**Cyber Mercenaries:**

**Review of the Cyber and Intelligence PMSC Market**

*A report for The Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the rights of peoples to self-determination*

**Dr. Ori Swed, Texas Tech University**

**Dr. Daniel Burland, The Peace, War, & Social Conflict Laboratory**

****

 The trend of outsourcing security and military functions has not omitted the intelligence and cyber realms. Good and reliable intelligence and cyber infrastructures and capacities have become the foundations of modern warfare and security forces. To master them, and to be able to provide them effectively in the field, require specialization, knowledge, access to technology, and organizational investments that are not available or accessible for many nations and armed forces. This situation opened a new market for private intelligence and cyber services. In this study we will map the trends in this sub-sector of the Private Military and Security (PMSC) industry, while providing a typology for the functions offered by different actors and presenting trends.

 As we consider the actors who carry out cyber and intelligence operations, it may be best to avoid the term "cyber mercenaries" (Maurer 2018; McMurdo 2016), or at least to use it with caution, since Maurer used this term to describe unidentified entities. In Maurer's work (2018), "cyber mercenaries" is a provocative and exotic term, focusing on entities and organizations that operate outside of the legal boundaries, that are associated with or are criminals and groups deprived of legitimacy, such as the Syrian Electronic Army (Perlroth 2013). We suggest that while this section of the market does exist, it is actually a fringe phenomenon and a small part of the activity. The bulk of cyber and intelligence services are provided by legitimate and established companies, with active webpages that describe their products and services. Some of these companies are traded on the stock exchange (*e.g.* Booz Allen Hamilton, Kellogg, Brown & Root, and Raytheon). Those actors are not hiding in the shadows; to the contrary, they have lobbies and connections with government officials, and they are often the official contractors for governments and their militaries. This report’s focus is on the PMSCs who are hired to provide cyber and intelligence services as a specialized form of outsourcing, and in this commercial sector, the actors carrying out cyber operations are employees whose actions are being coordinated and their results reported to clients by company executives.

 Our focus on both cyber and intelligence services is grounded in empirics. The typology we offer below is derived from the industry’s broad gamut of practices and the data we have gathered documenting those practices. We have utilized the PMSCs dataset of the Peace, War, and Social Conflict Laboratory at Texas Tech University (PWSCL-TTU) to map this sub-sector of the industry. The dataset identifies and catalogues companies’ services, aggregating them under five categories; one of those categories is cyber and intelligence-related services. Those categories capture a broad range of activities associated with this sub-field, from the supply and operation of hardware to the provision of skills and advanced software. Those services are often intertwined, with many companies providing both IT services and cyber defense capacities as part of their portfolio. As companies constantly strive to extend the services they offer and their potential markets, their efforts result in a familiar blurring (as described by Prem (2018)) between which providers are or are not "private." Therefore, we find the broader categorization of cyber and intelligence services useful for this report.

The management, control, production, and manipulation of information has always been an integral part of war and security functions (Herman 1996; Keegan 2010; Simpson 2015), and as such a potential market for outsourced services. Communicating information among units, maintaining control, and coordinating efforts involve infrastructure, hardware and software, access to technology and knowledge. All are potential services and specializations that are being marketed by the PMSC industry. Secure communication and the effective and safe management of data require high-end skillsets that may not be available within the traditional membership of a military or security organization. Information in this context may also include intelligence gathering, such as signal intelligence or geospatial intelligence, and the management and interpretation of this information. For example, having access to satellite imaginary can provide valid information only if one possesses the expertise to interpret the images, accounting for distortion, time lag, depth, and irregularities. Again, all those types of services are offered by the PMSC industry. The prevalence of information platforms has introduced new challenges and solutions, namely, services designed for extracting information or disrupting its flow, as well as services aimed at protecting the information and the infrastructure containing and organizing it. Those types of services are often considered as cyber defense and offense specializations, a sub-section in the PMSC industry. The saturation of data-gathering devices among the general population, through cell phones, personal computers, and other devices, opened the door for different ways of gathering and manipulating intelligence. Utilizing tactics taken from the commercial world that collect massive data on users to create profiles, to predict users' behavior, and to actively manipulate people to purchase commodities (De Vries 2010; Hofacker et al. 2016; Woolley and Howard 2017), several PMSCs have ventured into the world of mass surveillance and information manipulation on a grand scale (Chesterman 2008; Hintz 2014; Shorrock 2008). Some companies specialized in the surveillance aspect, introducing dual-use services, which fit commercial clients yet can be adapted to accomplish security and military functions as well. Examples include public health tools that track outbreaks and the spread of diseases within a civilian population (Buckee 2020); these can be transferred into the realm of terrorist hunting by security forces, to isolate targeted terrorists from the general population (McKendrick 2019). Other companies specialized in influencing public opinion (Stark 2018; Ward 2018), offering dual-function services that assist politicians to win reelection or to foster instability and division in other nations through virtual societal warfare (Mazarr et al. 2019).

 PMSC specialists in this sub-field are hired by private employers or by government agencies who have a temporary need for an expanded workforce in this area; they are used to carry out administrative functions and analysis as well as for specialized technical applications (Halchin 2015). The same companies also fill technological gaps, offering access to advanced technologies, such as offensive cyber software or communication arrays, to clients for the duration of the contract. This market-driven process of outsourcing specialized skills and technologies is not new and stands at the core of the PMSC industry. Avant (2005) and Singer (2008) explained that outsourcing military and security functions occurs when the clients do not possess the skills or technology due to a technological gap or an organizational decision based on cost-efficacy. The sub-field we are focusing on in this study, which operates within an environment saturated with advanced technology and which requires high-end skills, exemplifies the extreme end of this trend. Often this type of service involves high entry barriers in term of cost, human capital, and knowledge, which exclude most countries.

 Using the PWSCL-TTU to preserve and organize this information, we identified the companies that offer cyber and intelligence related services. Going through their webpages, we classified five different types of services offered by the industry: Communication infrastructure, IT services and cyber defense, Intelligence, Cyber offensive, and Big data-based services.

1. **Communication infrastructure.** A significant portion of PMSC services is associated with logistics, maintenance, and infrastructure (Kinsey 2009; 2014; Kinsey and Erbel 2011; Kinsey and Patterson 2012). In the context of the outsourcing of cyber and intelligence, those services focus on the erection of communication infrastructure such as cables, dishes and CCTV array, and the relevant hardware. This type of infrastructure is crucial and serves as the foundation of any military or security operation. It allows for command-and-control centers, communication among units, and secured communication. An example of the type of companies offering these services is the GEOS group, which describes itself as “specialising in the deployment and operation of telecommunication networks and information systems in sensitive areas, hostile environments or on behalf of the Defence industry” (GEOS group webpage). Many of the large PMSC logistics contractors, such as KBR, DynCorp International, and ANHAM, also offer these types of communications services.
2. **IT services and cyber defense**. Multiple PMSCs offer different levels of IT-related services, focused on establishing and maintaining the communication and cyber infrastructure. While the communication infrastructure often focuses on the hardware, the IT services and cyber defense focus mostly on the software. The two are not mutually exclusive, and often companies like GEOS group will offer both as complementary services. The procurement of these related but distinct services from a single provider allows the communications networks and command-and-control centers to operate more smoothly and securely. An example of this type of specialization is Research Analysis and Maintenance, Inc. (RAM), in El Paso, Texas, which offers “…the complete spectrum of information systems services and support to meet our Government and corporate customers' needs. We have substantial networking and telecommunication and system/software engineering capability and experience, permitting us to offer total life-cycle information system solutions” (RAM webpage). IT and cyber defense services are considered a basic package for technical support and are offered by numerous companies.
3. **Intelligence**. Another category within this sub-specialization includes PMSCs that focus on producing, collecting, and analyzing intelligence that is based on and/or utilizing computers. Those include geo-intelligence services, radar signals, satellite-based intelligence, and signals intelligence among other types of specializations. In this category there are PMSCs that work as intelligence sub-contractors for governments, working alongside governmental agencies and utilizing their technology, or as the providers of new toolkits and accompanying skillsets for commercial actors or states with gaps in intelligence capabilities. Shorrock (2008; 2015) describes the privatization of the intelligence industry, with the outsourcing of services such as the analysis of signal intelligence and the tracking down of suspected enemy combatants for U.S. Special Forces in the Middle East to companies such as Leidos, Booz Allen Hamilton, CSRA, SAIC, and CACI International.
4. **Cyber offensive**. This sub-field is narrower and includes only a handful of companies, which makes sense given that those type of services do not have a commercial market. These companies specialize in infiltrating or overwhelming cyber defenses. This specialization includes a gamut of tactics, among them taking over websites and disrupting the adversary’s services. The leading companies in this subfield are the large PMSCs with strengths in the field of information and communication, such as CACI, Booz Allen Hamilton, Lockheed Martin, Raytheon, BAH, Northrop, and Harris. The United States Cyber Command has been outsourcing not only parts of its cyber defense capacities but also its cyber offense (Sternstein 2015). The major role of private companies in building the cyber warfare capabilities of the United States is worth noting, at a moment when some analysts have said that there is a cyber arms race underway among some of the world's largest and most powerful nations (Gehem 2015). The implications of public-private partnerships in the areas of cyber warfare and cyber security have raised particular security and regulatory concerns (Chasdi 2019; Button 2019; Collier 2018; McCarthy 2018; Sales 2018).
5. **Big data-based services**. The wealth of data produced by individuals, groups, and organizations and regularly recorded through cell phones, apps, and other electronic devices have become a harvest field for commercial actors attempting to understand and predict their potential clients’ inclinations. Commercial actors have been using artificial intelligence and machine learning techniques to create self-learning, ever-collecting programs that harvest massive amounts of data about users. With the personalization of algorithms, which anticipates our intentions and needs (for example in prioritizing the results of a Google search) (De Vries 2010), and the large-scale personal data harvesting, big data can also go beyond descriptive functions and be used to manipulate people to buy or act in a particular way or to reshape the way they view the world around them (Bradshaw and Howard 2018). Those two venues started two new sub-specializations in the industry: mass surveillance and virtual societal warfare. Mass surveillance was described by Edward Snowden, a whistleblower and a Booz Allen Hamilton contractor who worked for the NSA. Several uncovered mass surveillance programs (for example PRISM and Tempura) had been utilizing commercial partners and had an outsourcing component. At the same time, a handful of companies developed similar methods and mass surveillance tools, to the point where they are outsourcing not just support services but the function itself. At present, one of the most well-known companies in this sub-field is the Israeli PMSC the NSO Group, whose spyware, Pegasus, makes it possible to engage in mass surveillance. Pegasus is used both by states and by non-state actors (O’Neill 2020). The second sub-specialization, known as virtual societal warfare, focuses on public opinion manipulation, utilizing macro targeting of political and social messages via social media. This is a form of information operations that can put pressure on representatives in democratic regimes and influence political processes and decisions (Tenove et al. 2018). If done during an election period, it even has the potential to influence the outcome of elections. Such activities include the creation of fake accounts to manipulate public discourse and disseminate fake news and other disinformation online and thereby influence public opinion. The most notable PMSC involved in those activities is the Russian Internet Research Agency, which was associated with the intervention in the 2016 U.S. Presidential election (Mueller 2019).

**Trends in the PMSC cyber and intelligence sub-industry**

We used the PWSCL-TTU dataset to identify trends in the industry. The dataset includes 1674 unique companies that specialize in providing services to the military and defense industry worldwide. All information is gathered from open sources, using the companies’ webpages and social media, government reports, nongovernmental organizations’ accounts, business listing webpages (such as Bloomberg), and leading media outlets (such as the New York Times, Washington Post, BBC, and others). The dataset does not capture the industry in its entirety, but it covers all the major actors and offers a comprehensive sample of the industry. The dataset does not capture newly formed companies and may not reflect the recent termination or mergers of companies.

Examining the proportion of PMSCs in the sample that provide cyber and intelligence related services shows that those types of services are very common, offered by about 62% of the companies listed in the dataset (Table 1). As previously mentioned, many of the companies that specialize in cyber and intelligence related services are also providers of logistics, construction, and maintenance services. Such diversified companies’ services are well-represented among the categories of communication infrastructure and IT and cyber defense. Within the sample, there are 316 PMSCs that provides both type of services, which accounts for about 20% of the sample. By contrast, companies that specialize mainly in cyber and intelligence services represent a small group within the sample, accounting for about 5% of the entire sample.

|  |
| --- |
| **Table 1. The Prevalence of Cyber and Intelligence among other Services in the PMSC industry** |
| **Sample**  | **Freq.** | **Percent** |
| PMSCs that specialize in cyber/intelligence, regardless of other type of specialization | 1,039 | 62.07% |
| PMSCs that specialize in both logistics and cyber/intelligence services | 316 | 18.87% |
| PMSCs that mainly specialize in cyber/intelligence services | 89 | 5.31% |

 Examination of the headquarters locations of the PMSCs that specialized mainly in cyber and intelligence services illustrates the distribution of providers. We use main headquarters location as a proxy, given that it is not a guarantee of exclusive activity; many companies have multiple headquarters across the globe. Figure 1 shows that a large proportion of PMSCs in this sub-field (36 out of 89) are located in the United States. The United Kingdom and China represent two other clusters, with 14 and 11 such PMSCs respectively. Hong Kong,[[1]](#footnote-1) the United Arab Emirates, and Israel are next, presenting 4, 3, and 3 PMSCs respectively. Those findings correspond with our earlier study on the global clustering of the industry (Swed and Burland 2020a). The United States, the United Kingdom, and China represent the leading countries in housing PMSCs headquarters.

**Figure 1. Main provider of Cyber and Intelligence**



 A review of the historical trend of this sub-sector indicates that it correlates with two historical events. The first is the Dot-Com market bubble of the 1990s, when high-tech companies garnered wide support and funding, which in turn facilitated the proliferation of many new companies. During the Dot-Com bubble era, this sub-sector experienced its greatest increase, illustrated as two peaks in Figure 2. A significant portion of the PMSC industry is technology-based and is located in the high-tech hubs of the United States, United Kingdom, and other countries. The focus on the PMSCs that specialize in cyber or intelligence related services underscores those relations. The second wave for these companies took place during the War in Iraq (beginning in 2003), as the response to a growing demand by the United States and its coalition for outsourced services. Figure 2 illustrates three waves of new companies founded during that period. A political decision by the Bush Administration, which preferred outsourcing over recruiting more soldiers or issuing a draft, opened the market for PMSCs, creating a market boom (Avant 2013). PMSCs that specialized in cyber and intelligence related services participated in that market boom.

**Figure 2. Trend of the creation of new PMSCs specializing mainly in Cyber/Intelligence 1980-2019**

**Discussing the trends**

 There are three main takeaways from this report. First, the term "cyber mercenaries" is a great framing to draw public opinion and policy makers into discussions about this topic. However, it is misleading, and as such, its use is recommended only where appropriate. While there are rogue actors that are borderline criminals, most of the industry is established and is in plain sight. The development of cyber defense and the provision of IT services are not unique to the military or security forces. Those and other functions have dual usage (Herr and Rosenzweig 2015; Miller 2018) and can be adapted easily to accommodate the needs of commercial actors, NGOs, or even individuals. Many of the companies offering such services have a website describing their services; some of them are even traded on the stock exchange. To put it simply, at this point of time, there is no need to go into the dark web to find the main providers of cyber and intelligence related services. You can instead just give them a call using the contact information on their webpages and social media sites.

 The second takeaway is that this trend is not new and is part of the broader outsourcing trend of military and security functions (Singer 2005; Stanger and Williams 2006; Swed and Burland 2020b). The market for outsourced security and military functions answers a capability gap for states, organizations, and in some cases individuals that want to use a particular set of skills and technology. When examining the cyber and intelligence sub-sector of this industry we can see that most of the functions outsourced are mundane and aimed at answering basic logistical and infrastructure needs in the field of communications. Even the most sophisticated intelligence organization needs functional workstations, secured and reliable communication, and IT support. This is what most of the PMSC industry looks like. A portion within that sub-sector offer skills of data analysis and manipulation that can be used for intelligence gathering and offensive cyber operations. An even smaller group of organizations within that sub-section in the industry create their own unique cyber and intelligence tools and market them as products.

 It is the outsourcing of functions related to the fifth category, big data-based services, which presents real challenges to human rights and democratic processes. The two main functions described, mass surveillance and virtual societal warfare, disrupt what we know about security and government control as well as our understanding of warfare in general. Mass surveillance is a powerful tool to catch terrorists, human traffickers, and organized crime members. At the same time, it can easily be utilized to suppress political opposition and free speech. Spyware that can go through massive data to detect individuals that are involved with terrorists and differentiate them from the general population can also be used to identify the individuals that complain to their friends about the leadership’s policies or actions, or the minority that follow a different religion or have a different sexual orientation. This translates into potentially massive infringements of human rights (Chan 2019; Marczak and Scott-Railton 2016). In 2018, Amnesty International stated that those type of technologies were used to spy on organization members in Saudi Arabia (Amnesty International 2018). Oppressive regimes and authoritarian politicians can easily utilize this type of service to seize power, repress opposition, and retain power. The high barrier of technological development vanishes the moment these types of services and tools become commodities. A report from The Citizen Lab indicates that this technology has become available also to violent non-state actors. The report shows that one such technology tool was used by a Mexican drug cartel to identify a journalist (Scott-Railton et al. 2017). Without proper regulation of these types of services and the companies that provide them, we can anticipate a rise in state repression and human rights abuses. The second function, virtual societal warfare (Mazarr et al. 2019), takes the battlefield into the heart of the civilian realm, using the general public to influence its politicians and political system and, in so doing, its foreign policy as well. The reliance on big data allows for the weaponization of ideas and the promotion of false narratives and disinformation. This is done thorough the creation of networks of fake personas and fake news accounts that disseminate false information, distorted information, or reshape and refocus media coverage on topics that benefit one candidate or political party over the others (DiResta et al. 2019; Jamieson 2020; Linvill et al. 2019). Disinformation through the use of big data can polarize nations and groups and sow discontent and distrust in the government and the democratic process. Nations with democratic systems are more vulnerable to this type of interference, as it can distort the available knowledge that influences voters’ decision-making (Hansen and Lim 2019; Sander 2019). Without equal access to reliable information, the democratic process can be skewed. It has been shown that higher exposure to those type of operations can mobilize people to action and affect their voting behavior (Jamieson 2020; Helmus et al. 2020). Furthermore, this particular tool is not regulated. Without proper regulations or international norms, we can expect to see this tool used more frequently, especially among nations that cannot properly safeguard their cyber infrastructure during elections.

**Conclusion**

There is an increasingly blurry line that separates the private and national spheres; there is a second increasingly blurry line that separates the military and civilian spheres. International law might insist on these distinctions, but the Internet crosses these boundaries as a matter of course. This is a perfect example of what sociologists call “culture lag,” (Ogburn 1957) where technology advances faster than the political and legal categories in place to regulate what society will allow to be done with that new technology. It is the new capabilities of cyber intelligence that pose the real threat, as well as the consequences of those capabilities falling into the hands of private security agents ("cyber mercenaries"). Human rights monitoring should devote at least as much attention to the technology itself as to the agents using it, whether governmental, criminal, or somewhere in between. In a world where information is weaponized on a mass scale and used for influence operations, propaganda campaigns, counterterrorism, population control, and state repression, the market for information capabilities and services has emerged rapidly and continues to flourish. The supply and demand for legitimate cyber intelligence services provided by lawfully registered, publicly traded firms poses at least as great a potential threat to international human rights as the work of small, rogue agents operating on the "dark web." The processing of Big Data requires vast resources and personnel which can be found in large, well-established, and diversified PMSC firms. The way in which technology is used by these large and influential corporations is an area where regulation is needed and where it could be expected to be effective, given the very visibility and formal legal status of these corporations. Yet, it is important to point out that PMSCs are not the source of the challenge here; they merely exacerbate an existing cleavage in international law where actors can use advanced cyber tools to influence civilians and rival actors. The realms of cyber warfare and mass surveillance are ill-regulated as a whole. As a low-cost, high yield and unregulated pathway to influence rival states and other political actors, the use of those type of technologies presents a great appeal. The process of outsourcing allows actors that could not gain access to this type of technology or skillset due to gaps in knowledge, cost, or technological development, to join this wide-open and unregulated field. The more actors using those unchecked technologies, the greater the threat for democratic processes and human rights violations.

At the same time, the outsourcing of cyber and intelligence services offers a path forward and an opportunity to regulate the use of those technologies, at least among PMSCs. Curbing the outsourcing of those services is an achievable goal, provided that we aim for regulating commercial activity and not states’ behavior. Regulating states’ actions proves to be a real challenge in international relations. On the other hand, influencing companies is easier, even if difficult. The regulation of PMSCs activities and contracts has improved dramatically in the last several years. Legal frameworks have been developed to differentiate PMSCs from mercenaries and other entities and to suggest the proper jurisprudence for dealing with their roles in the field. The advancement of similar laws and regulations in the cyber sector could help to restrain the outsourcing of the services and technologies that have the potential of harming human rights and democratic processes. Pressures on the industry facilitated the creation of professional associations and codes of conduct for PMSCs such as the International Stability Operations Association (ISOA), the American Society for Industrial Security International Association (ASIS), the International Code of Conduct for Private Security Service Providers’ Association (ICoCA), and the British Association of Private Security Companies (BAPSC). Similar initiatives could ensure that cyber related technologies would be better kept in check, encouraging PMSCs in this sub-field to follow acceptable and reasonable standards. A success here could spill over to the broader discussion about regulating cyber activities, by offering expectations and standards.

**Works Cited:**

Amnesty International. 2018. Amnesty International among targets of NSO-powered campaign. August 1. (Accessed February 9, 2021 at https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/)

Avant, Deborah. 2005. *The Market for Force: the consequences of privatizing security*. Cambridge University Press.

Avant, Deborah. 2013. The Mobilization of Private Forces After 9/11: Ad Hoc Response to Inadequate Planning. In *How 9/11 Changed Our Ways of War*, ed. James Burk. Stanford, CA: Stanford University Press, pp. 209-32.

Bradshaw, Samantha, and Philip N. Howard. 2018. "Challenging truth and trust: A global inventory of organized social media manipulation." *Oxford Internet Institute,* The Computational Propaganda Project 1.

Buckee, Caroline. 2020. "Improving epidemic surveillance and response: big data is dead, long live big data." *The Lancet Digital Health* 2, no. 5: e218-e220.

Button, Mark. 2019. The “New” Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions. *Journal of Contemporary Criminal Justice*.

Chan, Anna. 2019. The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by CyberSurveillance Spyware. *Brooklyn Journal of International Law*.

Chasdi, Richard J. 2019. A typology of Public–Private Partnerships and its implications for Counterterrorism and Cyber-security. *Online Terrorist Propaganda, Recruitment and Radicalization*. CRC Press.

Chesterman, Simon. 2008. "We Can't Spy… If We Can't Buy!’: The Privatization of Intelligence and the Limits of Outsourcing ‘Inherently Governmental Functions." *European Journal of International Law* 19, no. 5: 1055-1074.

Collier, Amie. 2018. Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision. *Politics and Governance.*

De Vries, Katja. 2010. "Identity, profiling algorithms and a world of ambient intelligence." *Ethics and information technology* 12, no. 1: 71-85.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. 2019. "The tactics & tropes of the Internet Research Agency." *U.S. Senate Documents.*

Gehem, Maarthen, Artur Usanov, Erik Frinking and Michel Rademaker. 2015. *Assessing Cyber Security: A Meta-analysis of Threats, Trends, and Responses to Cyber Attacks*. The Hague Center for Strategic Studies.

Halchin, Elaine. 2015. The Intelligence Community and Its Use of Contractors: Congressional Oversight Issues. Congressional Research Service Report, August 18.

Hansen, Isabella, and Darren J. Lim. 2019. "Doxing democracy: influencing elections via cyber voter interference." *Contemporary Politics* 25, no. 2: 150-171.

Hansen, Morten. 2014. Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community. *Intelligence and National Security* 29(1): 58-81.

Helmus, Todd C., James V. Marrone, Marek Posard, and Danielle Schlang. 2020.  *Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-interventions*. RAND.

Herman, Michael. 1996. *Intelligence power in peace and war*. Cambridge University Press.

Herr, Trey, and Paul Rosenzweig. 2015. "Cyber weapons and export control: Incorporating dual use with the prep model." *Journal of National Security Law & Policy* 8: 301.

Hintz, Arne. 2014. "Outsourcing surveillance-privatising policy: communications regulation by commercial intermediaries." *Birkbeck L. Rev.* 2: 349.

Hofacker, Charles F., Edward Carl Malthouse, and Fareena Sultan. 2016. "Big data and consumer behavior: Imminent opportunities." *Journal of consumer marketing*.

Jamieson, Kathleen Hall. 2020. *Cyberwar: how Russian hackers and trolls helped elect a president: what we don't, can't, and do know*. Oxford University Press.

Keegan, John. 2010. *Intelligence in war*. Random House.

Kinsey, Christopher. 2009. *Private contractors and the reconstruction of Iraq: Transforming military logistics*. Routledge.

Kinsey, Christopher. 2014. "Transforming war supply: Considerations and rationales behind contractor support to UK overseas military operations in the twenty-first century." *International Journal* 69, no. 4: 494-509.

Kinsey, Christopher, and Mark Erbel. 2011. "Contracting out support services in future expeditionary operations: Learning from the afghan experience." *Journal of Contemporary European Research* 7, no. 4: 539-560.

Kinsey, Christopher, and Malcolm Hugh Patterson, eds. 2012. *Contractors and war: The transformation of United States’ expeditionary operations*. Stanford University Press.

Linvill, Darren L., Brandon C. Boatwright, Will J. Grant, and Patrick L. Warren. 2019. "“THE RUSSIANS ARE HACKING MY BRAIN!” investigating Russia's internet research agency twitter tactics during the 2016 United States presidential campaign." *Computers in Human Behavior* 99: 292-300.

Marczak, Bill and John Scott-Railton. 2016. The million dollar dissident: NSO group's iPhone zero-days used against a UAE human rights defender. *Citizen Lab* (citizenlab.ca).

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

Mazarr, Michael J., Ryan M. Bauer, Abigail Casey, Sarah A. Heintz, and Luke J. Matthews. 2019. *The emerging risk of virtual societal warfare: Social manipulation in a changing information environment*. RAND Corporation, Santa Monica, CA.

McKendrick, Kathleen. 2019. "Artificial intelligence prediction and counterterrorism." *London: The Royal Institute of International Affairs–Chatham House* 9.

McCarthy, D.R. 2018. Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order. *Politics and Governance*.

McMurdo, Jesse. 2016. Cybersecurity Firms - Cyber Mercenaries. *Homeland & National Security Law Review*.

Miller, Seumas. 2018. "Cyber-Technology." In *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*, pp. 91-104. Springer, Cham.

Mueller, Robert. 2019. Report on the investigation into Russian interference in the 2016 Presidential election. U.S. Department of Justice. March. (Accessed February 6, 2021 at URL: https://www.justice.gov/storage/report.pdf).

O'Neill, Patrick. 2020. Inside NSO, Israel's billion-dollar spyware giant. *MIT Technology Review*. August 19. (Accessed February 6, 2021 at URL: https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/)

Ogburn, William F. 1957. "Cultural lag as theory." *Sociology & Social Research*.

Perlroth, Nicole. 2013. Hunting for Syrian hackers' chain of command. *New York Times*, May 17. Accessed at: https://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html, on January 27, 2021.

Prem, Berenike. 2018. Who am I? The blurring of the private military and security company (PMSC) category. In *Security privatization*, Springer, Cham, pp. 51-76.

Sander, B., 2019. Democracy under the influence: Paradigms of state responsibility for cyber influence operations on elections. *Chinese Journal of International Law*, *18*(1), pp.1-56.

Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. 2017. *Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware*.

Shorrock, Tim. 2008. *Spies for hire: The secret world of intelligence outsourcing*. Simon and Schuster.

Sales, N.A. 2018. Privatizing Cybersecurity. *UCLA Law Review*.

Shorrock, Tim. 2015. A new cybersecurity elite moves between government and private practice, taking state secrets with them. *The Nation*.

Simpson, Christopher. 2015.  *Science of coercion: Communication research & psychological warfare, 1945–1960*. Vol. 13. Open Road Media.

Singer, Peter W. 2005. "Outsourcing war." *Foreign Affairs* 84: 119.

Singer, P.W., 2008. *Corporate warriors: The rise of the privatized military industry*. Cornell University Press.

Stanger, Allison, and Mark Eric Williams. 2006. "Private military corporations: Benefits and costs of outsourcing security." *Yale Journal of International Affairs* 2: 4.

Stark, Luke. 2018. "Algorithmic psychometrics and the scalable subject." *Social Studies of Science* 48, no. 2: 204-231.

Sternstein, Aliya. 2015. CYBERCOM to outsource $475 million worth of offense and defense work. Nextgov.com, May 1. (Accessed February 6, 2021 at URL: https://www.nextgov.com/cybersecurity/2015/05/cybercom-outsource-475-million-worth-offense-and-defense-work/111619/).

Swed, Ori and Daniel Burland. 2020a. The Global Expansion of PMSCs: Trends, Opportunities, and Risks. *United Nations Office of the High Commissioner for Human Rights, Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination.* (Accessed on February 6, 2021 at URL: https://www.ohchr.org/Documents/Issues/Mercenaries/WG/ImmigrationAndBorder/swed-burland-submission.pdf).

Swed, Ori, and Daniel Burland. 2020b. "Outsourcing War and Security." In *Oxford Research Encyclopedia of the Military in Politics*. Oxford University Press. doi:10.1093/acrefore/9780190228637.013.ORE\_POL-01925.R1

Tenove, Chris, Jordan Buffie, Spencer McKay and David Moscrop. 2018. *Digital threats to democratic elections*. Centre for the Study of Democratic Institutions, University of British Columbia, Canada. (Accessed on February 6, 2021 at URL: https://pdfs.semanticscholar.org/ca1e/7ee79c0eb0720cc2343f5198eae86d20ac94.pdf).

Ward, Ken. 2018. "Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica’s behavioral microtargeting." *Journal of media ethics* 33, no. 3: 133-148.

Woolley, Samuel C., and Philip Howard. 2017. "Computational propaganda worldwide: Executive summary." *University of Oxford Computational Propaganda Research Project,* Working Paper 2017.11.

1. We separate Hong Kong from China since the data represent historical trends and not current reality on the ground. Some of the companies listed were terminated, merged, or acquired and no longer exist. [↑](#footnote-ref-1)