyikos, 'Governing Private Sector Self-Help in Cyberspace: Analogies from the Physical World', Carnegie Endowment for International Peace, Working Paper (2018), p. 32.

[17] Mariarosaria Taddeo, 'On the risks of relying on analogies to understand cyber conflicts', *Mind & Machines*, 26 (2016), pp. 317–21.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

security sector, which leads to somewhat different ethical challenges, even if *some* insights for the ethics of private cybersecurity can be obtained by looking to the ethical issues raised by PMSCs.

1. Private cybersecurity explicated

The role of the private sector in cybersecurity is widely seen as necessary. In 2015, Barack Obama remarked that '[t]here's only one way to defend America from these cyber threats, and that is through government and industry working together.'[18] Likewise, the EU has emphasised the vital role played by the private sector in providing cybersecurity.[19] In its national cybersecurity strategy, the UK states that it 'will draw on its capabilities and those of industry to develop and apply active cyber defence measures to significantly enhance the levels of cybersecurity across UK networks'.[20]

Important to understanding cybersecurity is the distinction between *defensive* and *offensive* cybersecurity. In his seminal discussion, Robert Jervis notes that '[t]he essence of defense is keeping the other side out of your territory. A *purely* defensive weapon is one that can do this without being able to penetrate the enemy's land.'[21] Likewise, Johan Galtung argues that the offensive/ defensive distinction turns on whether the measure can be used abroad: 'If it can be used abroad, then it is offensive', but '[i]f it can only be used at home then the system is defensive.'[22] In similar vein, in the cyber realm, whether measures are defensive or offensive depends on their effects beyond the defender's own network.

To elaborate, defensive measures vary in how 'passive' or 'active' they are, depending on the activity beyond the defender's own network.[23] *Passive* measures are akin to what Jervis calls 'purely' defensive weapons, that is, with no activity beyond the defender's own network. They include firewalls, patch management procedures, antivirus software, and limits to administrative authority.[24] *Active* measures involve some activity beyond the defenders' own network but, importantly, lead to little or no disruption of this network. Such measures are therefore still defensive. They include 'honeypots', which attract intruders and log their behaviour, 'tarpits', which slow down malicious traffic to disincentivise attackers from connecting to the network, 'beaconing' to alert the owner of unauthorised entry attempts and to provide the victim with information about the IP addresses and network configuration of the attackers, and intelligence gathering on the Dark Net.[25]

'Active-cyber defence' (ACD) comprises measures that go beyond the defender's network. It includes several of these active defensive measures, which are not disruptive, as well as some

[18] Barack Obama, 'Remarks by the President at the Cybersecurity and Consumer Protection Summit', White House Archives (2015), available at: {obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/summit}.

[19] Kristoffer Kjærgaard Christensen and Karen Lund Petersen, 'Public-private partnerships on cyber security: A practice of loyalty', *International Affairs*, 93:6 (2017), pp. 1435–52 (p. 1438).

[20] UK Government, National Cyber Security Strategy (2016–21), p. 10, available at: {www.gov.uk/government/uploads/system/uploads/attachment_data/file/564268/national_cyber_security_strategy.pdf}.

[21] Robert Jervis, 'Cooperation under the security dilemma', *World Politics*, 30:2 (1978), pp. 167–214 (p. 203); emphasis added.

[22] Johan Galtung, 'Transarmament: From offensive to defensive defense', *Journal of Peace Research*, 21:2 (1984), pp. 127–39 (p. 128).

[23] I largely follow here the definitions provided by the Center for Cyber and Homeland Security, which offers a detailed and plausible account: 'Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats', Project Report 2016, George Washington University.

[24] Ibid., p. 9.

[25] Hoffman and Nyikos, 'Governing Private Sector Self-Help', p. 19; Center for Cyber and Homeland Security, 'Into the Gray Zone', pp. 10–11. Honeypots are sometimes viewed as active, depending on the degree of interaction with the attacker and whether they actively search out malicious servers. They also sometimes contain weaponised files that cause significant disruption once exfiltrated, although they may still technically be 'defensive', as the attacker is the one who transfers the infected file into their own network. Michael Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), p. 174.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

offensive measures that are disruptive or significantly intrusive. Offensive ACD measures include 'botnet takedowns' (the disabling of the systems of infected attackers), entering into an attacker's network to obtain information about them (such as capturing an image through their webcam), and the (admittedly more speculative) possibility of white hat ransomware (malware to encrypt files on third parties' systems that require them to return stolen information to regain access) and rescue missions to recover stolen information.[26] More offensive still – and beyond ACD – is hacking back. This involves the intention to disrupt or destroy the defender's network, rather than simply to defend against the attack or to retrieve stolen data.[27]

Thus, to recap, there are: (1) passive measures that are strictly limited to the defender's network; (2) defensive measures of ACD that do not disrupt the defenders' network; (3) offensive measures of ACD that do involve notable disruption or intrusion into the defender's network in order to redress the attack; and (4) hacking back.

A range of private actors are involved in cybersecurity. Private firms are both the *objects* and *agents* of cybersecurity. In other words, they both need protection and provide protection –and sometimes do both. In terms of being the *objects* of cybersecurity, firms have been subject to notable attacks, with several high-profile cyber incidents for firms such as Equifax, FedEx, Google, Maersk, and Sony.[28] Important here is that the private sector is now responsible for much of the maintenance of some states' critical infrastructure – it owns much of it – and so is a key object in need of protection.[29] Inadequate cybersecurity of critical infrastructure has become a major concern. In addition to affecting critical public services, inadequate private cybersecurity also affects national defence and internal security. This is in part because civilian infrastructure is used to transmit military data, such as cables and satellites.[30] It is also due to the heavy reliance on defence firms by several states, most notably in the US. As Amitai Etzioni notes, 'General Dynamics, Boeing, Lockheed Martin, Raytheon, and Northrop Grumman – the United States' leading defense contractors – have all fallen victim to hackers'.[31]

In terms of being the *agents* of security, several private firms provide *in-house* cybersecurity to protect themselves. There are also cybersecurity firms such as Novetta, Cloudfare, Crowdstrike, Trend Micro, and FireEye that are *hired* by other firms, governments, and other actors to provide cybersecurity. For instance, in the run up to the 2019 UK election, the protection offered by the US-based firm Cloudfare helped the British Labour Party to survive a Distributed

[26] Center for Cyber and Homeland Security, 'Into the Gray Zone', pp. 10–12; Wyatt Hoffman and Ariel Levite, 'Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?' Carnegie Endowment of International Peace (2017), p. 8.

[27] Center for Cyber and Homeland Security, 'Into the Gray Zone', p. 12. There are differences in how the precise boundaries of ACD and hacking back are drawn in the various accounts of them. Indeed, some offensive ACD measures (for example, botnet takedowns) might be deemed to be hacking back if the intent is to disrupt. Not much turns on this definitional issue here since I will argue that both offensive ACD and hacking back should be precluded. Some use ACD rather differently; for instance, the UK uses ACD to denote purely defensive measures rather than offensive ones. See Tim Stevens, Kevin O'Brien, Richard Overill, Benedict Wilkinson, Tomass Pildegovičs, and Steve Hill, 'UK Active Cyber Defence: A Public Good for the Private Sector', Cyber Security Research Group, The Policy Institute, King's College London (King's College London, 2019).

[28] For instance, NotPetya cost Maersk and FedEx $300 million each, with a total cost estimated at US $10 billion. Erica D. Borghard and Shawn W. Lonergan, 'Cyber operations as imperfect tools of escalation', *Strategic Studies Quarterly*, 13:3 (2019), pp. 122–45 (pp. 132–3).

[29] The notion of critical infrastructure has expanded, to include agricultural food systems, energy systems, health facilities, banking and finance, commercial and shipping services, with it being estimated that 85 per cent of the critical infrastructure in most Western states is in private hands. Oldrich Bures and Helena Carrapico, 'Private security beyond private military and security companies: Exploring diversity within private-public collaborations and its consequences for security governance', in Oldrich Bures and Helena Carrapico (eds), *Security Privatisation: How Non-Security-Related Private Businesses Shape Security Governance* (Dordrecht: Springer, 2018), pp. 1–19 (p. 4).

[30] McMurdo, 'Cybersecurity firms', p. 42.

[31] Amitai Etzioni, 'The private sector: A reluctant partner in cyber security', *Georgetown Journal of International Affairs*, International Engagement on Cyber IV (2014), pp. 69–78 (p. 75).

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

Denial-of-Service (DDoS) attack.[32] Some firms are 'pure plays', which focus on a single market – often government clients – and get most of their revenue from that.[33] There are other cybersecurity firms that have a broader customer base beyond government agencies. These include many smaller firms and start-ups that have emerged, with some becoming established contractors and others being bought by larger firms (for example, Raytheon purchased Blackbird Technologies Inc. for $420 million in 2014).[34] An example of a smaller firm is Hacking Team, which allegedly sold offensive cyber tools to countries worldwide.[35] Other firms, such as HackerOne, act as brokers connecting 'white hat' hackers (that is, those who find vulnerabilities and sell them to the developers) to venders.[36] Other firms, such as ReVuln and Zerodium (formed by the founders of Vupen), and defence firms, such as Lockheed Martin and Raytheon, connect 'grey hat' hackers (that is, those who find vulnerabilities and sell them to other parties, such as governments, who are judged to be legitimate purchasers) to vendors.[37] The most notorious vulnerabilities are 'zero-day exploits', which are unknown to the vendor and other parties using the software, and are sold to (or shared with) various governments.[38] Moreover, private firms that provide military and security services – traditional PMSCs – now also provide cybersecurity. PMSCs have either expanded into cybersecurity or have purchased firms that do so. For instance, in 2016, G4S added a 'Cyber Consulting and Security Operation Centre' to its portfolio.

The range and number of private cybersecurity actors has expanded as states have been unwilling and unable to protect fully citizens and firms against cyberattacks. In the UK, the chances of being subject to a victim of a cybercrime or cyber fraud are reportedly greater than for any other offence.[39] The US has seen the development of a 'Home Depot' model, whereby private companies are responsible for the defence of their own network – including that of critical infrastructure – with the government responsible for prosecuting cybercrime, applying diplomatic pressure, sanctions, providing cyber threat information to companies, and defending the US from significant events.[40] Within this model, private actors are increasingly partnering passive cyber practices with more assertive forms of ACD.[41]

Why have private firms selling cybersecurity become so important? There are two key elements to the emergence of the cybersecurity market. First, several states, especially the UK and US, have internalised much of the neoliberal logic, whereby governments should rely on private actors, given supposed market efficiencies and the encouragement of free enterprise.[42] By the time that cybersecurity services became highly important, the free market philosophy stemming from the Reagan and Thatcher eras had been entrenched for several years. It seems almost natural in these states that private actors would be given a key role in providing security services, given that they have large roles in providing traditional military and security services, as well as a host of other public services.

[32] 'General Election 2019: "Cyber-attack" on Labour Party digital platforms', *BBC News* (12 November 2012).

[33] Traditional pure-play defence contractors such as ManTech, CACI, BAE systems, and Northrop Grumman have been increasing their activities to include cyber. See Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018), p. 73.

[34] Ibid., p. 74.

[35] Ibid., pp. 18–19.

[36] Nathan Alexander Sales, 'Privatizing cybersecurity', *UCLA Law Review*, 65 (2018), pp. 620–89 (p. 635).

[37] Ibid., pp. 641–2.

[38] McMurdo, 'Cybersecurity firms', pp. 43–4.

[39] Stevens et al., 'UK Active Cyber Defence', p. 5.

[40] Kristen E. Eichensehr, 'Public-private cybersecurity', *Texas Law Review*, 95:3 (2017), pp. 467–538 (p. 496).

[41] Hoffman and Levite, 'Private Sector Cyber Defense', p. 1.

[42] Elke Krahmann, *States, Citizens and the Privatisation of Security* (Cambridge: Cambridge University Press, 2010). Note here that, in large part, the article focuses mainly on the North American and European contexts of cybersecurity, although it will consider some issues for the Global South and for states in general.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

Second, the development of the cyber domain has happened to a considerable extent in private hands. Unlike traditional military and security services, which have been outsourced, cybersecurity was not in public hands in the first place. To be sure, some states now possess some of the largest and most sophisticated cybersecurity capabilities. However, private firms have been integral to the development of the cybersecurity domain, rather than states significantly outsourcing cybersecurity. The Internet was largely developed by private firms, and private firms have, in the Internet's relatively brief history, been central to much of cybersecurity. This differs from other areas of privatisation, including private security.[43] Thus, cybersecurity, unlike traditional military and security services, is not being privatised since it was private to start with. As we will see in the next section, this has important normative implications.

2. Private defensive cybersecurity

Let us consider the case for private defensive cybersecurity, that is, passive measures and defensive forms of ACD. Although I will argue that private defensive cybersecurity is somewhat morally problematic, and so the Highly Restrictive Approach has some initial plausibility, I will also argue that these problems are largely intractable, and so we are left with the Moderately Restrictive or the Permissive Approaches.

It will help to start by considering the prima facie case for defensive cybersecurity, which I think has some intuitive force and explains why, in the end, private defensive cybersecurity is permissible. This case runs as follows. The right to self-defence is a fundamental human right. If, for instance, an individual is facing an attack from a mugger, they can use (proportionate and necessary) measures to defend themselves and their property. They can also obtain assistance from someone to help defend them. Likewise, it seems that individuals can use (proportionate and necessary) defensive measures to protect themselves and their legitimate interests from cyberattack. They can, it seems, engage in passive measures such as authentication, encryption, firewalls, honeypots that set up a decoy to expose attackers, and tarpits that slow down attackers to ensure that their property – and sometimes livelihood – is protected, and hire others to do so. Private firms can also, it seems, use (proportionate and necessary) measures to defend their legitimate interests. Like individuals, they can, for instance, use authentication, encryption, firewalls, and set up honeypots and tarpits, and hire others to assist them with this.

Important here is that if the state is not protecting its citizens or their interests (potentially invested in firms), the state is not fulfilling the terms of the social contract, whereby citizens accept the authority of the state in return for its protection.[44] It follows that individuals (and firms) are permitted to protect their own interests and to use private firms to help them do this.[45] For instance, if a weak state fails to protect citizens in a particular town, meaning that they are subject to violent attack from rebel groups, the townsfolk could hire PMSCs to assist with their protection. Likewise, if a state fails to ensure cybersecurity, citizens and firms can hire private actors to assist with their defence, subject to the constraints of proportionality and necessity. Paul Rosenzweig puts this most forcibly, 'in the absence of an effective system of cybersecurity provided by the U.S. government, it is, in some sense, almost immoral to prohibit private sector actors from taking steps to protect themselves'.[46]

This prima facie, idealised case has some force, but it does not establish by itself that private defensive cybersecurity is permissible. The issue is that, in practice, private defensive

[43] Eichensehr, 'Public-private cybersecurity', p. 471; Dunn Cavelty, 'Cyber-security and private actors'.

[44] I assume here that the social contract applies to all major security threats, including those in the cybersphere.

[45] Lin, Allhoff, and Abney, 'Is warfare the right frame', p. 50; Patrick Lin, 'Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies', Policy Paper on Cyber Security (2016), pp. 8, 10–11, available at: {ethics.calpoly.edu/hackingback.pdf}.

[46] Paul Rosenzweig, 'International law and private actor active cyber defensive measures', *Stanford Journal of International Law*, 50 (2014), pp. 103–18 (p. 117).

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

cybersecurity faces some negative externalities, even if seemingly innocuous, particularly in relation to its effects on (1) inequality and (2) democratic accountability.[47] I will consider these in turn, before arguing that, notwithstanding these problems, private defensive cybersecurity is permissible (and required) because of a lack of feasible alternatives.

Inequality

The first set of ethical issues concerns the issue of inequality in access to cybersecurity provision. One concern in this context is *exclusion*, where those who cannot afford to purchase security are left unprotected. With PMSCs, the reliance on the market to provide security services creates what Anna Leander calls a 'Swiss Cheese' model, where there are significant lacunae in protection.[48] The poor and disadvantaged lack protection because they cannot afford it. Similarly, in the cyber context, those who cannot afford to purchase cybersecurity are vulnerable to cyberattack. As Kristoffer Kjærgaard Christensen and Tobias Liebetrau argue about cybersecurity, 'if we accept the centrality of private companies as providers of security, it is also a matter of who has the economic resources to retain the services of the "right" companies'.[49] This is manifest in the Global South, where the public and private sectors lack resources and so 'more easily become infected with viruses and malware'.[50] For instance, some banks in the Global South lack the resources to invest in cybersecurity. There have been notable thefts from the Banco del Austro in Ecuador, and from banks in the Philippines and in Vietnam.[51] Likewise, developing countries lack the resources to buy the latest software and so are more vulnerable to attacks such as the WannaCry ransomware, which targeted a vulnerability in the Microsoft operating system that was patched months earlier for supported versions.[52]

A second, related issue is *deflection*. When individuals or private firms purchase even private defensive cybersecurity, it can lead to insecurity being deflected onto those who cannot afford to top up their protection, meaning that they do not have a sufficient level of security. This is apparent in the physical world in gated communities, which can result in an increase in crime in surrounding areas.[53] In the cyber realm, the purchase of robust private defence systems can mean that attackers instead target those who cannot afford such systems. Indeed, systems that are related to poorly funded public infrastructure have often been the target of cyberattacks.[54]

Third, by introducing the market logic into cybersecurity, influential agents may no longer be willing to support a general, basic level of public protection because they do not require it since they can purchase expensive private protection. This can reduce political support for the public spending necessary to fund a basic level of protection and ultimately lower levels of security for those who rely upon the service. Analogously, when parents send their children to private

[47] These are documented extensively in the literature on the ethical problems posed by PMSCs. See Pattison, *The Morality of Private War*, and, more generally, Knight and Schwartzberg (eds), *NOMOS LX: Privatization*; especially, Satz, 'Some (largely) ignored problems'. Even if some of these effects are not apparent yet for private cybersecurity, they might still materialise. As Kristen Eichensehr argues, although the private cyber sector may have started out 'publicised' to the extent that it currently plays a helpful role in protecting public values, 'the private sector is a fickle guardian of public values, and business imperatives will not always align with public values': Eichensehr, 'Public-private cybersecurity', pp. 537–8.

[48] Anna Leander, 'The market for force and public security: The destabilizing consequences of private military companies', *Journal of Peace Research*, 42:5 (2005), pp. 605–22.

[49] Kristoffer Kjærgaard Christensen and Tobias Liebetrau, 'A new role for "the public"? Exploring cyber security controversies in the case of WannaCry', *Intelligence and National Security*, 34:3 (2019), pp. 395–408 (p. 404).

[50] Niels Nagelhus Schia, 'The cyber frontier and digital pitfalls in the Global South', *Third World Quarterly*, 39:5 (2018), pp. 821–37 (p. 826).

[51] Ibid., p. 829.

[52] Ibid., pp. 831–2.

[53] Rutger Claassen, 'The marketization of security services', *Public Reason*, 3:2 (2011), pp. 124–45 (p. 143).

[54] Camilla Turner, 'Cyber attacks are one of the biggest threats that schools face, experts warn', *The Telegraph* (17 March 2018).

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

schools, this can lead to calls for decreases in the spending on state schools.[55] In the cyber realm, in the US there has been significant lobbying by various interests (some of which are relatively well protected) to oppose stronger legislation on private cybersecurity that would help to ensure adequate protection for all.[56] This can significantly augment the problem of exclusion.

Democratic accountability

A second set of issues concerns the lack of democratic control over private, defensive cybersecurity. Democratic oversight has been one of the main challenges with PMSCs, given the secretive nature of the industry, the lack of understanding of it by the public and legislature, and the absence of data, such as money spent on contracts and the details of the contracts.[57] This has meant that it has been much harder for the media, public, and legislature to hold the executive to account. In a somewhat similar vein, democratically elected representatives and the public have little understanding of cybersecurity, and, even when they do, the transnational, complex, fragmented, and, to some degree, opaque nature of the cybersecurity industry renders democratic oversight tricky.[58] Moreover, private cybersecurity extends beyond traditional lines of democratic accountability – that is, the state – which is the main locus of democratic rights.[59] This can render it difficult to hold cybersecurity actors to account, including when they are engaged in defensive measures. For instance, the response to the WannaCry attack involved a myriad of public and private actors, such as the NSA and Microsoft, extending beyond traditional lines of democratic accountability.[60]

Second, PMSCs have become seen as experts in assessing security needs and potential solutions. As Leander argues, they influence how we understand security threats, possessing 'epistemic power', that is, the power to affect the meaning of discourses.[61] They often favour a military and technical view of security, thereby marginalising non-military, more political approaches to security and non-military solutions to complex political problems. In the cyber realm, private cyber firms (even when performing only defensive roles) are seen as experts, playing central roles in the attribution of cyberattacks and constructing the broader understandings about cybersecurity and the appropriate responses.[62] Compared to state actors, they focus on different objects – their continued operations as a firm – and on technical (and sometimes exclusionary) understandings of expertise.[63] For instance, in the development of the EU's Network and Information Security (NIS) programme, private cyber actors have shaped the regulatory standards, as the private sector is seen as holding significant expertise and efficiency.[64] In his Presidential Address to the RSA Conference 2017, Brad Smith, President of Microsoft, claimed

[55] Satz, 'Some (largely) ignored problems'; Michael J. Trebilcock, Ron Daniels, and Malcolm Thorburn, 'Government by voucher', *Boston University Law Review*, 80:1 (2000), pp. 205–32 (p. 224).

[56] Etzioni, 'The private sector'.

[57] Deborah Avant and Lee Sigelman, 'Private security and democracy: Lessons from the US in Iraq', *Security Studies*, 19:2 (2010), pp. 230–65 (p. 245); Krahmann, *States, Citizens and the Privatisation of Security*, p. 249; Sarah Percy, *Regulating the Private Security Industry,* Adelphi Paper (New York: Routledge, 2006), p. 21.

[58] Myriam Dunn Cavelty and Andreas Wenger, 'Cyber security meets security politics: Complex technology, fragmented politics, and networked science', *Contemporary Security Policy*, 41:1 (2020), pp. 5–32 (p. 19); Irving Lachow, 'The private sector role in offensive cyber operations: Benefits, issues and challenges', *Social Science Research Network* (2016), p. 12, available at: {http://dx.doi.org/10.2139/ssrn.2836201}; Maurer, *Cyber Mercenaries*, p. 80.

[59] Christensen and Liebetrau, 'A new role for "the public"?', p. 405.

[60] Ibid.

[61] Anna Leander, 'The power to construct international security: On the significance of private military companies', *Millennium*, 33:1 (2005), pp. 803–26.

[62] Eichensehr, 'Public-private cybersecurity'.

[63] Christensen and Petersen, 'Public-private partnerships'.

[64] Benjamin Farrand and Helena Carrapico, 'Blurring public and private: Cybersecurity in the age of regulatory capitalism'; Bures and Carrapico (eds), *Security Privatisation*, pp. 197–216.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

that, 'regardless of the government' that asks for its assistance in using offensive measures against its customers, it will not engage in these measures.[65] Although the reluctance to use offensive cyber measures should be welcomed (as I argue below), the point here is that Microsoft plays a leading role in determining which measures a government can and cannot use. Thus, private firms are now central security actors that have significant epistemic power in the construction of cyber threats, potential responses, and the role of various actors.[66] The underlying normative concern, then, is that largely unaccountable private actors influence the cybersecurity agenda (including for defensive measures), rather than public actors who are accountable to the demos.

Third, private firms engaged in defensive cybersecurity measures may not be subject to even basic forms of democratic control. Many of the current public-private cybersecurity relationships differ from those traditionally provided by PMSCs in that they are informal rather than contractual. Private actors provide or hire cybersecurity alongside an informal, de facto partnership with the state, not based on contacts but rather comprised of looser expectations.[67] This can also suit governments since they do not need to pay for cybersecurity and it allows them deniability, which can weaken transparency.[68] Yet, without a contractual relationship, the state lacks control over private cybersecurity firms, which is a particular issue when its objectives differ, even more so than with traditional PMSCs (which also face contractual issues).[69] For instance, the UK's National Cybersecurity Centre is unclear what to do about private firms that fail to implement sufficient cybersecurity.[70]

The problems of a public monopoly on defensive cybersecurity

How should we resolve these problems? On the Highly Restrictive Approach, there should be a public monopoly on defensive cybersecurity to avoid these issues. This follows the logic of the argument for a monopoly on kinetic defensive measures, which might help to ensure equality and democratic accountability.[71] A monopoly on kinetic defensive measures would include armed guards and protective services, as well as more seemingly more mundane measures such as alarm systems, fencing, and entry systems, to ensure that all are equally protected (and some are not more vulnerable than others). Similarly, a public monopoly on defensive cybersecurity could, in theory, first, increase, and even ensure, equality. The state could ensure the same level of cybersecurity for everyone and preclude individuals from hiring the services of private cybersecurity firms to prevent significant inequalities in cybersecurity developing.[72] Second, a

[65] Brad Smith, 'Transcript of Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention', San Francisco, 14 February 2017, p. 13.

[66] On the latter point (that private cybersecurity firms construct the roles of various actors) Smith also asserts that 'we are the world's first responders. Instead of nation-state attacks being met by responses from other nation-states, they are being met by us': Ibid., p. 4.

[67] Eichensehr, 'Public-private cybersecurity'.

[68] Ibid., p. 510. Many of the relationships are framed in terms of 'public-private partnerships', but how firms view this relationship is quite different to how governments do so. In short, both eschew responsibility for cybersecurity and assume that it is the responsibility of the other. Madeline Carr, 'Public-private partnerships in national cyber-security strategies', *International Affairs*, 92:1 (2016), pp. 43–62.

[69] Eichensehr, 'Public-private cybersecurity'. On this issue for PMSCs, see Lindsay P. Cohn, 'It wasn't in my contract: Security privatization and civilian control', *Armed Forces & Society*, 37:3 (2011), pp. 381–98.

[70] Stevens et al., 'UK Active Cyber Defence', p. 20. The undermining of democratic accountability is a deeper problem with private cybersecurity, given that it could not be redressed by a feasible system of regulation since firms can simply choose not to provide their services, thereby rendering it difficult to ensure that the dictates of the democratic polity are realised. Pattison, *The Morality of Private War*, pp. 205–32.

[71] Ibid.; Herbert Wulf, 'The future of the public monopoly of force', in Alyson Bailes, Ulrich Schneckener, and Herbert Wulf, 'Revisiting the State Monopoly on the Legitimate Use of Force', Policy Paper No. 24 (Geneva: Geneva Centre for the Democratic Control of Armed Forces, 2007), pp. 19–26.

[72] This provides a deeper reason in favour of the public defensive cybersecurity since even if there were an effective system of regulation of private cybersecurity, it could not force unwilling private actors to protect those who cannot afford protection

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

public monopoly on defensive cybersecurity could increase democratic accountability by having public agents in charge of who provides cybersecurity, with clear lines of accountability to the demos.

However, although a public monopoly on force *might* be desirable with kinetic force (I leave this open here), the case is weaker for public defensive cybersecurity. There are four potential problems with a public monopoly on defensive cybersecurity.

First, it is unfeasible. States are unlikely to have the technical expertise or capacity to be able to defend fully against cyber threats. The private sector is vital to much of cybersecurity. Private firms have been integral to the development of the cyber world and have far greater capacity to defend their products. Moreover, the centrality of private actors is likely to increase further still. This is with the advancement of the 'Internet of Things' and artificial intelligence (AI), which are primarily developed by global technology firms and the private sector, and are likely to result in state actors becoming more dependent on private actors further still.[73] To overcome the dependence on private actors would require huge public spending since, as it stands, the resources, capabilities, and expertise of private firms exceed those of many states. For instance, JP Morgan Chase spends more on cybersecurity than is within the budget of the US Cyber Command.[74] Such spending may also be undesirable, if there are limited state resources and these could be better spent elsewhere (for example, on ensuring the provision of education, health, and social care services). A public monopoly on defensive cybersecurity would also require a dramatic expansion of state control beyond national boundaries, given that cyber firms have systems and data across numerous states.[75] This would be likely to raise further normative challenges, such as the significant intrusion into private property (such as source code) across national boundaries.[76] To be sure, this problem should not be overstated; it largely concerns when the public monopoly would involve the state providing cybersecurity *itself*. But on another model of the public monopoly, there would be scope for private actors to be the providers of cybersecurity, paid for by the state – the state would have a monopoly over only the hiring of cybersecurity services within its borders. Thus, this objection applies in greater force only to *some* forms of a monopoly on defensive cybersecurity.

Second, there is a moral hazard problem. If the government provides a monopoly on defensive cybersecurity, developers will have fewer incentives to pay for extensive testing to detect potential vulnerabilities.[77] The upshot would be that poorly tested – and highly vulnerable – products may predominate, and, as a result, much more extensive cybersecurity is necessary, or that the state has to pay for testing. This is likely to significantly increase the resources required for effective cybersecurity, which is a challenge in the face of limited government budgets hamstrung by austerity and pressure to spend public money on the most pressing areas. Like the first issue, though, this might be redressed by carefully crafting the public monopoly on defensive cybersecurity. In this case, a state could require that testing of products be paid for by developers, subject to strict guidelines.

More serious are the third and fourth issues. Third, a public monopoly on defensive cybersecurity could restrict individual autonomy. The sorts of monitoring systems necessary to preclude individuals and firms from engaging in private defensive cybersecurity (for example, topping up their publicly mandated cybersecurity or going beyond their allocated amount of private defensive cybersecurity) would be highly intrusive. To ensure equality, the state would have to preclude

or whose protection is too risky; public defensive cybersecurity is required for this. See, further, Pattison, *The Morality of Private War*.

[73] Dunn Cavelty and Wenger, 'Cyber security meets security politics', p. 23.

[74] Hoffman and Nyikos, 'Governing Private Sector Self-Help', p. 48.

[75] Ibid., p. 49.

[76] Ibid., p. 42. In addition, if not ideal, a public monopoly may also fail to tackle the problems of inequality and democratic accountability (for example, as government bodies are not properly subject to democratic control).

[77] Sales, 'Privatizing cybersecurity', p. 681; also see Hoffman and Nyikos, 'Governing Private Sector Self-Help', p. 10.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

topping up, so that there are equal levels of even seemingly innocuous measures, such as antivirus software, firewalls, and authentication systems, so that no one is left more vulnerable (and so attacks are deflected onto them). The monitoring of individuals to see whether they have topped up could curtail Internet freedoms and privacy.[78]

Fourth, even if there were a monopoly on defensive cybersecurity at the state level, there may be significant inequalities between states in their capacities of defensive cybersecurity. States may also deflect attacks onto others. (Indeed, this is already happening with the implementation of the National Cybersecurity Centre in the UK.)[79] The problem, then, is that individuals will still experience significant inequalities, which will be determined by which state they reside in. To overcome this issue would require an even more infeasible scheme – some form of global arrangement that ensures equal defensive cybersecurity for all, regardless of which state they are in. This may, of course, be undesirable for other reasons, such as if the global arrangement were to be dominated by authoritarian states.

Where does this leave us? The Highly Restrictive Approach is clearly problematic, at least non-ideally (that is, where there are notable 'unfavourable circumstances', such as limits on public spending and a lack of cooperation between states).[80] Private defensive cybersecurity, including passive measures, such as firewalls and patch management, and defensive forms of ACD, such as beaconing and honeypots, is permissible, despite the potential effects on inequality and democratic accountability. The most likely alternative of not protecting legitimate interests against cyberattack seems unpalatable. As revisionist just war theorists hold, defensive force that may harm others is permissible providing that it is *necessary* (that is, there are no better means of defending against the threat) and *proportionate* (that is, it is better to defend against the threat than not).[81] Crucial here is that, in the absence of a feasible alternative – that is, effective public cybersecurity – any harms of private cybersecurity in terms of inequality and democratic accountability may often be necessary in the defence of legitimate interests against cyberattack.[82] To put this another way, private defensive cybersecurity is the only feasible way to ensure some protection, even if it leads to problems in terms of inequality and democratic accountability.[83] Thus, we need to look to the Moderately Restrictive Approach or Permissive Approach. In the next section, I will argue that the Permissive Approach is clearly inappropriate since offensive cyber measures are highly problematic.

Before we turn to this, it should be noted that firms may not simply be *permitted* to engage in defensive cybersecurity but *required* to do so. In other words, there may sometimes be a duty to provide defensive cybersecurity. This is particularly (but not solely) for critical infrastructure, given that the public could be at risk from inadequate protection.[84] My reasoning is this. In general, individuals have humanitarian duties to protect those at risk of notable harm.[85] Firms can be

[78] For an in-depth analysis of the effects on privacy, see George Lucas, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare* (New York: Oxford University Press, 2017).

[79] Stevens et al., 'UK Active Cyber Defence', p. 18.

[80] I leave aside whether a global public monopoly might be *ideally* desirable.

[81] See, for instance, McMahan, *Killing in War*; Seth Lazar, 'Necessity in self-defense and war', *Philosophy & Public Affairs*, 40:1 (2012), pp. 3–44; Jeff McMahan, 'Proportionate defense', *Journal of Transnational Law and Policy*, 21 (2013–14), pp. 1–36; Jeff McMahan, 'Proportionality and necessity in *Jus in Bello*', in Helen Frowe and Seth Lazar (eds), *The Oxford Handbook of the Ethics of War* (Oxford: Oxford University Press, 2018), pp. 418–39.

[82] To be sure, if the negative effects on inequality and democratic accountability are very large, then the measure might still be impermissible under the principle of proportionality. If might, for instance, be better not to defend even one's own interests if doing so will deflect the attack onto others who are more vulnerable.

[83] Private defensive cybersecurity should also, of course, still be subject to regulation nationally and internationally, and follow standards and best practice, such as the National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 2018).

[84] Even when critical infrastructure is not at stake, there are other duties to protect individuals or groups at risk of significant harm (for example, when the violation of their privacy would lead to basic rights violations).

[85] See, famously, Peter Singer, 'Famine, affluence, and morality', *Philosophy & Public Affairs*, 1:3 (1972), pp. 229–43.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

a means by which these humanitarian duties are discharged as, for instance, major shareholders bear some of the costs of ensuring that there is the adequate protection of critical infrastructure, so that innocent individuals are not harmed. It seems that firms can be asked to bear the costs of fulfilling such duties, given that, in a *laissez-faire* system, where there is not the public ownership of critical infrastructure, firms often enjoy significant benefits. These include, notably, reduced taxation and less regulation, which can increase the profit margins and the benefits enjoyed by shareholders, compared to a system where there is much greater taxation and regulation of firms.

As it stands, though, the private sector has often failed to protect both its own and the public interest. It has been estimated that 508,000 American jobs have been lost to cybercrime and the US alone has lost up to $120 billion.[86] The private sector has tended to under-protect itself because it has focused on short-term costs and benefits to the detriment of longer-term ones (for example, the negative effects of stolen trade secrets can take years to manifest) and because the costs of intrusions are faced by others.[87] In terms of critical infrastructure, Madeline Carr finds that the private sector accepts responsibility for securing critical infrastructure only to the point that it is profitable to do so, 'as far as the cost of dealing with an outage promises to cost more than preventing it'.[88] Thus, it should be mandated (for example, in national laws) that firms *must* provide adequate cyber defence (especially of critical infrastructure), by doing so themselves or hiring others to do so. This is in line with the EU's Directive on Security of Network and Information Systems (known as the 'NIS Directive'), which directs member states to require firms that are tasked with critical infrastructure protection to have adequate cybersecurity.[89]

3. Private offensive cybersecurity

Thus far, we have seen that defensive cybersecurity is permissible (and required). Let us now turn to offensive cybersecurity, such as offensive forms of ACD (for example, takedown of botnets and white hat ransomware) and hacking back. Is it permissible – and even obligatory – for private firms to engage in such measures, as suggested by the Permissive Approach?[90] Again, I will start with the prima facie, idealised case, which seems plausible, before considering the non-ideal problems. I will argue that private offensive cybersecurity should be precluded.

The prime facie case turns on extending the argument for defensive cybersecurity to offensive cybersecurity. The crux is this: if (necessary and proportionate) defensive action to protect legitimate interests is justified, why is (necessary and proportionate) offensive action to protect legitimate interests also not justified? To see this, consider first an individual-level case involving traditional security interests.

> *Terrorists*: You are reliably informed by an associate of a terrorist group that they will blow up your house whilst you are on holiday. What's more, the group have already begun the early stages of their attack by accumulating bomb-making material. Luckily, you can stop

[86] Etzioni, 'The private sector', p. 70.

[87] Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton, 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate', *Journal of Cyber Security*, 4:1 (2018), available at: {doi: 10.1093/cybsec/tyy006}; Etzioni, 'The private sector', p. 71.

[88] Carr, 'Public-private partnerships', p. 57.

[89] European Union, 'The Directive on Security of Network and Information Systems (NIS Directive)' (24 August 2018).

[90] Those sympathetic to this view include Hardik Gandhi, 'Active cyber defense certainty: A digital self-defense in the modern age', *Oklahoma City University Law Review*, 43 (2019), pp. 279–309; Lin Allhoff, and Abney, 'Is warfare the right frame'; Benjamin Powell, 'Is cybersecurity a public good: Evidence from the financial services industry', *Journal of Law, Economics and Policy*, 1:2 (2005), pp. 497–510; and Rosenzweig, 'International law and private actor active cyber defensive measures'. Others call for some offensive cyber operations to be permitted, for example, Hoffman and Nyikos, 'Governing Private Sector Self-Help', p. 56 and Center for Cyber and Homeland Security, 'Into the Gray Zone'.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

> the attack by acting quickly now. This is by breaking into their house and spilling the bomb-making material. You foresee that, in doing so, you will cause the terrorists' house severe damage. If you were to call the police, they would not be able to stop the attack in time.

In this case, it seems that you can justifiably engage in offensive force in order to protect yourself. Crucially, this is necessary – it is the only way that you will be able to defend yourself; your house will otherwise be blown up. Defensive measures, such as barricading your house, will not work. Moreover, the terrorists are liable to (proportionate) offensive force, given their enactment of their culpable plan to harm you.[91]

The same, it seems, is true of engaging in offensive cybersecurity. Consider an analogous case.

> *Hackers*: You are reliably informed by an associate of a group of hackers that they will steal much of your money. What's more, the group have already begun the early stages of their attack by developing their hacking tools. Luckily, you can stop the attack by acting quickly now. This is by hiring a private firm to hack into their network and disable it. You foresee that, in doing so, you will harm the hackers' computers, which will also mean that they cannot engage in legitimate online activity. The government lacks the spare resources to stop the attack.

Again, it seems that you can hire the private firm to hack their computers. The hackers are liable to force, given that they will culpably attack you. What is crucial, again, is that defensive measures will not be sufficient.

In fact, even if defensive measures might work *somewhat*, or be less likely to succeed, offensive force might be justified if it is likely to better protect your legitimate interests. For instance, if barricading your house might mean that only half of it is blown up, spilling the bomb-making material can be justified. Similarly, if using defensive cybersecurity measures will work somewhat, or be less likely to succeed, offensive cybersecurity might be justified. Suppose that defensive measures (for example, honeypots) might have only a 50 per cent chance of success of preventing the attack. Suppose further that, by contrast, an offensive cyber measure (for example, hacking back) has a 60 per cent chance of success. Crucial again here is that those subject to the force – for example, the hackers – are liable to it. They cannot complain that they are subject to offensive force (when proportionate to their degree of liability) since they are culpable. Indeed, for this reason, several philosophers of self-defence and just war theorists hold that proportionate and necessary preventive operations can be justified against liable attackers and not simply defensive or pre-emptive military action.[92]

Likewise, it seems that private firms could engage in offensive operations against hackers in order to protect legitimate interests, when doing so is the best means of defending themselves. This seems most intuitive when the interests protected concern those who are very poor. Suppose, for instance, that rich hackers target the pension funds of a small, impoverished mining community, which is invested in a local firm. It seems that the firm could use offensive operations

[91] To be sure, if your information is not reliable, it might not be permissible to target the terrorist. Also note that it is important here that the terrorists have already *begun to act* upon the plan; I leave aside the controversial issue of whether individuals can be liable for merely *intending* a culpable act (that is, which they have not yet enacted). See Larry Alexander and Kimberly Kessler Ferzan, 'Danger: The ethics of preemptive action', *Ohio State Journal of Criminal Law*, 9:2 (2012), pp. 637–67.

[92] See, for instance, Allen Buchanan, 'Justifying preventive war', in Henry Shue and David Rodin (eds), *Preemption: Military Action and Moral Justification* (Oxford: Oxford University Press, 2007), pp. 126–42; Allen Buchanan and Robert O. Keohane, 'The preventive use of force: A cosmopolitan institutional proposal', *Ethics & International Affairs*, 18:1 (2004), pp. 1–22; Jeff McMahan, 'Preventive war and the killing of the innocent', in David Rodin and Richard Sorabji (eds), *The Ethics of War: Shared Problems in Different Traditions* (Aldershot: Ashgate, 2005), pp. 169–90. To reiterate, any response must be proportionate to the degree of liability of the attackers. It would, for all intents and purposes, not be proportionate to use lethal or significant physical force in these cases, if the sort of harm from the attacker involves only property damage.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

against the hackers if they are likely to be more effective, even if defensive operations would be somewhat likely to succeed.

What *ideally* appears to matter, then, is how justifiable a response is at tackling the unjust threat and, in doing so, protecting legitimate interests, rather than simply whether the operations are defensive or offensive (to be sure, I will argue shortly that the distinction between offensive and defensive operations is important in practice, that is, *non-ideally*). Somewhat analogously, humanitarian intervention may be viewed as 'offensive', given that it involves coercive action beyond the borders of the state, but is sometimes permissible (and indeed required) to tackle mass atrocities.[93] This is because, although it transgresses state sovereignty (on a view of sovereignty as authority), this can sometimes be outweighed by the greater importance of effectively saving lives. In a somewhat similar vein (where the stakes are often lower), it does not seem that the fact that offensive cyber measures occur within the networks of others is decisive, if the response would be likely to bring about a significant enough benefit, such as stopping a significant theft of property or attack that threatens significant harm to innocents. In fact, when the basic interests of others are at stake and they would otherwise not be protected, there may be a *duty* to engage in offensive operations. Not properly protecting the interests of, for instance, the impoverished mining community by engaging in the more effective offensive operations would be highly problematic. The firm would be morally *required* to hack back. The Permissive Approach can, then, potentially ground not only a *permission*, but also a *duty* to engage in offensive cybersecurity.

There is, then, a seemingly plausible *idealised* case for offensive action. Yet when we consider more non-ideal features, it becomes clear that private offensive cybersecurity is highly problematic. The problems that face defensive cybersecurity of inequality and undermining democratic control are also likely to apply to offensive cybersecurity as, for instance, the poor cannot purchase private offensive cybersecurity and the private cybersecurity firms engaged in private offensive cybersecurity transcend traditional lines of democratic accountability. In addition, offensive cybersecurity faces three further problems.[94] These mean that, *in practice*, whether a measure will be offensive or defensive will be central to its justifiability.

Collateral damage

First, offensive cyber measures are of particular concern because they can cause collateral damage to innocent third parties or networks, or to those wrongly attributed as the source of the attack.[95] As Eugene Volokh notes, we should be sceptical about drawing a straightforward analogy between physical self-defence and self-defence in the cybersecurity sector.[96] This is because, compared to physical self-defence (where the risks are serious), there is an even greater risk of error in the cybersecurity sector that you might attack the wrong target, given the well-known problems of attribution, and there is significant potential that your response will harm third parties.[97] To

[93] Gregory Reichberg and Henrik Syse, 'Humanitarian intervention: A case of offensive force?', *Security Dialogue*, 33:3 (2002), pp. 309–22.

[94] These problems are not unique to private cyber actors; they may also apply (to varying degrees) when states engage in offensive operations. I leave aside the issue of whether states should engage in offensive operations, which has been subject to significant attention already. See, for instance, Gandhi, 'Active cyber defense certainty'; Lin, 'Ethics of hacking back'; Emilio Iasiello, 'Hacking back: Not the right solution', *Parameters*, 44:3 (2014), pp. 105–13; Orin Kerr, 'The hackback debate', *Steptoe Cyberblog* (2012), available at: {www.steptoecyberblog.com/2012/11/02/the-hackback-debate}; Brandon Valeriano and Benjamin Jensen, 'The Myth of Cyber Offense: The Case for Restraint', Policy Analysis, Cato Institute (15 January 2019); and Eugene Volokh, 'The hackback debate', *Steptoe Cyberblog* (2012), available at: {www.steptoecyberblog.com/2012/11/02/the-hackback-debate}.

[95] Hoffman and Levite, 'Private Sector Cyber Defense', pp. 4–10.

[96] Volokh, 'The hackback debate'.

[97] Orin Kerr, 'Virtual crime, virtual deterrence: A skeptical view of self-help, architecture, and civil liability', *Journal of Law, Economics, and Policy*, 1:1 (2005), pp. 197–214 (pp. 204–05); Volokh, 'The hackback debate'.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

elaborate, the servers attacked may also host important civilian services, such as for emergency services, hospitals, or schools.[98] It is also very difficult to contain a cyberattack. For instance, Microsoft's takedown of two botnets associated with No-IP.com (a domain name server (DNS) service) had the effect of denying five million legitimate users access to their domains.[99]

In their defence of private ACD, Patrick Lin, Fritz Allhoff, and Keith Abney claim that the worry about innocent third parties being harmed is exaggerated.[100] First, they argue that innocent cyber threats can be liable. Second, they claim that the innocence of third parties can be overridden by the 'greater good of public health' in the cyber realm.[101] Third, they claim that those involved in botnets can fail in their obligations to preclude themselves from being hijacked and so can be viewed as somewhat morally responsible (that is, negligent) for being botnets. If this is true, they would be what are called 'innocent threats' in the literature on revisionist just war theory.[102]

These claims rest, however, on a far too permissive notion of liability for harm. First, although space precludes a detailed assessment of the issue, it seems wrong to hold that innocent threats are liable.[103] Innocent threats are not culpable for their threat and so have not forfeited their right not to be subject to force. Thus, if those involved in botnets are innocent threats, they are not liable. Second, although consequentialist considerations can sometimes outweigh liability (that is, through what are called in the literature on revisionist just war theory 'lesser-evil justifications'), it is very doubtful that this is the case with private offensive cybersecurity. The potential benefits of targeting botnets are too uncertain and vague, and the harms too clear, for this to be justified.[104] One worry in this regard is that there is a risk that permitting offensive cybersecurity creates an incentive to hide their location even more.[105] Another worry is that, even if a firm takes down one botnet, there may be multiple botnets, which limits the effectiveness of the responses.[106] Third, many of those who become part of botnets will have taken reasonable precautions or lack the means to take reasonable precautions, and so are not negligent.[107] Thus, many who are part of botnets are still innocent threats. Moreover, even if some involved in botnets are *somewhat* negligent (for example, if they have failed to take reasonable precautions), this does not seem to be sufficient to render them liable to offensive cyber measures, which would be a large cost for them to bear. This seems to be beyond that which can be required by their degree of liability for failing to fulfil their obligations to protect themselves.

Putting these points in terms of Jeff McMahan's influential terminology of 'wide' and 'narrow' proportionality, taking down botnets would fall foul of *narrow* proportionality, that is, how much those who are liable can be required to bear, for example, for some minor negligence in failing to update a security patch.[108] Such measures could also fall foul of *wide* proportionality, that is, how much those who are innocent threats or innocent third parties can be required to bear, with innocent individuals having to bear unreasonable costs. Hijacked computers can, for instance, play an

[98] Rosenzweig, 'International law and private actor active cyber defensive measures', p. 108.

[99] Nuala O'Connor, 'Additional views of Nuala O'Connor', in Center for Cyber and Homeland Security, 'Into the Gray Zone', p. 36.

[100] Lin, Allhoff, and Abney, 'Is warfare the right frame', pp. 51–2.

[101] The greater good here concerns the potential to access command and control machines and potentially compromise the attacker's home machine and identify other victims who do not yet know that they have been attacked. Stewart Baker, 'The hackback debate', *Steptoe Cyberblog* (2012), available at: {www.steptoecyberblog.com/2012/11/02/the-hackback-debate}.

[102] See, for instance, McMahan, *Killing in War*.

[103] Seth Lazar, 'Responsibility, risk, and killing in self-defense', *Ethics*, 119:4 (2009), pp. 699–728.

[104] Kerr, 'The hackback debate'.

[105] Kerr, 'Virtual crime'; Kerr, 'The hackback debate'.

[106] Iasiello, 'Hacking back', p. 108.

[107] Shane Huang, 'Proposing a self-help privilege for victims of cyber attacks', *George Washington Law Review*, 82 (2014), pp. 1229–66 (pp. 1254–6).

[108] McMahan, 'Proportionality and necessity'.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

important public role, such as a high-tech computer that belongs to a hospital or an airport, and so disabling them could have excessive costs for innocent third parties.[109]

Rights violations

Second, offensive cyber measures – and particularly those that involve espionage – can increase rights violations. This is when private cybersecurity firms provide services to help governments spy on populations. Cyber espionage provided by private firms can be used by governments to facilitate the repression of dissidents and human rights activists. In October 2019, head of WhatsApp, Will Cathcart, identified the NSO Group, an Israeli-based company, as the source of a hack that had led to more than one hundred incidents of abusive targeting of human rights defenders and journalists.[110]

To be sure, just as conventional PMSCs often appeal to governments by promising not to do business with other states, cybersecurity firms claim that they will work only for legitimate organisations (both private and public). For instance, Netragard, a firm that focuses on exploits, claims that it works only for US customers, the Grugq (a broker) claims that he does not sell to Russian or Chinese buyers in part out of self-interest (because they do not pay much), and Vupen claimed that it sells only to NATO members and those currently not subject to international sanctions.[111] Others, however, are less reticent and are instead willing to let numerous clients hire their services. The co-founder of ReVuhn reportedly claimed that 'I don't see bad guys or good guys. It's just business.'[112] The clients of Hacking Team allegedly included Azerbaijan, Bahrain, and Sudan – and their products have allegedly been used to target dissidents.[113] For example, a pro-democracy activist in the UAE was allegedly targeted by a remote-control system sold by Hacking Team and he was subsequently arrested in the UAE and tortured.[114]

Private cybersecurity firms may be able to attempt to stop some abuses by requiring customer service and product updates, especially given the transitory nature of software, although some firms may have no control over their products once they are sold.[115] Analogously, defence firms may have little control over the conventional weapons that they sell to governments and rebel groups, including when they are used for human rights abuses and to fuel conflicts. Moreover, states can easily circumvent firms' self-imposed limits by commissioning private firms or other states to serve as proxies.[116] For instance, despite extensive sanctions, in 2011 Syria was able to obtain Internet filtering devices, which it used to block and monitor thousands of attempts to connect to websites of opposition figures and those covering the Syrian uprising, even though the devices were originally supposed to be for Iraq's Ministry of Communications.[117]

Instability

The third point is more speculative: it concerns when private actors engage in hacking back. There are notable risks, particularly if a more permissive environment develops (which I consider

[109] Volokh, 'The hackback debate'.

[110] Will Cathcart, 'Why WhatsApp is pushing back on NSO group hacking', *Washington Post* (29 October 2019).

[111] Maurer, *Cyber Mercenaries*, p. 78; Sales, 'Privatizing cybersecurity', p. 640.

[112] Sales, 'Privatizing cybersecurity', p. 642.

[113] Maurer, *Cyber Mercenaries*, p. 78.

[114] Ibid., p. 79.

[115] Ibid.

[116] Sales, 'Privatizing cybersecurity', p. 655.

[117] Ibid.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

shortly) where private firms are permitted to engage in hacking back.[118] Various firms could conceivably use offensive operations to accidentally or intentionally target other firms. Such hacking back operations might potentially also drag states into conflicts. As Irving Lachow notes, '[i]f a contractor inadvertently launched a cyber attack that was perceived by another country as an act of war, the United States could be held responsible for that action.'[119] A related worry here is that of 'friendly fire', where hackers attack from an allied or friendly country (for example, through a botnet) and a response risks creating tensions with allies.[120] To reiterate, I am not claiming that these risks are *currently* manifest; my aim here is to highlight the *potential* dangers of a Permissive Approach in the future.

In reply, Lin argues that escalation is unlikely because private cyberattacks will be seen as more like 'frontier incidents', that is, force short of war – rather than outright attacks.[121] Such incidents are, he suggests, less provocative because they are invisible and less visceral, even if the economic costs are sometimes high.[122] In response, Lin is right that escalation is not necessary.[123] However, it might still occur *sometimes* (as he admits). Much depends on whether the incidents are, in fact, perceived by the victims (even if the harms are small compared to kinetic warfare) as minor transgressions or major attacks.

But this is to some extent beside the point: the forms of instability that might develop from offensive operations are not simply about dragging states into conflicts. It is broader than this: the issue is increasing the number and range of actors that are engaged in offensive cyber operations. This can, in the longer term, increase instability, even if this takes a while to be manifest. In addition, there are other ways in which international stability can be undermined through private cybersecurity offensive operations, beyond hacking back, most obviously through *political* instability with interference in democratic elections. As Tim Maurer notes, focusing too much on military conflict 'ignores the full spectrum of political effects hacking has been used for, as the events in Ukraine and the malicious hacks during the 2016 US elections make clear'.[124]

Regulating offensive cybersecurity

Given these issues, it is clear that the Permissive Approach is mistaken and that the Moderately Restrictive Approach is favourable, where private actors perform only defensive cybersecurity. Unlike for defensive cybersecurity, there is also a plausible, potentially feasible solution: do not permit private firms to engage in such operations. If private firms are not permitted to engage in offensive operations, and states cannot fill the void, this might well be desirable, given the risks of offensive cybersecurity. (As noted above, I leave aside the issue of whether states should also be precluded from engaging in offensive cyber operations, although some of these problems seem likely to apply to statist operations as well.) Whereas the risks of precluding firms from engaging in defensive operations are serious, especially as they are responsible for protecting much critical infrastructure, the risks of precluding offensive operations are far lower (given the potential efficacy of defensive approaches) and the harms potentially much greater. Important here is that private offensive operations may not be necessary because the ineffectiveness of passive cybersecurity is often exaggerated. Many firms do not implement basic defensive security procedures, such as the 'Twenty Critical Security Controls for Effective Cyber Defence'

[118] For somewhat analogous issues with PMSCs, see Deborah Avant, 'The implications of marketized security for IR theory: The democratic peace, late state building, and the nature and frequency of conflict', *Perspectives on Politics*, 4:3 (2006), pp. 507–28.

[119] Lachow, 'The private sector role', p. 12.

[120] Iasiello, 'Hacking back', p. 110.

[121] Lin, 'Ethics of hacking back'.

[122] Ibid., p. 17.

[123] Also see Borghard and Lonergan, 'Cyber operations as imperfect tools'.

[124] Maurer, *Cyber Mercenaries*, pp. 3–4.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

(CSC), which has been found to reduce vulnerability by 88 per cent.[125] In short, if firms defend themselves properly, offensive measures would not be required. The upshot is that there should be a presumption against engaging in offensive operations. This may be overridden on occasion, when the evidence is patent, but there is a significant burden of proof, given what we know about private offensive cybersecurity.

It also follows that there should be robust domestic and international regulation to preclude offensive cyber measures.[126] Domestically, although several states preclude offensive cybersecurity, especially hacking back, few enforce it, and some states permit it tacitly.[127] To be sure, domestic regulation, when enforced, can play an important role in precluding private offensive cybersecurity. Yet, although valuable, it is unlikely to be sufficient because if the regulation is strict, firms may relocate.[128] Indeed, some cybersecurity firms have entire divisions located abroad so that they can engage in activity that they would not be permitted to undertake in the US.[129] A coordinated, international approach is therefore required. Yet, according to the authors of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, 'international law by and large does not regulate cyber operations conducted by non-State actors, such as private individuals or companies'.[130] For instance, if Sony had chosen to hack back against North Korea for its attack on it in 2014, 'it would have violated no customary rule of general international law' (although it might have raised the issue of US due diligence).[131] There needs, then, to be clear and strong global norms against offensive private cyber action, and ultimately, as Mette Eilstrup-Sangiovanni powerfully argues, a new 'International Cyberwar Convention' (ICWC).[132] This would hold states responsible for cyberattacks launched from their jurisdiction, most clearly, when the attackers are under the direct control of the state, but also when the state is not in direct control – specifically, when it fails in its duties to take reasonable measures to prevent non-state actors from launching attacks against other states from within its borders.[133] Although a diplomatic breakthrough on a new cyber treaty is unlikely anytime soon, given *some* states' interests in allowing offensive cyber operations to occur, attempts to bring the ICWC into existence could add political weight and visibility to the issues.[134]

In the meantime, the room to engage in offensive cyber operations seems likely to expand as the market for private cybersecurity firms grows and existing laws change to become more

[125] Iasiello, 'Hacking back', p. 111.

[126] To the extent that regulation is feasible and would address the issues raised by private offensive cybersecurity, these issues are not deeper ones, although they are still are, of course, serious. (There are deeper issues with private cybersecurity in general, discussed in the first half of the article, which would apply to private offensive cybersecurity). Also note that it may be better to preclude states from engaging in offensive cyber operations, but, again, this is beyond the scope of this article.

[127] Hoffman and Levite, 'Private Sector Cyber Defense', p. 4; Huang, 'Proposing a self-help privilege'; Rosenzweig, 'International law and private actor active cyber defensive measures'.

[128] Hoffman and Levite, 'Private Sector Cyber Defense', pp. 14–15.

[129] Ibid., p. 15.

[130] Michael Schmitt (ed.), *Tallinn Manual*, p. 175. For instance, the Budapest Convention on Cybercrime does not cover important states such as Russia and Brazil and the Tallinn Manual has failed to gain widespread support from states. Mette Eilstrup-Sangiovanni, 'Why the world needs an International Cyberwar Convention', *Philosophy & Technology*, 31 (2018), pp. 379–407 (p. 388, n. 19). The Wassenaar Arrangement precludes states from exporting some offensive cyberweapons but covers only 42 states.

[131] Michael Schmitt (ed.), *Tallinn Manual*, p. 130.

[132] Eilstrup-Sangiovanni, 'Why the world needs an International Cyberwar Convention'.

[133] Ibid., p. 397. It might be worried that an ICWC would lead to authoritarian states increasing their violations of human rights domestically. However, this could be avoided if the ICWC is carefully crafted so as to focus on offensive measures. Moreover, it is unclear whether an ICWC would change existing practice where authoritarian states can already use extensive Internet controls.

[134] Tim Maurer, 'A dose of realism: The contestation and politics of cyber norms', *Hague Journal on the Rule of Law*, available at: {doi: 10.1007/s40803-019-00129-8}; Eilstrup-Sangiovanni, 'Why the world needs an International Cyberwar Convention', p. 400.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

permissible.[135] The Active Cyber Defense Certainty (ACDC) Act, introduced by Republican Tom Graves in 2017 (and reintroduced in 2019), aims to create a far more permissive environment, amending the Computer Fraud and Abuse Act (CFAA) to allow for individuals and firms to, for instance, go beyond their networks to disrupt and identify attacks and retrieve stolen data.[136] Even if this bill is defeated, it seems that private offensive cyber operations are more likely in the future. The US's previous reluctance to use offensive cyber measures has waned, as the more defensive cyber stance adopted by the Obama administration has moved to a more aggressive, preventive one under the Trump administration.[137] The US has acknowledged openly that it hacked the media operations of ISIS, by, for instance introducing dropped connections, access denials, and program glitches, in order to frustrate its online operations without it realising that it was being hacked.[138] Other states perceive a need to adopt more offensive stances, including Russia, China, Germany, and France.[139] The reliance on the private sector, and the experience with PMSCs, suggests that it is likely that private firms will play a role in states' offensive postures.

Conclusion

In conclusion, private firms can permissibly launch defensive cybersecurity (passive measures and defensive ACD) and are obliged to do so (most clearly for critical infrastructure), despite concerns about equality and democratic accountability, given the problems of a public monopoly on defensive cybersecurity. They are not, however, permitted to perform offensive cybersecurity (offensive ACD and hacking back), given the myriad of problems with this, despite the idealised, prima facie case for it. On the contrary, there should be international regulation to preclude private offensive cybersecurity. Thus, I have defended the Moderately Restrictive Approach against the Highly Restrictive Approach and Permissive Approach.

I will finish by highlighting how this analysis is significant more broadly for the fields of the ethics of cyber operations and the privatisation of military force. First, in regard to the ethics of cyber operations, the issue of private cybersecurity is clearly of major importance. This is not simply because private actors currently play major roles in cybersecurity and are likely to do so for the foreseeable future. It is also because the issue of private cybersecurity calls into question how much the existing frameworks in this literature are fit for purpose. These tend to focus on applying statist just war conditions to the cyber realm.[140] At the very least, such frameworks that rely on just war theory should reflect the significant role played by private actors by, for instance, updating the principles to reflect the changing security landscape.

However, it might be preferable to move away from the standard, state-focused lists of just war criteria, and instead adopt new fit-for-purpose frameworks. These may still draw on some of the morally relevant *underlying* principles that are crystallised in just war criteria, such as proportionality and necessity, and that are widely held as relevant in moral and political philosophy, and highlighted by revisionist just war theorists. Yet the frameworks would use these principles to offer criteria that are *particularly applicable to the cyber world*, which relies heavily on the private

[135] Maurer, *Cyber Mercenaries*, p. 19.

[136] Gandhi, 'Active cyber defense certainty', p. 300.

[137] Valeriano and Jensen, 'The myth of cyber offense'. This is notable with the Department of Defence's 'Defend Forward' posture, which concerns confronting threats before they reach US networks and the Director of the National Security Association Paul M. Nakasone's recent statements that the US will react robustly to cyberattacks. Stéphane Taillat, 'Disrupt and restraint: The evolution of cyber conflict and the implications for collective security', *Contemporary Security Policy*, 40:3 (2019), pp. 368–81 (p. 375); Dina Temple-Raston, 'How the U.S. hacked ISIS', *National Public Radio* (26 September 2019), available at: {www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis}.

[138] Ibid.

[139] Eilstrup-Sangiovanni, 'Why the world needs an International Cyberwar Convention', p. 386.

[140] See, for instance, Eberle, 'Just war and cyberwar'; Lee, 'The ethics of cyberattack'; Brian Orend, 'Fog in the fifth dimension'.

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press

sector.[141] An applied, specifically relevant framework – specific principles for cybersecurity, including private firms – would be quite different to the principles normally offered in just war theory, drawing only on the underlying insights for thinking about international ethics, and would not depend on the war context.

Second, in regard to the privatisation of warfare, PMSCs have been criticised heavily when performing traditional security functions. In this article, we have seen that there are also problems with the use of private firms for security in the cyber realm. Our understanding of the problems of PMSCs performing traditional security helps *somewhat* with understanding the problems posed by private cybersecurity firms. However, we have also seen that there are two major differences between cybersecurity and regular security. The first is that cybersecurity has not, unlike regular security, been outsourced. The second is that, in large part, private firms are not contracted to ensure cybersecurity, but instead are largely entrusted to do so. The former means that there is not an obvious process to reverse privatisation that can be followed to reduce the role of the private sector, which lends further credence to the Moderately Restrictive Approach as the Highly Restrictive Approach seems even more infeasible. The latter – that private firms are entrusted to provide cybersecurity – means that the private cybersecurity sector largely steers, and not simply rows, whereas the state plays a much larger contracting, and to some degree controlling, role in the traditional security sector. Whereas the state has some form of control that comes from the contracting process, this is not relevant for much of private cybersecurity. As we have seen, this gives us perhaps even more reason to be concerned about the prevailing systems of private cybersecurity than those of PMSCs.

Acknowledgments. An earlier version of this article was presented at the Annual Convention of the International Studies Association, Toronto, March 2019. I would to thank the participants for helpful discussions, particularly Charles Mahoney, Chris Spearin, and Benjamin Tkach. I would also like to thank the anonymous reviewers for their very helpful comments and suggestions that improved the article significantly.

James Pattison is Professor of Politics at the University of Manchester. His work focuses on ethical issues in international politics and he has particular expertise on the responsibility to protect, just war theory, private security, and non-military measures to resolve crises. He has written three books (all published by Oxford University Press), the most recent of which examines the ethics of the alternatives to war: *The Alternatives to War: From Sanctions to Nonviolence* (Oxford: Oxford University Press, 2018).

[141] The cyber realm may not raise different *fundamental* challenges to the central moral principles in moral and political philosophy governing war and self-defence. My point, rather, is that it raises different *applied* issues. See Roger Crisp, 'Cyberwarfare: No new ethics needed', *Oxford Practical Ethics* blog (19 June 2012). See, further, James Pattison, *The Alternatives to War: From Sanctions to Nonviolence* (Oxford: Oxford University Press, 2018) and James Pattison, 'The ethics of foreign policy: A framework', *SAIS Review of International Affairs*, 39:1 (2019), pp. 21–35.

Cite this article: Pattison, J. 2020. From defence to offence: The ethics of private cybersecurity. *European Journal of International Security* 5, 233–254. https://doi.org/10.1017/eis.2020.6

https://doi.org/10.1017/eis.2020.6 Published online by Cambridge University Press