BUSINESS AND SECURITY SERIES Nº3

The Privatization of Security and the Market for Cyber Tools and Services

DCAF Geneva Centre for Security Sector Governance

TIM MAURER AND WYATT HOFFMAN

Carnegie Endowment for International Peace

About the series:

The Business and Security Series provides a focus on contemporary security governance challenges and examines the ways in which greater cooperation between states, international organisations, civil society and the commercial sector can help to address them. The series promotes policy relevant research as part of the mandate of DCAF's Business and Security Division to support innovative partnerships that bring stakeholders together to realize shared security and development goals.

The Privatisation of Security and the Market for Cyber Tools and Services
Edited by Anna Marie Burdzy and Teresa Hatzl
Published by the Geneva Centre for Security Sector Governance
Maison de la Paix Chemin Eugène-Rigot 2E 1202 Geneva Switzerland
Website: https://www.businessandsecurity.dcaf.ch/
©2019 DCAF

TERMINOLOGY[1]

Cybersecurity:

For the purposes of this paper, cybersecurity may be defined as the body of technologies, measures, processes, and practices designed to protect networks, devices, programmes as well as data from attack, damage or unauthorized access.

Cyber attack:

For the purposes of this paper, cyberattack is an action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself.

Cyber vulnerability:

Cyber vulnerability is a cybersecurity term referring to a flaw or any type of weakness in a computer system that can leave it open to attack.

Distributed Denial of Service (DDoS):

A Distributed Denial of Service (DDoS) attack is a type of cyberattack where multiple compromised systems are used to target a single system causing its disruption. Generally, a DDoS attack uses multiple computers and Internet connections to flood the targeted system. Very often these attacks are global in nature.

'Hacking back':

Hacking back is one form of active defence that might be used to gather intelligence about the source of an intrusion to determine attribution or what data might have been stolen. It might also involve neutralizing or shutting down an attacking system to stop it from causing further damage.

Malware exploit:

A malware exploit is software that utilizes vulnerabilities in systems or networks, allowing the attackers to take control of a piece of software or entire computing system.

Payload:

A payload is code written to achieve some desired malicious end, for instance to delete data or manipulate industrial control systems.

[1] This terminology section was added by the Geneva Centre for Security Sector Governance to help clarify key terms used.

Private military and security company (PMSC):

“PMSC” encompasses all companies that provide either military or security services or both, irrespective of how they describe themselves. Examples of military services that companies can provide include but are not limited to: material and technical support to armed forces, strategic planning, intelligence, investigation, training activities, satellite surveillance, or other related activities.

Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict:

The Montreux Document reaffirms the existing obligations of states under international law, in particular international humanitarian law (IHL) and human rights law, relating to the activities of PMSCs in situations of armed conflict. As a non-binding document, it also lists good practices designed to help states take national measures to implement these obligations. Launched by Switzerland and the International Committee of the Red Cross (ICRC) in 2008, the Montreux Document clarified the misconception that PMSCs operate in a legal vacuum by recalling and compiling applicable international obligations.

International Code of Conduct (ICoC) and the Association (ICoCA):

The ICoCA promotes the responsible provision of security services and respect for human rights and national and international law in accordance with the ICoC. The ICoC includes a wide range of standards and principles for the responsible provision of private security services which can be broadly summarized in two categories: first, principles regarding the conduct of Member Company personnel based on international human rights and humanitarian law standards including rules on the use of force, sexual violence, human trafficking and child labour; and second, principles regarding the management and governance of Member Companies including the selection, vetting and proper training of personnel.

The UN Guiding Principles on Business and Human Rights:

UN Special Representative John Ruggie proposed a framework on business & human rights to the UN Human Rights Council in June 2008, resting on three pillars: the state duty to protect against human rights abuses by third parties, including business; the corporate responsibility to respect human rights; and greater access by victims to effective remedy, both judicial and non-judicial. Unanimously endorsed by the UN Human Rights Council in 2008, these principles form the UN “Protect, Respect and Remedy” Framework.

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies (WA):

The WA was established in 1996 in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. The aim is also to prevent the acquisition of these items by terrorists. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

Introduction

Five years ago, most experts would list around half a dozen countries with offensive cyber capabilities. However, according to the former U.S. Director of National Intelligence, James Clapper, "as of late 2016, more than 30 nations are developing offensive cyber attack capabilities."[1] In addition to military and intelligence agencies, law enforcement agencies contribute to the demand for cyber capabilities as more countries establish policies and institutions focusing on 'lawful hacking.'[2] The demand covers the full spectrum of activities ranging from software vulnerabilities to malware exploits and payloads.[3] To complete the picture, reports suggest demand also comes from private companies seeking support from specialized cybersecurity companies to defend or even retaliate against cyber attacks.[4]

A growing global market of private cybersecurity companies is meeting this demand from governments and private actors. Conventional private military and security companies (PMSCs) are expanding their activities into this area.[5] They either build their own cybersecurity teams or acquire smaller, boutique firms specializing in cyber tools and services.[6] Private security contractors are not a phenomenon unique to cybersecurity but companies are easier to establish in this field because capabilities primarily depend on brains and a computer rather than conventional weaponry. Barriers to entry into the business are therefore comparatively low. [7]

Private sector cyber activities pose a range of challenges for good security governance. Most conventional PMSCs operate on land or at sea. Such conventional PMSCs' operations may bring them in close physical proximity to a conflict zone. However, most hacking operations are based on remote access and this implies that cybersecurity companies are far removed from the target their services may help reach. Moreover, because physical location is less important and because some of these companies consist only of a few dozen employees, it is more difficult to ascertain the jurisdiction that pertains to their cyber activities, making accountability and monitoring of compliance with international and national legal requirements an additional challenge. It has been suggested that some private companies tried to avoid such compliance through so-called "jurisdiction-shopping".[8]

These challenges are not unprecedented. International PMSCs that provide physical guarding or other services across different jurisdictions also pose challenges for State regulation. There is no international instrument on PMSCs and the normative and 'good practice' frameworks developed indicate a dearth of guidance for governments. Cyberspace therefore amplifies, rather than revolutionizes these challenges. However, an even more difficult conundrum is posed by the effect of the unique characteristics of cyber operations in blurring the traditional distinctions between legitimate and illegitimate activities for private sector participation and even between peace and war.

To date, most cyber security activities have involved the collection of data, rarely anything close to approximating the use of force. As a result, the attention to private actors in this space has largely been driven by human rights concerns. However, there is a governance gap concerning private actors contributing to or engaging in risky cyber activities including offensive cyber operations (such as 'hack backs'). The effects of cyber operations usually fall below the threshold of an "armed attack" or even "use of force" under international law. Consequently, there is far more uncertainty regarding state responsibility for private sector cyber activities and what constitutes appropriate behaviour, including in the use of private cybersecurity contractors.[9]

This paper seeks to identify the emerging and expanding gaps in the governance of private cybersecurity companies and activities and to explore ways forward and policy options for governments. The first section of the paper will explore the characteristics of typical cyber operations and challenges related to their conduct by private actors. Section two will address the governance challenges around cybersecurity and three main departure points for regulation: the fact that geographic scope does not limit cybersecurity companies, that cyber operations can slide from defensive to offensive very quickly; and that cybersecurity services are often exported for the purpose of (or with the knowledge they will be) violating human rights. This section will also integrate perspectives of international law. Section three will lay out suggestions for policy options in relation to international law and existing international normative frameworks. In conclusion, the paper will offer a framework and way forward as food for thought in order to address cybersecurity operations in relation to PMSCs.

1. The Conundrum: Cyber Operations and the Role of Private Actors

PMSCs are a major player in the cyber operations landscape. The nature of the services they provide for governments blurs roles and responsibilities of public and private sectors. Moreover similar to many conventional PMSCs, there is often a very close relationship between government and industry in cybersecurity. A growing number of governments develop their own cyber capabilities and train their military and intelligence staff accordingly. Some leave government for the private sector, with more and more companies counting ex-government employees among their staff. The result is a situation in which private actors frequently have the most sophisticated cyber capabilities and employ them on behalf of governments or even in their own defence. Addressing the emerging gaps in the governance of private cybersecurity companies requires an understanding of intertwined technical, legal, and policy challenges. This section seeks to outline the unique "geography" of cyberspace, characteristics of cyber operations, and the novel ways in which private actors are engaging in this space.

While malicious 'hacks' or 'cyberattacks' are often depicted in the media as instantaneous events, a typical cyber operation occurs in stages often drawn out over time.[10] The early stages involve reconnaissance, for example, to identify how to gain access to a system in the first place. Next is preparation, including probing target networks to identify the data of interest to the attackers, identify vulnerabilities in those networks (i.e. flaws in the computer code that create a security weakness), and develop code that exploits those vulnerabilities in order to gain access without being detected. An attacker might be searching for a specific target, such as valuable intellectual property or access to industrial control systems, or simply exploring potential opportunities without a clear objective. The attacker then delivers the code (for instance, through a "spear phishing" email designed to trick a target into accepting the malicious code), gaining access to the target network. At this point the attacker will often spend time (in some cases months) inside the network developing alternative routes of access and ways to take control of the target networks and systems by installing other malicious code, and mapping out the network to locate the systems or data that are the real target of the attack.

As a typical cyber operation progresses through these stages, the attacker moves closer and closer to critical data and functions until ultimately a "payload" (weaponized code analogous to the warhead of a missile) is delivered that either steals data or attacks the integrity of data (by altering or deleting it) or functions to create some adverse effect – from disabling a network to destroying information to generating effects in the physical world by manipulating physical systems that are increasingly connected to the Internet to facilitate maintenance, monitoring, etc. (such as industrial control systems). In the most extreme cases a payload could cause physical damage or destruction. The Stuxnet malware, for example, disrupted the functioning of centrifuges used at the Natanz nuclear facility in Iran.[11]

For the purposes of describing and categorizing cyber capabilities and cyber weapons a useful framework is the "PrEP Model." In this model, three components comprise a cyber capability:[12]

- Propagation methods: "the means of transporting malicious code from origin to target" (e.g., a spear-phishing email);
- Exploits: software "to enable the propagation method and payload's operation, allowing the attackers to take control of a piece of software or entire computing system";
- Payload: "code written to achieve some desired malicious end such as to delete data or manipulate industrial control systems."

Mapping out the stages of cyber operations helps illuminate five key characteristics of cyber operations relevant to private sector governance:

First, the vast majority of cyber operations are conducted through the Internet, so each of these stages, including delivering payloads, can be undertaken remotely from across the world. Cyber capabilities thus allow for remote participation in activities ranging from law enforcement surveillance to offensive military operations in war. Rather than think of the "frontline" in a conflict in terms of physical proximity to an adversary, it is more useful to conceptualize cyber operations in terms of proximity to the critical data and functions of a system. Private actors can be on the frontline in contemporary conflicts without leaving their home state. They can likewise participate remotely in foreign law enforcement activities or assist repressive governments with targeting their citizens.

Second, cyber operations are usually modular in nature. There are specific kinds of tools and capabilities designed to operate at each stage. This modularity allows for the commodification of certain stages of cyber operations. Grey markets cater to the demands of governments for discovered cyber vulnerabilities, exploits, and even weaponized code. Some tools used in the beginning stages of an operation to identify vulnerabilities and exploit a network are essentially the same as commercially available capabilities and services used by legitimate actors to improve security.

Third, cyber operations allow for a continuum of malicious effects. These range from the isolated disruption of a network or theft of data from a personal computer to catastrophic damage caused by an attack on a nation's critical infrastructure. Only in the rarest cases have cyberattacks even come close to the latter, which would require sophisticated capabilities and extensive intelligence. Nevertheless, there is significant potential for cyberattacks that, even if they do not cause physical damage, could cause severe disruption or harm to a target. For instance, targeting a country's political institutions or financial system with even a relatively minor cyber operation could cause significant ripple effects impacting the economy and even public safety.

Fourth, cyber operations for purposes of intelligence collection, stealing information, or creating effects, up to and including physical destruction, may all be virtually indistinguishable until the point at which a payload, the piece of code that actually determines if data is stolen, manipulated, or destroyed, is delivered. It is the delivery of a payload that actually determines what the access to a system is exploited for and thus differentiates an offensive attack from other kinds of intrusions.

Fifth, the ambiguous and modular nature of offensive cyber operations similarly complicates the task of defining the scope of "defence" in cyberspace. Defence is often traditionally thought of as purely passive measures – in cyberspace this means virtual defensive barriers in the form of firewalls or encryption that aim to secure data and protect networks against external attacks. But the extended process of an offensive operation is mirrored by the spectrum of options available to the defender. This includes a range of measures, such as measures designed to identify the location of stolen data, to the borderline offensive, such as "hacking back" into an adversary's network in retaliation.[13] There is growing evidence that private corporations are offering a range of aggressive defensive services to other corporations transnationally.[14] For instance, a corporation may hire a contractor abroad to "take down" a network used by a malicious actor in another country to conduct operations.

Cyber capabilities have had, to some degree, a democratizing effect on the ability to wield power and participate in conflict – in particular by cybersecurity PMSCs. The bar to the development and use of cyber capabilities is low; private companies are able to enter this market relatively easily. Compared to conventional military capabilities or even traditional private security capabilities, basic cyber capabilities are, generally speaking, cheap and easy to acquire. Certain components can be reproduced and repurposed for a vast range of malicious activities. Cyber weapons deployed by states have been reverse-engineered and retooled by less sophisticated actors, further lowering the barriers to entry in this space.[15]

2. Cybersecurity Governance Challenges

The lines drawn between legitimate and illegitimate private sector activities in the physical world rely largely upon tangible and visible distinctions – between weapons and commercial goods, military and civilian activities, foreign and domestic activities, etc. Even if, in practice, the enforcement of such distinctions is far from perfect, there is a common, objective basis of understanding or convergence upon norms. Cyberspace, however, has the effect of blurring these lines.

2.1 Rethinking Conventional Governance Reference Points: The Grey Space of Cyber Operations

- **Geographic scope of cyber activities:** The Internet allows for most cyber operations to be launched from virtually anywhere in the world (with an Internet connection). Private contractors can engage in surveillance activities on behalf of a repressive regime or even participate in an armed conflict abroad without leaving their home country. Not only does this make it difficult to control the export of cyber tools and capabilities, it makes it difficult to distinguish their development and production from their employment. A contractor could be located thousands of miles away from the theater but nevertheless be on the "frontline" of offensive cyber operations.

- **Functional distinctions of a cyber operation:** The lack of geographic constraints creates a potential "slippery slope" from providing technical support to conducting defensive or even offensive cyber operations. This blends together the various functions that traditionally characterize private contractors' participation in armed conflict – from logistics support to consultants to participation in military operations. Private contractors in support roles might quickly find themselves embroiled in military operations if their networks are targeted. Likewise, a contractor undertaking reconnaissance activities could easily shift to delivering a payload to a target network. The potential to move between these roles makes it possible for civilians to engage in activities that bring them closer to directly participating in hostilities, without a commensurate level of oversight.

- **Dual-use nature of cyber capabilities:** Conventionally, the term "dual-use" applies to the potential use of a tool for both civilian and military purposes, for example, in the context of a nuclear program. With respect to cyber tools, this challenge may also arise. At the same time, "dual-use" has taken on an additional meaning in the context of cybersecurity. Companies export their products to law enforcement and intelligence agencies around the world. Most of these agencies use them for legitimate law enforcement and intelligence activities in line with international human rights law. However, some companies have also exported their products to governments known to regularly violate human rights. "Dual use" in this context has therefore become used to describe these tools' use for both legitimate and illegitimate – from an international human rights law perspective – purposes. A third dimension is that the same tools and techniques for identifying and exploiting vulnerabilities in information and communications technologies (ICTs) could be used to either improve their security or attack them thereby either contributing to cybersecurity or cyber insecurity.[16]

In short, the ability to cordon off certain spaces of private sector activity necessary for effective regulation – like producing or exporting cyber weapons, conducting surveillance on behalf of a repressive regime, or participating in armed conflict – is significantly attenuated in cyberspace. Yet the blurring of these lines is less a revolutionary challenge than an extension of broader trends from the physical world in the shifting roles and capacities of a global market for security products and services. The rise of transnational markets for military capabilities and globally-operable PMSCs in the post-Cold War international environment engendered similar pressures on traditional approaches to governance.[17] The private sector developed unique security capacities tailored to the demands of both contemporary military conflicts and globalized commercial activities. Simultaneously, the ability to outsource or contract for security services in this globalized market created new ways for contractors and those hiring them to circumvent national regulations and accountability.[18]

2.2 Regulatory challenges

National regulatory and governance mechanisms face a persistent challenge in overcoming the practical and technical complexities of cyberspace. However, there is a more fundamental challenge posed by the unique characteristics of cyber operations: They blur traditional distinctions critical to the foundation of governance of private actors, including between offensive and defensive capabilities, between legitimate commercial as well as law enforcement activities and illegitimate ones, abusive behaviour by governments, and even between peace and armed conflict.

Central to international law, including the application of International Humanitarian Law (IHL), is the distinction between situations of armed conflict and situations prior to it – *jus in bello* and *jus ad bellum*, respectively. There is a growing consensus that cyber operations with effects equivalent to an armed attack should be treated as such under international law, and thus a cyberattack could reach the threshold of an "armed attack" triggering the right to self-defence.[19] For example, if an air traffic control tower is targeted with a cyberattack and a plane crashes as a result, the effect is the same as the plane having been shot down.

However, applying this threshold in practice is challenging. Cyber operations allow for a range of disruptive or harmful effects that fall below the threshold of an "armed attack" or even an unambiguous "use of force." Nearly all cyberattacks to date fall within this range, and this vast space of low-level malicious activity is precisely where the bulk of private sector participation in cyber conflict occurs. These low-level cyberattacks are increasingly consequential for states, as malicious cyber activities can have cumulative impacts over time even more harmful than an armed attack, without overtly crossing this threshold and triggering the justification for self-defence under international law. The rules and norms for this space remain weak even for state actors, much less private actors in their territory or under their employment. If fully elaborating these intertwined legal and political issues lies beyond the scope of this paper, it remains an important area for further work.

The specific concern of this paper is how this normative grey space of cyber operations contributes to the emerging gaps in governance of private actors in cyberspace. Determining what rules apply to the conduct of cyber operations, and, in turn, that should apply to private actors participating in them, depends to some extent on being able to differentiate which context the operation is occurring in. Because of the ambiguity of offensive operations, private contractors may be conducting activities, such as probing critical infrastructure, that could put them in a position to conduct extremely risky or harmful attacks without a level of oversight commensurate with these risks. As a case in point, in 2016 the U.S. Department of Justice indicted seven Iranian hackers – believed to be proxies for the Iranian government and Islamic Revolutionary Guard Corps – for hacking into and attempting to take control of industrial control systems operating a small dam in New York as well as launching DDoS attacks on U.S. financial institutions.[20] The thin lines between stages create the potential for private actors to quickly move between roles – the difference between conducting espionage and launching a disruptive or destructive attack may simply be a few lines of code.

The commodification of cyber operations creates a situation in which private corporations may be providing capabilities and services for abusive activities by repressive governments or even offensive military operations – potentially without even knowing. Or they may be actively supporting and conducting these operations while being treated as a purveyor of commercial security tools. More than just a challenge of regulating the export of dual-use capabilities, the problem here is how these dual-use capabilities and activities blend together the worlds of commercial activity, law enforcement, and national security.

Finally, the blurred lines in this space also complicate the task of defining boundaries of legitimate defensive behaviour for private actors. States may choose to determine the services that can be offered by a private actor differently depending on the context. A private contractor serving the military might engage in a countermeasure against an attack viewed as perfectly legitimate and proportional under international law. But that same measure, if done independently to defend its own networks, could be a violation of the state's domestic laws governing private actors.

There is an ongoing, contentious debate in the United States and elsewhere over the scope of defensive activities that should be considered legitimate for private actors securing their own networks from malicious activity. This debate again underscores the challenge presented by the blurred domestic and international contexts: Private actors are undertaking far more aggressive, offensive activities in the service of governments but when they themselves are targeted their response options are significantly curtailed. The distinction between domestic and foreign territory/jurisdiction has become less useful as a guiding principle given that most hacking is carried out remotely. For example, under domestic U.S. law, the Computer Fraud and Abuse Act criminalizes the "unauthorized access" of a computer system regardless of the purpose (and comparable prohibitions are found in many countries).[21] At the international level, however, the U.S. government has been forcefully defending the position that such unauthorized access for the purposes of intelligence collection is not prohibited under international law.[22]

The collective effect of these unique considerations of cyber operations is to call into question some of the fundamental assumptions that have been translated onto this space. Private sector cyber activities cannot easily be partitioned into different silos – export controls, regulations on private military contractors, etc. A serious effort is needed to adapt existing mechanisms to the cyber context.

3. Policy options

This paper has highlighted some cybersecurity tools and services and how the characteristics of cyberspace amplify existing challenges for governance posed by the role of PMSCs in this space. These can be dealt with in part by updating and adapting the various initiatives that have emerged in response to the privatization of security in the physical world. A number of existing international governance frameworks are instructive and may be useful for States seeking to manage the risks associated with the activities of private cybersecurity companies/actors. In other cases, cyber activities fall into a new area of grey space calling for a new initiatives and tailored framework. As a first step in this direction, the following section outlines a set of recommendations as food for thought.

3.1 Concretising the applicability of international law in cyberspace

Existing international law is a good starting point for a comprehensive framework to manage private sector cyber activities. While one may be tempted to call for new laws or policies whenever a new technology emerges, it is not necessary to reinvent the wheel. In fact, some areas of law already explicitly take into account the emergence of new technology. For example, Article 36 of the 1977 Geneva Additional Protocol I states that "[i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."[23]

To remove any doubt, the international community has expressed its view repeatedly over the past several years that existing international human rights law applies online as well as offline. In 2012, the UN Human Rights Council affirmed "that the same rights that people have offline must also be protected online."[24] The 2013 consensus report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security states that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."[25] A few countries still contest that existing international law applies but the overwhelming majority of the international community has moved on to discuss how, not if, existing international law applies.

However, how existing international law applies online remains a challenging translation exercise. This is particularly the case for the type of effects that fall below the threshold of "use of force" and "armed attack," and on the issue of States' responsibility for cyber activities within or emanating from their territory. Fully resolving the complex legal and policy issues surrounding private sector cyber activities may eventually require formal international agreements. But serious impediments stand in the way of international cooperation toward even informal norms of State behaviour, much less rules governing their relationships with private actors. The incentives for States to continue to exploit the cyber domain for their own interests weigh heavily against the desire for norms, particularly in light of the inevitable challenges with verifying any commitments in this space. Solutions to the governance gap are therefore more likely to come from multi-stakeholder initiatives and approaches that have been successful in making progress in similarly contentious areas.

3.2 Adapting existing initiatives

As previously discussed, certain aspects of this governance challenge are evolutionary, rather than revolutionary in nature. They reflect an extension or amplification of trends characterizing the shifting roles and capacities of the private security sector in delivering physical security in the post-Cold War international environment. A range of initiatives emerged to meet these modern challenges, tailored to a context in which private corporations had developed military capabilities even on par with some states and powerful multi-national corporations had become major players in shaping norms of behaviour - as is the case with cyberspace. By pursuing pragmatic objectives to create incentives and promote standards of responsible conduct and accountability of the private sector, these initiatives have been able to make progress despite fundamental differences in states' views and interests that precluded convergence upon formal commitments or institutions.[26]

Together with existing international law, these initiatives and voluntary agreements provide a foundation for managing specific aspects of private sector cyber activities within a broader approach to this space. These fall into two categories: Initiatives designed to harmonize national approaches with international legal obligations, norms and good practices, including the Wassenaar Arrangement and the Montreux Document, and multi-stakeholder initiatives designed to promote human rights and corporate social responsibility (CSR) in a transnational context, including the International Code of Conduct for Private Security Service Providers, and the United Nations Guiding Principles on Business and Human Rights.

3.2.1 Harmonizing National Approaches with International Good Practice

An uneven international regulatory environment contributes to the challenge of governing cyber activities. Even when states do have clear laws and regulations for the provision of cybersecurity products and services, the transnational character of cyberspace makes it easy to circumvent these and for actors to engage in 'jurisdiction-shopping'. For instance, corporations in jurisdictions with strict limits on the type of activities they can conduct in response to cyberattacks can outsource these activities to more permissive jurisdictions. Initiatives and mechanisms are needed that can promote convergence upon common rules and standards for the various kinds of private sector activities described here.

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies provides the most prominent example of ongoing efforts to adapt existing initiatives to specific cyber activities—and demonstrates some of the pitfalls of such efforts. The Arrangement was established in 1996 to harmonize countries' national approaches to regulation and control of exports of dual-use technologies and weapons. It broadened the scope of prior multilateral export control efforts, providing a foundation for convergence internationally on identifying, defining, and controlling those items posing significant risks, including complex, dual-use technologies.

Following pressure by various human rights NGOs, such as Privacy International, and press coverage, such as the Wall Street Journal's Surveillance Catalog,[27] the French and the British governments proposed updated export controls to cover intrusion software and network surveillance systems to be added to the Wassenaar Arrangement, which were agreed upon in 2012. These changes were heavily criticized by the cybersecurity industry for threatening to impede legitimate security research such as sharing information on vulnerabilities in products.[28] Subsequently, exemptions for tools and information used in security research were agreed upon in December 2017 designed to minimize the potential impacts on legitimate activities.[29]

Some discussion of the role and responsibilities of private cybersecurity companies has also taken place in the context of the Montreux Document Forum. The *Montreux Document On Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict,* is the outcome of a process initiated in 2006 by the Swiss government and International Committee of the Red Cross, which aimed to elucidate states' obligations under international law with respect to their regulation and oversight of PMSCs. The Montreux Document delineates states' obligations based on their different relations to PMSCs – those under their direct employment or operating out of or within their territory. Particularly in light of the fact that many of the major traditional PMSCs are leading the way in developing and employing cyber capabilities, the Montreux Document provides an effective starting point for extending the guidance to states to include cybersecurity activities by PMSCs operating from or in their territory or under their employment. Home States (where PMSCs are headquartered or based) as well as Contracting States (who hire or contract PMSCs) are particularly addressed under the Montreux Document. As the Montreux Document is meant to be a practical guidance tool and does not represent a one-size-fits-all approach, governments can adapt the good practices contained therein for their specific context.

Drawing on the Montreux Document good practices, adapting and updating these initiatives to cover cybersecurity services and capabilities should aim to:

- Focus on using notification requirements as part of national export control regimes requiring companies to notify the government of specific exports so that governments have a more detailed picture of the emerging market and can develop more tailored policies;
- Continuously update export controls and licensing requirements for cybersecurity service providers and vendors of cybersecurity capabilities;
- Distinguish the different modules of a cyber operations (namely weaponized payloads) which should be subject to greater restrictions, for the purposes of export controls;[30]
- Reinforce and clarify states' commitments under international law and their applicability to cyber activities;
- Ensure proper oversight and control of PMSCs conducting cyber operations, such as by encouraging states to extend their regulatory requirements for PMSCs to include specific provisions for cybersecurity services;
- Encourage governmental mechanisms to monitor how cyber operational skills and expertise are employed by former government personnel who move to the private sector.

3.2.2 Promoting human rights and corporate social responsibility through multi-stakeholder initiatives

States' authority and control over and within cyberspace has inherent limits. The fact that cyberspace – and the physical infrastructure, hardware, and software that comprises it – is to a large extent built and maintained by private corporations gives the latter significant power. The viability of norms and accountability of corporations to prevent risky or destabilizing behaviour and the abuse of cybersecurity products and services to violate human rights will inevitably depend to some extent on the ability to foster internal company policies as well as external market incentives to shape private sector behaviour. Business and human rights as well as CSR initiatives can play an essential role in creating and shaping these incentives.

Here, too, there are existing initiatives pertaining to activities in the physical world that could be extended to cyberspace. The Swiss-led initiative that led to the Montreux Document also produced the International Code of Conduct for Private Security Service Providers (ICoC)– a complementary initiative with a multi-stakeholder oversight mechanism aimed at the industry itself rather than governments. The ICoC includes a wide range of standards and principles for the responsible provision of private security services which can be applied to cyber activities. The ICoC articulates principles regarding the conduct of private security company personnel based on international human rights and humanitarian law standards including rules on the use of force, sexual violence, human trafficking and child labour. Secondly, the ICoC contains principles regarding the management and governance of companies including the selection, vetting and proper training of personnel. With clients requiring compliance with the ICoC and membership in its oversight mechanism (the ICoC Association), this agreement addresses the "supply" side of the equation, fostering incentives within the industry to engage in responsible conduct and undertake commitments to respect human rights. These principles could be clarified and extended to apply to cyber activities of many of these same PMSCs.

Other existing high-level frameworks can be applied to private cybersecurity companies. Namely, the Guiding Principles on Business and Human Rights, also known as "the Ruggie Principles" and developed by Special Representative of the UN Secretary General, John Ruggie, provide a useful road map for mitigating human rights risks associated with the services provided by such companies. Developed in consultation with governments and industry, the Guiding Principles detail a multi-step process that the UN Human Rights Council endorsed in 2011.[31] This 'Protect, Respect and Remedy' framework focuses comprehensively on the roles and responsibilities of governments and industry alike to protect individuals' human rights.

The Ruggie Principles provide a common foundation upon which specific approaches to human rights due diligence can be tailored to the cyber context.[32] While this framework is more general in scope than the ICoC, it is nevertheless useful to address the specific human rights concerns around PMSCs carrying out activities in cyberspace. This may in particular include the responsibility of PMSCs to respect human rights by ensuring that their services and products are not abused to infringe and violate human rights, as well as to verify the end-use of their products, and to provide certain remediation measures in case of adverse human rights impacts.

These initiatives should be adapted and updated to:

- Develop frameworks for ensuring human rights risks are adequately addressed in the export or provision of cybersecurity tools and services;
- Encourage companies to develop more robust know-your-customer processes focusing on the end user;
- Extend the same kinds of rules and precautions pertaining to contractors' participation in military operations to cyber operations in service to governments;
- Translate corporate risk management practices, such as proper vetting of personnel and testing of capabilities, to the context of cybersecurity activities;
- Explore common metrics, certification processes, and standardized procedures for qualifying companies and personnel to engage in certain cybersecurity services or develop specific capabilities.

Taken together, these initiatives can be adapted to help motivate both states and the private sector to address in a complementary manner the human rights and humanitarian concerns surrounding cyber activities. The benefit of the Montreux Document and ICoC is the focus on international humanitarian law and international human rights law. In contrast, the Wassenaar Arrangement is not a human rights-focused institution as it evolved from efforts to control technology exports during the Cold War as part of strategic competition. For this reason and because of its more collaborative approach and culture, the Montreux Document and the ICoC seem more promising as potential comprehensive and sustainable institutional arrangements to manage the activities of private cybersecurity companies.

Ultimately, all existing institutions and processes have a specific focus and path dependence that may hamper an effective arrangement to manage the activities of private cybersecurity companies. For example, the Montreux Document's historical focus on activities occurring during armed conflict and international humanitarian law may distract from the particular and pressing challenges posed by the effects of offensive cyber operations below the threshold of 'use of force' and 'armed attack' that drove the Wassenaar discussions.

Finally, it's worth reflecting on a few lessons from the development of these initiatives that may help anticipate and preempt challenges that will likely emerge with their adaption to the cyber context. The historical experience with private security regulation suggests that a clear roadmap for resolving the political and legal issues surrounding these activities is unlikely to emerge. Rather, as Deborah Avant argues, governance may be better understood as a *process* rather than an outcome.[33] The ICoC process was characterized by the steady fostering of "pragmatic networks" that brought together the relevant stakeholders – states, civil society, and both the supply and demand sides of private sector security services. By acknowledging the reality that some degree of risk from contractors' activities was inevitable, these initiatives were able to identify risk management measures that were both reasonable and practicable. Modest, initial steps and interim agreements created a foundation for more robust efforts. This experience bears several important lessons for a similar pragmatic approach to governing cybersecurity operations carried out by private cybersecurity companies:

- **Start from a common foundation:** Private security activities have always been contentious internationally. Fundamentally conflicting views toward the legitimacy and legality of PMSCs created an impasse for efforts at the UN and elsewhere, with some states arguing that any effort to regulate PMSCs would legitimize "mercenary" activities. The Montreux Document was able to overcome these differences and bring together states at opposite ends of the spectrum by starting with the very modest objective of taking stock of existing international law applicable to PMSCs, and explicitly committing to limit the scope of the initial discussion.[34] The same foundation in international law exists for cyber activities, even if its applicability in specific cases remains contested. Moreover, states share a common interest in preventing the expansion of private sector cyber activities that could pose systemic risks, such as unrestrained "hacking back" or the proliferation of cyber weapons.

- **Consider stopgap solutions:** Given the diminishing prospects for international cooperation toward cyber norms, the pursuit of formal institutions and mechanisms might prove futile. Stopgap measures can make real progress toward improving the reality on the ground. A "soft law" approach should not necessarily be viewed as an inevitable concession to security providers. Arguably the PMSC industry's participation, rather than resulting in the watering down of standards, led to the adoption in some cases of best practices and standards that exceeded those of legal requirements. The industry's participation had an overall effect of increasing security providers' investment in norms, creating a "self-reinforcing" legitimacy.[35]

- **Calibrate expectations:** Finally, it is important to start with realistic expectations that recognise the limits of state control over this space. In some cases, a realistic objective may be to manage and minimize risks rather than eliminate them altogether. The initiatives governing PMSCs have not resolved the controversies surrounding their activities – nor were they intended to do so. The persistence of governance challenges was recently underscored by a UN expert panel, which found pervasive gaps in national legislation and recommended the creation of a legally-binding treaty regulating PMSCs.[36]

5. Conclusion: Towards a Framework for Defining Responsible Conduct in the Grey Space of Cyber Operations

Existing mechanisms can only go so far. A major challenge to date remains the opaque nature of this market and lack of information to understand its dynamics. As more information becomes available, a new framework may be needed to help navigate this grey space, to guide both national approaches and international normative efforts. Precisely because of the characteristics of cyber operations, the legal distinctions of *jus ad bellum* and *jus in bello* have clear limitations. Rather, an approach to minimizing risks must extend beyond these lines. For instance, when exercising oversight over contractors, it may be necessary for states to treat any private actor in a position where it could *potentially* deliver a weaponized payload as if it were doing so because the ease of moving between roles in offensive operations - even though an actor conducting cyber espionage may not be viewed as conducting military operations.

Recognising how cyberspace has blurred (or erased) some of the traditional distinctions between conventional PMSCs and private cybersecurity companies, the aim of this concluding section is to identify those distinctions upon which norms and initiatives should be built. Three general directions to orient policy approaches are proposed. The question of what specific rules should apply to different activities, and what kinds of mechanisms and modalities these could be anchored in, should flow from a framework for differentiating and prioritizing the various areas of private sector activity of potential concern.

5.1. Expand the scope of activities that should be considered inherently governmental functions

Identifying the key distinctions that should delineate the spaces of legitimate versus illegitimate engagement by private actors should start with those activities posing the most pressing concerns. Offensive cyber operations have unique, intrinsic risks that should engender significant caution even among the most sophisticated operators. The manipulation of a network could have unpredictable effects, including collateral damage and other unintended consequences. There is a need to identify certain kinds of cyber operations or specific stages of operations that should either be completely off-limits for private actors or only conducted under direct and strict supervision by governments. The need for governments to include a strict determination of services is not a new concept – the Montreux Document recommends this with respect to conventional PMSCs. Cyber PMSCs should be held to the same standard.

Naturally, the most extreme caution should be with respect to the delivery of *weaponized payloads*. A payload that targets the integrity of data or systems for destructive or disruptive effects could have the potential impact equivalent to an “armed attack” in the physical world (e.g. by targeting industrial control systems). There is an essential distinction, then between a private actor manipulating the integrity of data or delivering such a weaponized payload and one simply exfiltrating information from a network.

This relates to a further distinction in the *targets* of any offensive operation. There are certain targets that, due to their sensitivity and the potential risks of targeting them, should be considered unequivocally off-limits for private actors even with respect to intrusion or reconnaissance.

For instance, the potential consequences and ripple effects of even a minor impact on nuclear infrastructure would be of serious enough concern to rule out any justification for attempted intrusion by private actors (potentially even governments).

5.2. Build a firewall between those activities that should be on and off-the-table for private actors

Robust international norms to prevent risky and destabilizing behaviour are needed. Yet circumscribing the space for private sector engagement also demands an effort to more clearly define the rules of the road for private actors below the upper limit. The delivery of a payload – whether a weaponized payload or one that steals information – inevitably entails a higher level of risk than developing one or potentially carrying out an intrusion to develop permanent access, and the latter realistically are not going to be ruled out for private actors. Of course, this is not to say that breaking into networks should simply be considered a 'civilian' activity, but neither is it necessarily an attack in its conventional sense in international affairs.

Further, there is a need to account for the opportunities that cyber capabilities create for new kinds of effects that fall short of the threshold of "use of force" or "armed attack" but are nevertheless harmful and potentially destabilizing. Thus the *type of effects* is another important distinction – specific rules for such activities may be needed compared to traditional military effects. For instance, there are potentially kinds of cyber operations to conduct disinformation campaigns that might not be permitted for private contractors.

5.3. Define responsible and professional conduct for legitimate cybersecurity services

Finally, while it is essential to prevent risky and destabilizing private sector cyber activities, it is important to recognize the legitimate need for corporations to defend themselves. Stepping away from the context of state activities, there is a need for convergence internationally on norms that would clarify the distinction between legitimate and illegitimate cyber activities by private actors in defence of their own assets. There is good reason to differentiate the use of a limited measure like a "beacon" attached to stolen data that sends information back to the victim on its location from a military cyber operation. However, locating on the spectrum of potential defensive activities precisely where the line is crossed is difficult.

The network boundary remains an important distinction. Activities by a defender with impacts outside of its network inevitably entail an additional set of risks and considerations – collateral damage, escalation, and the potential for transnational impacts – than activities solely inside the defender's network. Yet, as in the physical world, the technical characteristics of an activity should not be the *only* determinant. The circumstances under which an activity is taken (i.e. whether it is taken out of necessity in response to an attack) should also weigh in.[37]

Complementary efforts leveraging the range of key stakeholders – including both the supply and demand sides of cybersecurity services – shape the incentive structure for security providers to encourage responsible conduct, minimize risks and ensure accountability. These efforts could draw parallels from the experience of the Montreux Document and ICoC. Furthermore, a dedicated CSR effort for cybersecurity services analogous to ICoC but specifically aimed at the spectrum of defensive cyber activities outside of the context international conflict could be explored.[38]

Taken together, these suggestions comprise an ambitious agenda for private security governance efforts. In light of the objectives and activities referenced above, it is clear that no existing single model or institution captures the complexity of private sector cyber activities. A general question is whether the scope of existing institutions and normative frameworks such as the Montreux Document and ICoC can be expanded to effectively fill the gap in the current governance architecture for private cybersecurity companies or whether a new mechanism needs to be developed. The future will tell if policy-makers will choose the path of expanding the scope of existing institutions or eventually create a stand-alone initiative or both. At this point, there are clear gaps in understanding, monitoring, and nudging the market and that more can be done to strengthen responsible behaviour by states and companies alike.

ABOUT THE AUTHORS

Tim Maurer

Tim Maurer is Co-director of the Cyber Policy Initiative at the Carnegie Endowment for International Peace. Since 2010, his work has been focusing on cybersecurity, human rights in the digital age, and Internet governance. Maurer is a member of several U.S. track 1.5 cyber dialogues and has contributed to the Global Commission on the Stability of Cyberspace, the Global Commission on Internet Governance, the Freedom Online Coalition's working group "An Internet Free and Secure" as well as the OSCE's cyber confidence-building efforts. In January 2018, Cambridge University Press published his *Cyber Mercenaries: The State, Hackers, and Power*, a comprehensive study examining proxy relationships between states and hackers. He holds a Master in Public Policy from the Harvard Kennedy School.

Wyatt Hoffman

Wyatt Hoffman is a senior research analyst with the Cyber Policy Initiative and the Nuclear Policy Program at the Carnegie Endowment for International Peace. His research focuses on private sector cyber capabilities, emerging technologies, and the intersection of nuclear weapons and cybersecurity. He is a graduate of Carnegie's James C. Gaither Junior Fellows Program and was a Rotary Global Grant Scholar in Peace and Conflict Prevention and Resolution at King's College London's Department of War Studies.

Endnotes

[1] James R. Clapper et al. (2017): Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States, available at https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf

[2] Susan Hennessey (2016): Lawful hacking and the case for a strategic approach to "Going Dark", available at https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/

[3] Lockheed Martin, The Cyber Kill Chain, available at https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[4] Joseph Cox, "Revenge Hacking is Hitting the Big Time," The Daily Beast, Sept. 19, 2017. https://www.thedailybeast.com/inside-the-shadowy-world-of-revenge-hackers

[5] See, for instance, Aliya Sternstein, "Here are the Companies That Won a Spot on $460M Cyber Command Deal," Nextgov, May 23, 2016, available at https://www.nextgov.com/cybersecurity/2016/05/cybercom-inks-460m-operations-support-deal-booz-saic-others/128523/; for examples of "traditional" PMSCs offering cybersecurity services see Northrop Grumman, available at http://www.northropgrumman.com/Capabilities/Cybersecurity/Pages/default.aspx; and Lockheed Martin, available at https://www.lockheedmartin.com/en-us/capabilities/cyber.html

[6] Tim Shorrock (2009): Spies for Hire: The Secret World of Intelligence Outsourcing, Simon & Schuster, 2009, available at http://www.simonandschuster.com/books/Spies-for-Hire/Tim-Shorrock/9780743282253

[7] Mattathias Schwartz, Cyberwar for Sale, 4 January 2017, The New York Times Magazine, available at https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html. For example, the company Hacking Team, headquartered in Italy, has become near-synonymous with a growing number of small companies that have sprung up over the past two decades often consisting of former government employees. Counting less than 50 employees, Hacking Team has sold its services to law enforcement and intelligences agencies in several countries. The company attracted widespread criticism for providing services to clients commonly known to infringe human rights. This draws attention to one of the specific governance challenges associated with cyber tools and services.

[8] In 2013, after criticism of its business grew in the United Kingdom, Gamma International tried to shift its exports to other jurisdictions such as Switzerland: https://privacyinternational.org/blog/1183/gamma-attempting-export-surveillance-tech-out-switzerland.

[9] Herbert Lin (2011): Responding to Sub-Threshold Cyber Intrusions: A Fertile Topic for Research and Discussion, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity, Georgetown Journal of International Affairs, 2011, Georgetown University Press, available at https://www.jstor.org/stable/43133821

[10] These stages are often referred to collectively as the "cyber kill chain." See Lockheed Martin, The Cyber Kill Chain, available at https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html; for further discussion of the stages of cyber operations, see Herbert Lin (2010): Offensive Cyber Operations and the Use of Force, Journal of National Security Law & Policy, Vol. 4, No 63, available at: http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf

[11] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[12] Trey Herr and Paul Rosenzweig, "Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model" Journal of National Security Law and Policy Vol. 8, No. 2 (2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2343798

[13] For further discussion of the spectrum of "active cyber defences" and the issues surrounding their engagement by the private sector, see Wyatt Hoffman and Ariel E. Levite, Private Sector Cyber Defence: Can Active Measures Help Stabilize Cyberspace? (Washington, DC: Carnegie Endowment for International Peace, 2017), available at http://carnegieendowment.org/files/Cyber_Defence_INT_final_full.pdf .

[14] See, for instance, Nicholas Schmidle, "The Digital Vigilantes Who Hack Back" The New Yorker May 7, 2018, available at https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back; and Joseph Cox, "Revenge Hacking Is Hitting the Big Time," The Daily Beast September 19, 2017. https://www.thedailybeast.com/inside-the-shadowy-world-of-revenge-hackers.

[15] See, for instance, Kim Zetter, "The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks," Wired February 10, 2015, available at https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/

[16] Tim Maurer (2016) : Internet Freedom and Expert Controls, Briefing, Carnegie Endowment for International Peace, available at https://carnegieendowment.org/files/Tim_Maurer_final_briefing_-_03.03.20162.pdf

[17] See Deborah D. Avant The Market for Force: The Consequences of Privatising Security (New York, NY: Cambridge University Press, 2006)

[18] For instance, the rapid growth of a market for private maritime security contractors in response to the escalating threat from Somali piracy in the mid-2000s posed significant challenges for national and international regulation. See Carolin Liss (2015): (Re)Establishing Control? Flag State Regulation of Antipiracy PMSCs, Ocean Development & International Law 46, no. 2: 84–97.

[19] The Tallinn Manual provides the most thorough analysis of the applicability of international law to cyber operations. See NATO Cooperative Cyber Defence Centre of Excellence Tallinn Manual on the International Law Applicable to Cyber Warfare (New York, NY: Cambridge University Press 2013). For further discussion see Michael Schmitt, "Armed Attacks in Cyberspace: A Reply to Admiral Stavridis," Lawfare January 8, 2015, available at https://www.lawfareblog.com/armed-attacks-cyberspace-reply-admiral-stavridis.

[20] Dustin Volz and Jim Finkle, "U.S. indicts Iranians for hacking dozens of banks, New York dam," Reuters March 24, 2016, available at https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF

[21] The Computer Fraud and Abuse Act (CFAA, 18 U.S.C. 1030); for a comparison of various countries' national laws pertaining to hacking, see Amanda Craig, Scott Shackelford, and Janine Hiller, "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis," American Business Law Journal 2015.

[22] The U.S. government distinguishes political and economic espionage considering the former legitimate intelligence collection and the latter to be inappropriate as highlighted in the September 2015 agreement between President Obama and President Xi Jin Ping with both sides committing not to engage in the cyber-enabled theft of intellectual property for competitive advantage.

[23] International Committee of the Red Cross, IHL Database, Article 36 Additional Protocol I, available at https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=FEB84E9C01DDC926C12563CD0051DAF7

[24] United Nations General Assembly Resolution A/HRC/20/L. 13, The promotion, protection and enjoyment of human rights, 29 June 2012, available at https://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc

[25] United Nations General Assembly, A/68/98*, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General, 24 June 2013, available at https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/UNGROUP-2013.pdf

[27] "The Surveillance Catalog" The Wall Street Journal available at http://graphics.wsj.com/surveillance-catalog/

[28] Tim Maurer (2016): Internet Freedom and Expert Controls, Briefing, Carnegie Endowment for International Peace, available at https://carnegieendowment.org/files/Tim_Maurer_final_briefing_-_03.03.20162.pdf

[29] Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research," Lawfare January 5, 2018, available at https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research

[30] For further discussion, see: Trey Herr (2014): PrEP: A Framework for Malware & Cyber Weapons, The Journal of Information Warfare, Vol. 13, No. 1, 2014 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2343798

[32] For an extensive discussion on this framework's relevance to the cyber context, see Scott J. Shackelford, "Human Rights and Cybersecurity Due Diligence: A Comparative Study" University of Michigan Journal of Law Reform Vol. 50, No. 4 (2017). https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1191&context=mjlr

[33] Deborah Avant. 2016. "Pragmatic Networks and Transnational Governance of Private Military and Security Services." International Studies Quarterly 60:2

[34] Deborah Avant. 2016. "Pragmatic Networks and Transnational Governance of Private Military and Security Services." International Studies Quarterly 60:2

[35] Daphne Richemond-Barak. 2014. "Can Self-Regulation Work? Lessons from the Private Security and Military Industry." Michigan Journal of International Law Vol. 35 No. 4. (pp. 819)

[36] Office of the United Nations High Commissioner for Human Rights. "UN expert panel calls for new international standards on private military and security companies." September 15, 2017, available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22081&LangID=E

[37] For further discussion of the circumstances and factors that might be used to delineate legitimate self-help from unacceptable conduct, see Wyatt Hoffman and Steven Nyikos. Governing Private Sector Self-Help in Cyberspace: Analogies From the Physical World (Washington, DC: Carnegie Endowment for International Peace, 2018) http://carnegieendowment.org/2018/12/06/governing-private-sector-self-help-in-cyberspace-analogies-from-physical-world-pub-77832

[38] For further exploration of what a specific CSR initiative for private sector cybersecurity services might look like, see Wyatt Hoffman and Ariel E. Levite, Private Sector Cyber Defence: Can Active Measures Help Stabilize Cyberspace? (Washington, DC: Carnegie Endowment for International Peace, 2017)

Geneva Centre
for Security Sector
Governance

www.dcaf.ch

DCAF – Centre pour la gouvernance du secteur de la sécurité
Chemin Eugène-Rigot 2E
P.O. Box 1360
CH-1211 Genève 1