Corporate Liability in the Production and Sale of Cyber Weapons

Ian Heimgartner
184538HAJM

Advisor: Alexander Antonov

Table of Contents

Abstract

The interplay between cyber technologies and international law is a rapidly developing but infantile field. In recent years there have been court cases at the national level that indicate a shift in western legal systems towards tighter restrictions on trade in cyber technologies. Still however, there is not an international framework that addresses the intricacies of cyber weapon proliferation by non-state actors. In this paper, I will develop the issue through an in-depth look at possible extrapolations of existing international treaties into the cyber realm; a look at the growing importance of Corporate Social Responsibility, it's roots in soft law and developments that are pushing it into hard law; and examinations of cases involving corporations that deal in cyber technologies and the national response to them. I will attempt to argue that non-binging international treaties such as the Wassenaar Arrangement are taking on more importance as the international regulatory schemes shift to an emphasis on export licesnses as a means of control. Finally I will examine the Arms Trade Treaty as a basis for a future international cyber weapons convention.

Chapter 1: Introduction

A. Overview

The Treaty of Westphalia created the international order that we live in today. It's a state centric system that is reflected throughout international law with notable exceptions to individual responsibility coming from fields such as international criminal law. With globalization and the advent of the internet however, the landscape has shifted somewhat dramatically from the era of kingdoms versus other kingdoms or even the more nationalistic flavors of the pre-world war two era. Armed conflicts since the 1950s have consistently taken on a more non-state actor flavor. While international conflicts do still exist, the majority of wars around the world are internal and driven by motives outside our traditional concept of state vs. state hostilities. Further compounding the issue is the shift in the means and methods of warfare, namely the trend of rising cyber-attacks on developed nations' infrastructure or communications systems. While fields such as humanitarian law and human rights law have shifted to reflect the changing nature of war, there is still no international consensus when it comes to attacks in the virtual world. While that topic has been researched and argued about somewhat extensively over the previous years, it's difficult to determine if any consideration at all has been paid to the potential rise of virtual defense contractors.

There is a science fiction story, The Weapon Shops of Isher, centered around the notion of arms manufacturers that have become so skilled in their craft that they possess weapons far beyond the acting government; this gives them immense political power, and they are only beholden to their own established judicial system. While the concept may seem outlandish as surely modern day arms manufacturers exist at the very least with the tacit approval of their headquartered company, when applied to the field of cyber weapons, where resources and knowledge are widely available to individuals from anywhere in the world, suddenly the fictional setting of Isher begins to take on a more real tone. Before the idea is completely written off by the demonstrable power of national cyber defense agencies like the United States Cyber Command, largely operated by the military and Department of Defense, consider some of the alternatives to state controlled agencies. One such corporation, a focus within this paper, is the Israeli tech firm, NSO. They have developed the world's most powerful spyware, code named "Pegasus," which they have then exported to foreign governments and other groups throughout the years, with little impunity. The only semblance of control over their business dealings is the export licenses they obtain through the Israeli government; however, as this paper intends to show, those measures are what can be described at tokenism.

While there are promising international efforts to help curb this type of behavior, the majority are focused primarily on private military corporations and miss the mark in terms of legal language when it comes to the cyber realm. Further, there are larger liability issues in the interplay of corporations and human rights law as well as international criminal law that seem to foster the dangerous business ethics of cyber defense contractors.

B. The Process/Study Area

This research was done in a number of stages that consisted of a set of literature reviews. The first being about cyber weapons and international law in a more general sense, attempted definitions as put forth in the Tallinn 2.0 Manual, as well as opinions on the applicability of humanitarian law to cyber war. The second and perhaps the crux of this research was the focus on private military corporations, their place within both international and national legal frameworks, various scandals that led to developments in attempted regulatory regimes, and their obligations towards international human rights law. The final set of literature reviews were aimed solely at the field of international criminal law, and how if at all it can apply to corporations.

With the literature reviews in place, my focus was shifted to analyzing current, in some circumstances still on-going, legal cases around the world involving corporations that deal in software or hardware and have allegations of Rome statute violations or various other human rights concerns. The applicability of Rome statute violations was of particular interest at this stage; however, for reasons that will be discussed in the results chapter, the focus had to shift to other forms of control, specifically export licenses and end-user license agreements. The latter of which is more demonstrably shown through manufacturers of traditional weapons, but clear comparisons will be drawn between small arms and cyber weapons in that context.

The case analyses were a large part of the research, although access to specific case files was difficult to obtain and/or find translations for. Because of this the final angle of my results portion took on a wider study of international legal trends that were seeking to find an answer to this issue or within which a proper framework for control lay dormant. In this section, I specifically studied the Wassenaar Arrangement, as well as other successful international tools of control with respect to nuclear and chemical weapons. My aim was to respond to the academic community, that seems to extol the latter two relevant conventions as a possible solution for the control of cyber weapons, while positing my own theory for an international framework.

C. Assumptions made in the course of this research

There were a number of assumptions made in the course of this research that bare some weight in the findings. The biggest and perhaps the most controversial was alluded to earlier, the definition of cyber weapons. While there remains no international legal definition of "cyber weapon," the Tallinn 2.0 Manual puts forth a definition of "cyber-attacks" and by extension, weapons, that was agreed upon by industry experts, albeit from predominantly NATO countries. That definition comes in rule 92, paragraph 2:

> "The notion of 'attack' is a concept that serves as the basis for a number of specific limitations and prohibitions in the law of armed conflict. For instance, civilians and civilian objects may not be 'attacked' (Rules 92, 94, and 99). This Rule sets forth a definition of 'attack' that draws on that found in Article 49(1) of Additional Protocol I: 'attacks means acts of violence against the adversary, whether in offence or defence'. By this widely accepted definition, it is the use of violence against a target that distinguishes attacks from other military oper-

> ations. Non-violent operations, such as psychological cyber operations and cyber espionage, do not qualify as attacks[1].”

There was then a good deal of disagreement over the nuances of that particular article, namely the issue of a ‘kinetic’ consequence, i.e. something being physically destroyed. It was the general consensus of the group that while physical harm doesn’t necessarily have to occur, there must result some physical harm as a consequence. The example they give is of hacking a power grid that later results in an electrical fire. The fire was not caused by the initial hack, but was a consequence thereof. They state quite clearly in paragraph 14 of that section that not all cyber operations constitute and attack, and that most forms of cyber espionage do not unless the means or methods used qualify as an attack.

For the purposes of my research I reject the notion put forth in paragraph 14, and instead adopt the minority opinion they present in paragraph 13, wherein they discuss cyber operations that do not result in such consequences, but nonetheless have wide-spread adverse effects (such as shutting down the email system of a country), should be categorized as cyber-attacks. This was ultimately struck down because such an attack has no basis for understanding in humanitarian law; however, I am accepting this definition of an attack and by extension the “weapon” that caused it. Further I am expanding the scope of that definition to remove the “wide-spread” notion as my research does not focus solely on humanitarian law, and instead encompasses human rights law where the idea of a “wide-spread” attack against an individual makes no feasible sense. It should be noted that this is a somewhat dangerous definition of a cyber weapon as it now expands to what can be considered intrusive surveillance software; however, for the purposes that will be discussed below, particularly in the section about the Wassenaar arrangement, it makes sense from an export control point of view.

Another assumption that this research makes is on the nature of cyber weapon development and sales. While presumably, the majority of cyber weapon or defense development comes from national or military agencies, there always exists the possibility of development outside such structure. This can readily be seen from the numerous DDoS attacks against websites, perpetrated by individuals with no connection to a state entity. Whether or not the problem is widespread enough in the business sector to raise to the level of international concern is unknown given the nature of cyber operations themselves; however, it is safe to say that corporate cyber espionage is a very real threat, even though it may be predominantly state driven. Further, I conscribe to the notion that the sale of these weapons follows the traditional path of arms contracts, which it very well may not, but corporations like NSO have demonstrated that they do.

The final assumption to mention at this stage is more for definitional ease than controversial arguments. When I discuss cyber weapons under the definition I set forth, I am including both software and hardware, if that hardware is designed to function as a whole or part of a cyber weapon. This is merely to remove any confusion about tangible and intangible products, even though it may have an impact in my discussion of possible frameworks particularly as it relates to intellectual property; however, such disparities will be discussed and dealt with at the appropriate time.

[1] Tallinn Manual 2.0 page 415.

Chapter 2: Literature Review

A. Cyber weapons in the context of international law and the potential responses to a cyber-attack

Perhaps the earliest form of a cyber weapon, sometimes called a logic bomb, is from farther back in history than most realize, before the internet was as widely used as is the case today. In 1982, in Serbia, there was a large explosion witnessed from American early warning satellites. Contrary to popular belief, it was not a fired missile or a Russian pipeline explosion. According to the memoirs of former Air Force Secretary Thomas Reed, the blast was caused by a malfunction in the computer control system that Soviet spies had stolen from a firm in Canada. The system had actually been tampered with by the CIA to the point that the software, when installed, had been directed to change the pump speeds and pressure settings to produce an unstable result that reached far beyond the threshold of the welds and joints in the pipeline; ultimately producing a huge explosion seen from space[2]. This is another excellent example of 'kinetic' consequences of a cyber-attack as discussed by the Tallinn group; however, it's interesting to note that this was similar to the Stuxnet attack on Iran in that this was a "supply chain hack," meaning it was an attack that targeted the components or hardware of the target. As for liability in this case, the part was initially stolen.

The fear however of such attacks in the future have only risen since 1982 as increasingly governments and militaries are dependent on information communication technology systems to operate. At a cyber defense forum in 2012, all the attendees where polled and asked what was their biggest perceived threat to national cyber security. Not surprisingly, the largest portion of answers at 34% turned out the be attacks by foreign states; however, 10% of those polled cited individual hackers and organized crime as the biggest threat, while a mere 1% answered none of the options listed[3]. Now, no conclusions can be drawn directly from this quick poll, but it's clear that the largest perceived threat from the cyber defense community is attacks from foreign states. This is reflected by the statements of Richard A. Clark, the United States government expert, who defined "cyber warfare" as:

> *"actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption*[4]."

This, combined with various similar definitions of the topic, point to two main elements that must be present for cyber warfare to occur:

1. Nation-state commitment
2. Intent of the offensive

However, this is far too narrow of a definition for cyber warfare, and speaks to the logical fallacy that many experts still fall prey, that warfare in the digital realm is still tied to the antiquated

---

[2] Maitra, A. (2015). Offensive cyber-weapons: Technical, legal, and strategic aspects. *Environment Systems and Decisions, 35*(1), 169-182

[3] Ibid.

[4] Ibid.

concepts of nations. Cyber-attacks by foreign states by no means encompasses all cyber-attacks, and it's short sighted to limit the definition in such a way because as terrorists or other non-state actors develop their methods technologically, there will be situations where a country could fall under protracted cyber-attacks.

As for the 'intent of the offensive' this can easily be seen from Stefano Mele's research into cyber weapons, where he gives the first legal definition of one:

> "A cyber-weapon is [an] appliance, device or any set of computer instructions designed to unlawfully damage a computer or telecommunications system having the nature of critical infrastructure, its information, data or programs contained therein or pertaining there to, or to facilitate the interruption, total or partial, or alteration of its operation[5]."

Here, the intent as Clark describes it, is built into the software or hardware, rendering it a weapon. The creator justifiably is aware from the outset of the intent of his or her product. The important element of intent to cause 'damage or disruption' in Clark's definition of cyber warfare are inherently present in Mele's definition of a cyber weapon, just the state attribution section is missing. That however, is a bigger issue.

Thomas Ridd argues that every single incident of a cyber-attack to date relies upon the problem of attribution. They are "sophisticated forms of espionage, sabotage, and subversion" and as a result depend almost entirely on the anonymity that cyber-attacks afford[6]. In a stunning example of this, Koblentz highlights a famous cyber-attack against a conglomeration of five multinational oil companies, code named "Night Dragon." The attackers stole gigabytes of highly sensitive commercial information about western energy development practices, essentially trade secrets and government contract details. Investigators were later able to track the IP addresses of the perpetrators back to Beijing, and even were able to confirm that the attacks occurred between 9 a.m. and 5 p.m. Beijing time, suggesting that the attacks were done by someone who was operating on a traditional government working schedule; however, even though all indications were that someone or a group of people who were affiliated with the Chinese government carried out the attack, there was no conclusive evidence and Chinese officials simply denied any involvement[7]. Now this clearly was not an attack on a critical infrastructure, but it underlines one of the greatest challenges facing national cyber security experts, an issue that scholars highlight but offer no real solution to when proposing international frameworks for cyber weapons.

One of the more promising proposals developed from the successes of the Chemical Weapons Convention that entered into force in 1997. Of particular interest to cyber weapons legal scholars are the specific articles that confer obligations upon states, namely articles 1(2) and 1(4):

> 1*(2). Each State Party undertakes to destroy chemical weapons it owns or possesses, or that are located in any place under its jurisdiction or control, in accordance with the provisions of this Convention.*

---

[5] Mele, Stefano. Legal Consideration on Cyber Weapons and their Definitions. Journal of law and cyber warfare. Vol. 3 No. 1 pp. 52-69 2014

[6] Koblentz, G., & Mazanec, B. (2013). Viral Warfare: The Security Implications of Cyber and Biological Weapons. *Comparative Strategy, 32*(5), 418-434.

[7] Ibid

> *1(4). Each State Party undertakes to destroy any chemical weapons production facilities it owns or possesses, or that are located in any place under its jurisdiction or control, in accordance with the provisions of this Convention*[8].

Legal scholars like Geers point to the wording of these articles as bright spots of state responsibility for actions within their jurisdiction as 1(2) and 1(4) makes clear that even if they're not state sponsored, the state has the obligation to monitor and stop any such activities[9]. Curiously, the issue of cyber jurisdiction is glossed over a little in Greer's analysis, however it's clear that he supports the idea of cyber infrastructure in a state's jurisdiction as comprising of that state's territory and therefore would be subject to the same obligations as chemical weapons monitoring should the wording be similar.

While this offers a good base for comparison of chemical and cyber weapons, there are inherent issues with the rote transfer of principles between the Chemical Weapons Convention and the imagined Cyber Weapons Convention, which Geers to his credit points out. He lists 5 such principles that are absolutely key to the functioning and success of the CWC:

1. Political Will: In the early 1990s, the political will to create such a convention for chemical weapons was high, as Bill Clinton and Boris Yeltsin agreed. In today's world, such a political will for restraint in the field of cyber warfare doesn't exist among the key players it would need to be successful. As just a singular example, one could point to the disagreement that arose in 2017 during the meeting of the United Nations Group of Governmental Experts over the applicability of humanitarian law in cyberspace[10].
2. Universality: This is more about the subject itself than the applicability of the law, although that is universal as well. Greer's point was that chemical weapons are simple to produce and their raw materials are widely available, the combination of those two factors is what drove the importance of the CWC into the minds of political leaders around the world. Similar comparisons can certainly be drawn between chemical and cyber weapons in this context, as the materials are even easier to obtain and the specialized knowledge to create them is also widely distributed around the world today. In fact, Geers mentions the ease with which non-state actors can procure such weapons[11], though his fears seem to surround terrorist groups, which perhaps owes to his definition of cyber weapons being in line with Mele's as attacks on critical infrastructure would have a political or ideological motive, which marginalizes the economic motives but the fact of universality remains the same.
3. Assistance: Another bright spot in the CCWC is the multitude of assistance programs offered by the organization setup under this convention, The Organization for the Prohibition of Chemical Weapons (headquartered in The Hague). They offer a number of monetary and legal assistance programs from destruction of stockpiles/production center aid to advocacy in the event of an international incident involving chemical weapons. In terms of aid for state obligations, this organization is

[8] Chemical Weapons Convention, 1997.
[9] Geers, K. (2010). Cyber Weapons Convention. *The Computer Law and Security Report, 26*(5), 547-551.
[10] United Nations Group of Governmental Experts, 2017
[11] Ibid, Geers.

invaluable and Geers as well as many other scholars point to this as a main factor of the convention's success; similarly he states that a complimentary regime could easily be setup for a cyber weapons convention as many countries around the world already have CERTs (Computer Emergency Response Team) setup in their respective jurisdiction. The only difference is CERTs aren't necessarily setup to monitor internal development, but their function could be changed to suit treaty obligations.

4. Prohibition: The efficacy of this principle is demonstrated by Geers in statistics of verifiable destruction of chemical weapons stockpiles and munitions. By 2010 over 50% of the world's declared chemical agents stockpiles had been destroyed. By 2012, it was estimated that nearly 90% of the world's stockpiles had been destroyed. While seven nations still lay outside the obligations of the CWC treaty, Geers notes that since 1997, no new states had acquired chemical weapons[12]. This stands in stark contrast to the Nuclear Non-Proliferation Treaty, which has been in force for much longer since 1968, but the results of which have seen the number of nuclear proficient countries raise from five to nine. As for the translation to cyber weapons, malicious code is notoriously difficult to define, and probably the biggest obstacle to prohibition is the issue of attribution. Geers admits this openly and contends that the only way forward is for a concerted international effort to develop technological and legal advances that would make attribution an achievable goal. Considering the stealthy nature of cyber warfare however, he offers no further solutions.
5. Inspection: Under article 5(3) of the CWC all chemical weapons production facilities are subject to on-site investigations. And since its inception in 1997, over 4000 sites in 81 member states have been subject to inspections to ensure compliance, which is clearly a success as there were just over 5000 chemical weapons production facilities worldwide at the time Geers wrote this article[13]. However, contrasting that with cyber weapons production facilities, which could be something as simple as a laptop points to the near impossibility of similar inspection regimes. To his credit, Geers cites several internet service provider level monitoring schemes from China's "Golden Shield Project" to the European Union Convention on Cybercrime, to Russia's SORM and the United States Patriot Act, but the issue remains the same, the amount of traffic data that would need to monitored is simply something we are currently unable to deal with.

To further the debate on the inspection issue, Roscini throws some weight into the actual legality of international monitoring through the framework proposed in the Comprehensive Nuclear Test Ban treaty, specifically article IV(A)(5):

> *(5). For the purposes of this Treaty, no State Party shall be precluded from using information obtained by national technical means of verification in a manner consistent with generally recognized principles of international law, including that of respect for the sovereignty of States*[14].

As Roscini points out, the specific wording that includes the phrase "consistent with generally recognized principles of international law," presents an issue. This would presumably include surveillance methods such as remote sensing or satellite surveillance, but not activities

[12] Geers, ibid.

[13] Geers, ibid

[14] Comprehensive Nuclear Test Ban Treaty, page 35.

that would violate the sovereignty of a state[15]. Unfortunately, this is arguably the case for intrusion into the cyber infrastructure of another state. So as it stands this would amount to a breach in the monitoring activities of the international community even for what would be considered remote sensing surveillance. Simply put, there is no middle ground in cyberspace where one state may conduct surveillance without violating another's territory.

Perhaps a different angle can be in the classification and methods used to deal with cyber-attacks or intrusions. To this end, O'Connell defines two distinct classes of cyber-attacks:

-CNE: Computer Network Exploitation; this includes non-physical kinetic consequences like espionage, and cyber-crime/theft.

-CNA: Computer Network Attacks; where the actual computer network is harmed or stalled due to the nature of the attack. These are also classified a 'serious attacks' by O'Connell and several well-known examples are given; the 2008 attack on Georgia's government and health system website in coordination with a Russian offensive in the north of the country[16], the Stuxnet virus that incidentally caused actual physical destruction of centrifuges in Iran's nuclear enrichment program.

The most interesting CNA attack to discuss, which hits at the heart of the issue, is the 2007 attack on Estonia's government websites. In response to the on-going attack, Estonia enlisted NATO, United States, European Union, and Israeli tech experts to trace the source of the attack. This group was ultimately unable to pinpoint the exact source of the source however, as many computers around the world had been high-jacked to carry out the cyber offensive. Owing to recent developments within the country of Estonia however, it was highly likely that the attacks were directed by or at least facilitated by the Russian cyber infrastructure. To which Estonia called for military action of some kind, which subsequently went unanswered because of the issue of attribution once again.

If attribution could be achieved however, what could be the legal response to such a non-violent (in the traditional humanitarian context) attack? Well, this where O'Connell makes a rather clever contribution, pulling from the legal defense developed by Bowett during the 1956 Suez Crisis, regarding armed invasion as a response to non-violent attacks. The defense rests on an 1841 correspondence over the sinking of an American ship called The Caroline by British forces. The correspondence confirmed that at the time, customary international law permitted the use of armed force in self-defense in response to a non-violent attack if the necessity was 'instant', 'overwhelming', and 'leaving no moment for deliberation[17].' While this may seem like an intriguing option, and a legally valid excuse for the use of armed force in response to a cyber-attack, it's also a very heavy handed approach as O'Connell states himself. The problem, he contends, with current discourse on cyber security is the issue of governments resulting to the militaristic angle or paradigm as a response. He attributes this to the fact that nearly all of the legal scholars during the advent of cyber warfare had a military background; Michael Schmitt[18], Walter Gray Sharp, and George Walker as the U.S. examples. It's an interesting notion and does

---

[15] Roscini, M. (2014). Cyber Operations as Nuclear Counterproliferation Measures. *Journal of Conflict and Security Law, 19*(1), 133-157.

[16] O'Connell, Mary Ellen. Cyber Security Without Cyber War. Journal of Conflict and Security Law. Oxford University Press, 2012.

[17] O'Connel Ibid.

[18] Michael Schmitt was one of the foremost leaders of the group that developed the Tallinn 2.0 Manual.

lend some credence to the idea that most responses coming from the legal academic field have a distinctly militaristic flavor. Take for instance Sleat's description of how cyber warfare fits into the Just War Theory:

> *"…any entity that disrupts or endangers the well-being of the infosphere becomes a licit target, and that it becomes a moral duty for all other entities to prevent that licit entity from causing more evil*[19]*."*

It may not sound inherently militaristic, but consider the language used such as 'licit target' which speaks to the principle of distinction in humanitarian law; as well as the 'moral duty' being a call-back to political justifications for armed conflict in the past[20]. O'Connell argues that this is one of the main reasons why the issues surrounding cyber warfare are unable to move forward in the international community.

The final consideration in this section will be given to a short discussion on regional cyber security defense collectives and their issues relating to non-state actor cyber activities. For clarity, the convention being discussed is the African Union Cyber Security Convention (AU CSC), it should be noted that additional conventions have been adopted by the Economic Community of West African States for example, however as a whole the issue of territoriality and jurisdiction persist. Article 28 of the AU CSC reads as follow:

> *"State parties that do not have agreements on mutual assistance in cyber- crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis*[21]*."*

As Orji points out in his analysis of this convention, the entire systems rests on the assumption that states will individually seek out bi-lateral agreements and accept the principle of double criminality between their jurisdictions without giving an international legal framework to do so. This creates in his words cyber safe havens from criminals to continue their illicit activities without the threat of extradition to a country where their activities cause actual harm. It's a real issue considering the global nature of cyberspace; however, there is no current international agreement that can remedy this for the entire world. The EU Convention on Cybercrime currently has only 67 signatories from every continent, and even within the party states the issues of jurisdiction and extradition remain.

B. Private Military Companies and their responsibilities and limits

---

[19] Sleat, M. (2018). Just cyber war?: Casus belli , information ethics, and the human perspective. *Review of International Studies 44*(2), 324-342.
It should be noted that Sleat here considers non-violent attacks on the infosphere to constitute acts of war given all the other precursors are also in line.

[20] Most notably, this can be observed in the justification of the *lege ferende* of the Responsibility to Protect, the 'moral duty' is often used to justify breaches of international law or extra-judicial activities.

[21] Orji, Uchenna Jerome. Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation? 2015 7th International Conference on Cyber Conflict. NATO CCDCOE Publications

It is more feasible to begin a discussion on private military companies (PMCs) with examples and a study in national legislation before moving on to the overarching trends in international law. As such, the situation in the United Kingdom will be the main focus of this section primarily because of their interplay with both European Union laws and international law while head-quartering the second most of such companies (second only to the United States). For a brief overview, PMCs throughout the world are without a legal definition in either national or international law. The leading PMCs are: Control Risks; Dyncorp; Executive Outcomes (Disbanded in 1999); Kellogg; Brown and Root; Military Professional Resources, Inc.; and Vinnel Corp. And together their theaters stretch across many different regions including: Afghanistan, Angola, The Democratic Republic of the Congo, Congo, Ethiopia, Iraq, Eritrea, Kashmir, Liberia, Sierra Leone, and the former Yugoslav States. It's also important to note that they are not only employed by governments but also business enterprises such as banks and mining companies, human rights organizations and peace keeping agencies[22]. So they aren't the traditional definition of mercenaries as they also engage in peace-keeping efforts and general security for commercial enterprises in hostile regions. It may also seem as if they are secondary to traditional militaries; however, as a report in the Guardian illuminated in 2003:

> "Private military companies have penetrated western warfare to such an extent that they are now the second biggest to coalition forces in Iraq after the Pentagon…The US military would struggle to wage war without them[23]."

While that is a fast growing and extremely lucrative industry in the United States, the United Kingdom also hosts a number of these companies and their domestic legislation paints a good picture of the approach governments are taking considering regulation.

In U.K. domestic legislation surrounding PMCs rests on a somewhat antiquated act from 1870, the Foreign Enlistment Act, of which section 4 is of particular note:

> *"If any person, without the license of Her Majesty, being a British subject, within or without Her Majesty's dominions, accepts or agrees to accept any commission or engagement in the military or naval service of any foreign state at war with any foreign state at peace with Her Majesty, and in this Act referred to as a friendly state, or whether a British subject or not within Her Majesty's dominions, induces any other person to accept or agree to accept any commission or engagement in the military or naval service of any such foreign state as aforesaid, He shall be guilty of an offence against this Act, and shall be punishable by fine and imprisonment, or either of such punishments, at the discretion of the court before which the offender is convicted[24]."*

This act includes the definition of Foreign States to be "princes, colony, province, or any peoples of a province". Notably it doesn't include guerilla movements or stateless fighters, which could account for some of the confusion in litigation, and help explain why apparently, there has never been a successful conviction under this act. The Terrorism Act of 2000 does help to bolster domestic legislation against PMCs as is evidenced in part VI:

> *A person commits an offense if they provide instruction or training in the making or use*

---

[22] Walker, Clive and Whyte Dave (2005). Contracting Out War?: Private Military Companies, Law and Regulations in the United Kingdom. International and Compartive Law Quarterly, 54, pp 651-689

[23] Ibid. Figures for actual PMCs employed on the ground in Iraq by the U.S. ranged from 15000-25000 personnel.

[24] Ibid.

of;

-(a) firearms

-(aa) radioactive materials, or weapons designed or adapted for the discharge of any radioactive materials.

-(b) Explosives

-(c) Chemical, Biological or Nuclear weapons (as amended by section 120 of the Anti-Terrorism, Crime and Security Act 2001)[25]

This went a long way towards being able to hold PMCs accountable for actions committed on foreign soil. And sections 59-61 of that act took it a step further and sought to give the United Kingdom exclusive jurisdiction over offenses committed "partly or in whole" outside of the U.K. territory. Sections 59-61 are increasingly important when considering any cyber aspect of PMC operations, as they would almost surely fall into the category of "partly" outside the U.K. Of last interest in criminal liability, section 59 states that a person has committed an offense if he "under the Criminal Damage Act of 1971, section 1(2) Endangers life by damaging property[26]."

The main star of domestic legislation in the U.K. surrounding PMC activity however comes not in the field of criminal law, but from the 2002 Export Control Act. This is a powerful act that allows the Secretary of State to impose transfer bans on any technology from persons inside the U.K. to persons outside the U.K.[27]. Similarly, section 3 of that act seeks to limit technical assistance, which is described as such:

"technical assistance" means services which are provided or used, or which are capable of being used, in connection with the development, production or use of any goods or technology[28]."

These two sections together are subject to the stipulations set forth in section 5 of that act which limit somewhat the power of the secretary of state, with notable respect paid to international and European Union law:

(2)Controls of any kind may be imposed for the purpose of giving effect to any [E.U.] provision or other international obligation of the United Kingdom

(3)In subsection (2) "international obligation" includes an obligation relating to a joint action or common position adopted, or a decision taken, by the [European Council][29].

Aside from basic adherences to international and E.U. law, there is a schedule of goods listed at the end of this act that will always require special permission for transfer, exportation, or

[25] Walker Ibid.

[26] Whether or not this specific section has been used in the U.K. court system, I was unable to determine, still it opens up possibilities of convictions for cyber-attacks on critical infrastructures like hospitals, energy grids, etc. essentially a CNA attack as Roscini stated. Theoretically this could be extrapolated to include loss of data as property, especially if it is data related to medical information.

[27] Export Control Act, section 2 on transfers.

[28] Export Control Act, section 3

[29] Export Control Act, section 5.

technical assistance. The entire list revolves around military equipment, technology, or technical assistance. What is important is subsection 1(4) which describes in detail military equipment and technical assistance:

> *In this paragraph (without prejudice to the generality of the terms)—*
> *"military equipment" includes—*
> *(a)firearms and other weapons (whether or not intended, designed or adapted for military use or in military use); and*
> *(b)goods intended, designed or adapted for military use (whether or not in military use); and*
> *"military technology" includes—*
> *(a)technology intended, designed or adapted for military use (whether or not in military use); and*
> *(b)technology intended, designed or adapted for use in connection with the development, production or use of military equipment or goods falling within sub-paragraph (1)(c)*[30].

This gives the U.K. significant control over PMCs that primarily export military equipment or technical assistance, but how effective is this system[31]?

Later in 2002 after the adoption of the Export Control Act, the publication of a "Green Paper" by the Foreign and Commonwealth Office shed some light on the intentions of the U.K. government to curb PMC activity within their territory. The publication itself was driven by the Sandline incident, where a PMC that ceased operations in 2004 called Sandline, was involved in an international incident with then president of Sierra Leone Kabbah. Defying embargo restrictions set in place by the U.N. security council, Sandline continued to fulfill arms contracts to President Kabbah through 2003. This incident by a PMC headquartered in U.K. was then considered a breach of the United Kingdom's international obligations in its failure to uphold the strict embargo. As a result, the Foreign and Commonwealth Office made its intentions very clear in the opening paragraphs of the Green Paper:

> "Bringing non-state violence under control was one of the achievements of the last two centuries. To allow it again to become a major feature of the international scene would have profound consequences. Although there is little risk of a return to the circumstances of the seventeenth and eighteenth centuries when privateers were hard to distinguish from pirates, and corporations commanded armies that could threaten states, it would be foolish to ignore the les- sons of the past. Were private force to become widespread there would be risks of misunderstanding, exploitation and conflict. It would be safer to bring PMCs and PSCs within a framework of regulation while they are a comparatively minor phenomenon[32]."

In the Green Papers, a full or partial ban on PMCs was discussed as the most effective away to curtail behavior that then cause the U.K. to breach its international obligations through a failure of regulation; however, that did not end up being the prevailing course of action as one very telling passage in the Green Papers illuminates:

---

[30] Export Control Act 2002, Schedule for categories of goods and technical assistance

[31] An example of this is shown through the DynCorp case involving their storage of "gator weapons" for the U.S. military in Bahrain.

[32] White, N. (2016). Regulation of the Private Military and Security Sector: Is the UK Fulfilling its Human Rights Duties? *Human Rights Law Review, 16*(3), 585-599.

> "An Outright ban on the provision of all military services would deprive British Defense exporters of contracts for services of considerable value. Since exports of defense equipment are frequently dependent on the supplier being able to provide a service package a large volume of defense export sales would be lost in addition to the value of the services themselves. It is not possible to estimate what this could amount to but it is clear that the cost to British Industry would be considerable. Significant losses could also impact on the defense industrial base to the detriment of our defense capability[33]."

While the Green Papers are clearly not hard law, it does represent the political will of the U.K. government in relation to harsher regulations of its defense industry.

This issue was again revisited in 2009 after the Montreux Document was published in 2008[34], with the U.K. government ultimately setting up a two-tiered system of 'government-backed self-regulation at the national level, and adherence to international norms[35].' As white highlights rather acidly:

> "Although there are binding norms of international law applicable to the UK Government, none of these have been designed to specifically cover PMSCs or their activities, so it is true to say that the system of PMSC regulation being developed by the UK is a purely voluntary one[36]."

A further international document regarding PMCs was put forth in 2010 called the International Code of Conduct for Private Security Providers, which outlines further the concept of "Corporate Social Responsibility" and adherence to human rights law. From the United Kingdom's point of view, it's international obligations towards human rights stemming from regulatory controls of their PMCs is for a matter of these international guidelines, not domestic legislation or further regulatory control[37].

In a brief discussion on arms trades in the context of human rights law at the state level, in this example also involving the U.K. for coherence, the case study of the Saudi-led coalition in Yemen yields some interesting insights. The Saudi coalition is a group of nine countries from the Middle East and Africa that have conducted a number of air strikes into Yemen territory that non-governmental organizations and human rights watchers have largely condemned for their apparent disregard for humanitarian law. These strikes rely somewhat heavily on arms trades from the United Kingdom and United States to the Saudi Air Force, some of which were under pre-existing contractual arrangements[38]. The statistics of which are quite telling in the level of assistance given, as between 2010 and 2015 the U.K. approved licenses for arms exports to the

---

[33] Clive.

[34] The Montreux Document is a non-binding agreement that attempts to set out basics of regulations for both state practice and PMC business practices at an international level. This will be discussed more in the research portion of this thesis.

[35] White.

[36] White. It's a rather pessimistic view considering the regulatory framework they have in place, whether or not it is used, the groundwork for the legal validity of future restrictions has been laid. The "voluntary" nature of the current U.K. regulations could more aptly be attributed to the economic concerns of their defense industry.

[37] Ibid.

[38] Musa, S. (2017). The Saudi-Led Coalition in Yemen, Arms Exports and Human Rights: Prevention Is Better Than Cure. *Journal of Conflict and Security Law, 22*(3), 433-462.

Saudis that amounted to 6.7 billion English pounds, with exports from the beginning of the air strike in Yemen to the latter part of 2015 totaling 2.8 billion pounds.

In the first day of the Saudi-led intervention, both Amnesty International and SaferWorld had condemned the airstrikes, citing past Saudi incursions into Yemen from 2009 using U.K. Tornado fighter jets. As time went on in this conflict, the numbers became even more grim:

> "Figures from 25 October 2016 show that 19 months into the conflict, there have been approximately 44 000 casualties, which included 7100 deaths. In the period between March 2015 and October 2016 alone, the majority of deaths and injuries were caused by coalition airstrikes, including 4125 deaths and 7207 injuries[39]."

High numbers of children were being killed in these air strikes, which prompted a United Nations investigation in which the U.N. group of experts determined:

> "the coalition led by Saudi Arabia did not comply with international humanitarian law in at least 10 air strikes that targeted houses, markets, factories and a hospital[40]."

It should be noted here that the U.K. was not directly involved in these attacks, it was merely providing technical assistance to the Saudi coalition, and as Musa rights points to the decision in the *Nicaragua* case sets a higher threshold for control in terms of state responsibility. However, the Cluster Munitions Convention comes into play when considering that one of its obligations towards states party to the convention clearly says that states "must not assist, encourage, or induce anyone to violate any activity prohibited by this convention[41]." The technical assistance given by the U.K. to the Saudi Air Force concerning the operation of its Tornado fighter jets could at the very least be considered a failure of due diligence in the arms deal conducted by the U.K. government. It may be unclear why this is relevant when clearly this was a state actor selling to another state actor. The answer lies in the failures of due diligence, both in the past operating functions of Saudi Arabia in the region from their strikes in 2009, to the technical assistance that was then used to deliver illegal weapons in the subsequent airstrikes. It highlights the fact that even amongst one of the most liberalized states in the world, a cornerstone of self-regulation in arms deals isn't being followed at the state level, despite the expectations that its PMCs will do so.

That expectation of "due diligence" is a large part of one of the three pillars of a widely cited self-regulation tool of international law, "Corporate Social Responsibility." It was developed by John Ruggie in 2008 as a way to further integrate international human rights law into business ethics and on the surface consisted of three pillars, "Protect, Respect, and Remedy." IN the three years that followed the release of this initial idea, Ruggie worked further to create implementation strategies for corporations. In his explanation, the reasons for doing so were:

> "Protection of human rights is the role of the state expressed as a duty; respect for human rights is the second pillar and is the role given to corporations. The difference in liability for states and corporations expressed as 'duty' and 'respect'

[39] Musa. In these figures, "casualties" is meant to mean serious injury.
[40] Ibid.
[41] Musa. The Saudi-led air strikes allegedly involved cluster munitions that were mounted specifically on U.K. Tornado Fighter Jets.

> reflects the established view that no legal liability attaches to non-state actors in international law[42].”

And that quote highlights one of the main issues with Corporate Social Responsibility(CSR), in that no legal liability attaches to non-state actors in international law. It should be fairly self-evident considering signatories to the International Covenant on Civil and Political Rights are states, not corporations. Ruggie firmly believed that the remedying of human rights violations was the responsibility of the corporations themselves, expressing his view that all corporations should have a mechanism which victims can file grievances under and seek recourse. Failing that, corporations should engage in a legitimate process driven by the state to find a remedy.

The more important pillar in terms of everyday business dealing, especially in the defense industry, is the exercise of due diligence in an effort to protect potential victims of human rights abuses. According to Wheeler, this concept of due diligence has four elements, the first of which is an obligation by the corporations to institute a human rights policy, the following three elements revolve around the ideas of transparency, external participation, and independent verification[43]. It was Ruggie's concern that if human rights practices were not fully integrated into the daily business practices of a corporation, but were added as an after-the-fact cosmetic[44], then it would be highly ineffective at best. He even goes on to state that employees should be trained in human rights practices and how to avoid violations. It is a nice sentiment, but it is hard to imagine how this would transfer to the defense industry, especially in the production on small arms. According to one study, small arms were the only weapons used in 46 out of 49 major conflicts in the world during the 1990s, in which 80-90% of the casualties were civilians, a staggering increase from the world war two figures of just 5%, and were the single biggest cause for the rise in refugees. Further and perhaps more appalling, small arms are light weapons and can be used by child soldiers, of which there are over 300,000 under the age of 18[45]. So how then can a corporation square CSR responsibility with the nature of the industry they are in?

One potential point of interest could lay within government regulation of arms dealers. In a study of arms dealer practices within the United States, Green comes to a startling conclusion:

> “The industry's marketing and distribution system provides one illustration of the problem. Federal regulations require that gun dealers be licensed, but the ATF's supervision of this process is minimal. Virtually anyone over 21 without

---

[42] Wheeler, S. (2015). Global production, CSR and human rights: The courts of public opinion and the social licence to operate. *The International Journal of Human Rights, 19*(6), 757-778.

[43] Wheeler.

[44] Cosmetic in Wheeler's interpretation in this section most likely refers to the kind of public relations campaign a company must undergo after a major blunder. Essentially it's just a way of saying meaningless.

[45] Byrne, E. (2007). Assessing Arms Makers' Corporate Social Responsibility. *Journal of Business Ethics, 74*(3), 201-217.

> a criminal felony record can be licensed, with the result that there are more federally licensed firearms dealers in this country than gas stations[46]."

While this may have no bearing in the discussion as these are private dealers and not corporations bidding on government contracts or making foreign arms deals, the lack of governmental regulation is stark. One potential answer to this in the context of CSR and the defense industry is that crucial element of due diligence.

An example, or failure, of this in recent events is the widely publicized Heckler and Koch/Mexico scandal that just two years ago resulted in a negligible corporate fine. From 2006 to 2009, the German arms manufacturer Heckler and Koch completed an arms trade deal with the government of Mexico, in violation of national laws[47]. It had been determined prior to the sale that there was a high risk of human rights abuses in several Mexican states and arms sales were temporarily halted. Heckler and Koch then proceeded to sell 4000 G36 (assault rifles) to Mexican authorities with a strategy of using end-user license agreements that specified the states in which the guns were to be used, as a shield from domestic prosecution. Ultimately these guns were used to commit human rights abuses in the affected states, including the high-profile murder of Iguala Guerrero in 2014. Heckler and Koch were then brought to court in Stuttgart and the lengthy court appearance resulted in a scant 4.2 million dollar fine[48]. In fact, Heckler and Koch was allowed to maintain its arms manufacturing facilities, which included facilities in the states of Mexico[49]. This isn't simply an example of the failures of due diligence, but the complete neglect of that element of CSR, reminiscent of the failures of the U.K. government in Saudi arms deals.

This almost complete lack of supplier-side regulatory control is perhaps best explained at an international level by Cooper, who states:

> "…current conventional arms transfer control mechanisms are inadequate to deal with the future challenges of weapons circulation, because they overwhelmingly concentrate on affecting the supply side of the arms trade equation therefore failing to take sufficient account of two critical trends. Firstly, that a lack of 'political will' has combined with strategic and commercial interests to make most supplier-based export controls little more than acts of tokenism[50]."

The second factor Cooper alludes to is the emerging trend of dual-use technology integrated in the illicit arms trade network; however, his first point is incredibly strong in light of the examination of U.K. resistance to regulatory control, to the inherent failures of self-regulation within the defense industry. One success that Cooper accedes to is the non-proliferation of nuclear, biological, or chemical weapons. As discussed earlier the international legal mechanisms for these types of weapons is relative strong and as Cooper points out, 'enforced with a high degree of rigor.' He then goes on to highlight the issue with transferring the success of non-proliferation from weapons of mass destructive to small arms by discussing the

---

[46] Green, R. (2000). Legally Targeting Gun Makers: Lessons for Business Ethics. *Business Ethics Quarterly, 10*(1), 203-210.

[47] The War Weapons Control Act.

[48] NPR.

[49] Green.

[50] Cooper, N. (2006). What's the point of arms transfer controls? *Contemporary Security Policy, 27*(1), 118-137.

effectiveness of trade embargos in conflict zones. A quote from the United Nations Experts panel on Liberia explains the futility:

"Despite nine years of an embargo on arms and military equipment to Liberia, a steady supply of weapons has reached the country. Indeed, in their conversations with the panel, the Liberian authorities appeared not bothered about the embargo and never complained about it[51]."

This in Cooper's opinion is due to the fact that there is an extensive network, or black market, of arms dealers willing to push past embargos, which may very well be the case. And yet, there are still examples of PMCs like Sandline and arms manufacturers like Heckler and Koch that consistently skirt trade bans with little domestic consequences.

The E.U. currently constitutes about a third of the world's arms trade suppliers. And as a result, the European Union attempted to put forth a regional arms control regime in 2008 through the Council Common Position 2008/944/CFSP. This position would become the cornerstone of that regime, but was fraught with issues in specificity of language, as noted by a report from the British NGO SaferWorld:

> "[a]mend the language of the [regime] or produce new guidance on criteria implementation which reduces the current excessive room for Member States to make decisions contrary to the spirit and intent of the [regime] and reduces the incidence of Member States making contradictory and contrary decisions[52]."

This issue was later amended in 2014 with the E.U. adoption of the Arms Trade Treaty on a larger scale; however, it's still useful in positing potential solutions to any cyber arms control regime to discuss the basic 8 tenants of the original council common position:

> -Respect for the international commitments of the member states of the EC, in particular, the sanctions decreed by the UN Security Council and those decreed by the EC, agreements on non-proliferation and other subjects, as well as other international obligations.
>
> -Respect for human rights in the country of final destination.
>
> -The internal situation in the country of final destination, as a function of the existence of tensions or internal armed conflicts.
>
> -The preservation of regional peace, security and stability.
>
> -The national security of the member states and of territories whose external relations are the responsibility of a member state, as well as that of friendly and allied countries.
>
> -The behavior of the buyer country with regards to the international community, in particular, as regards its attitude to terrorism, the nature of its alliances and respect for international law.

---

[51] Ibid.

[52] Hansen, S. (2016). Taking ambiguity seriously: Explaining the indeterminacy of the European Union conventional arms export control regime. *European Journal of International Relations, 22*(1), 192-216.

-The existence of a risk that the equipment will be diverted within the buyer country or re-exported under undesirable conditions.

-The compatibility of the arms exports with the technical and economic capacity of the recipient country, taking into account the desirability that states should achieve their legitimate needs of security and defense with the least diversion for armaments of human and economic resources[53].

A bulk of the ambiguity seems to have arisen from the lack of action in addressing how to implement these criteria. Indeed, it seems that the European Council was "merely hopeful that a 'common approach' based on 'criteria of this nature' might lead to a 'harmonization of national policies[54]'". The actual criteria did not ask member states to stop exporting if any of the criteria weren't meant, or provide any guidance on when reception conditions in the intended country violated any criteria at what point would a license denial be warranted? So it seems as though this regime, while noble in its intent was lacking any sort of actionable guidelines and did nothing to address the mains issues it discusses. Moreover, member states do have the option of deviating from E.U. law, though such deviations would generally require states to express great concern for social interests deemed more appropriate than the economic interests of the Union[55], which would be hard argument to make in arms deals.

As for the larger international picture, the regulation and control of the defense industry is closely linked with the protection of sensitive information. In some facets, the protection of information predated the defense industry[56]. And since any discussion on the regulation of the cyber weapons industry would invariably circle back to the secretive classification of information by governments in whose territory these corporations are head-quartered, it is imperative to take a brief look at how select countries deal with information in the defense industry[57].

First, in the United Kingdom, the Official Secrets Act was passed in 1898 and has been subject to periodic reviews and amendments throughout the years. This act makes it a criminal offence for any person who is bound by it to pass on classified information to another person not bound by the act[58]. It should be noted that this is an Act that remains for the entirety of a person's life, but other than that is a pretty standard version of classified information legislation.

In the United States, the systems is a little more complex, but revolves around the same idea of authorized persons. In their respect, it has more to do with classifications of information in an attempt to protect both business and military technologies. Different levels of security clearances are given to private-sector people and a "robust government

---

[53] Hansen. It should be noted that these are generalizations that are reflected in the much more detailed versions of the 2008 position; however, it doesn't change the ambiguity issue.

[54] Hansen.

[55] Koutrakos, P. (2010). The Notion of Necessity in the Law of the European Union. *Netherlands Yearbook of International Law, 41*, 193-218

[56] Heidenkamp, H., Louth, J., & Taylor, T. (2013). IV. The Regulation and Control of Defence Businesses. *Whitehall Papers, 81*(1), 98-137.

[57] Especially given the fact that the majority of cyber-attacks are CNE and result in crucial information for military or economic operations.

[58] Heidenkamp

direction of standards relating to defense sites, whatever their ownership[59]." By requiring compliance with government directions, this means that the U.S. government retains a modicum of control even over private sector companies dealing with classified information. In Heidenkamp's words for example, "It is not possible to act as a defense contractor without embracing these security standards as they are backed by federal and state statutes." All in all, it's a promising system for implementing regulatory reforms. The actual legal instruments involved are the United States Espionage Act of 1913, where the classified information of the defense industry is a specifically protected type of information.

C. Corporations and their relation to International Criminal Law.

In recent years there has been some movement in international law to prosecute corporations for violations of human rights. An example of this is examined by Amos in her first article, describing managers of German corporations being prosecuted for the forceable removal of rural populations in Sudan for the purposes of dam construction; however, she concedes that a comprehensive formal structure is still missing[60]. In a separate article, Amos gives the basis for what she terms International Economic Criminal Law (IECL). Where this differs from national economic laws, is that it seeks not to defend the economic intergrity of markets, to protect human rights from the exploitations of corporations in the interest of profits[61]. It is this concept of IECL that is of most interest to this research, as it directly applies to PMCs and their global activities. Amos lays out three forms of factual complicity:

> *-Direct complicity: ''when a company provides goods or services that it knows will be used to carry out the abuse'';*
>
> *-Indirect or beneficial complicity: ''when a company benefits from human rights abuses even if it did not positively assist or cause them'';*
>
> *-Silent complicity: ''when the company is silent or inactive in the face of systematic or continuous human rights abuse''*[62]

[59] Heidenkamp. This also takes into account private sector defense companies or PMCs.
[60] Ambos, K., & Momsen, C. (2018). Introduction: Human Rights Compliance and Corporate Criminal Liability. *Criminal Law Forum, 29*(4), 495-497.
[61] Ambos Kai. *The Foundation of Companies' Criminal Responsibility Under International Law*. Criminal Law Forum. Copyrite Springer Nature B.V. 2018
[62] Ibid

Corporations have been prosecuted for their complicity in the past, including for their complicity in war crimes and even genocide, as was the case with Lundin Energy and LafargeHolcim[63]. While Nolan, Posner, and Labowitz argue that courts are only one among many options to remedy the disparity between trans-national corporations and their liability in international law (particularly regarding human rights abuses), their solutions are focused heavily on increased labor market regulations[64]; unfortunately, this does nothing to address more serious breaches of human rights amounting to crimes against humanity, which is the focus of cyber weapon regulation attempts. The main issue, as van der Wilt puts it is that the implication of a legal entity such as a corporation require knowledge and contribution of coporate agents[65]. While his focus wasn't in the cyber realm it's important to note that the knowledge element presents itself in the Rome Statute as well, and is often indvisible from cyber weapons given the highly targeted nature of their development. The presiding theme of holding coporations legally responsible in international law, is that it's mostly based in soft law[66]. This is of course relating to Ruggie's "Guiding Principles on Business and Human Rights." However, as Simons points out there are a number of issues with this soft law approach. The main problem is that it has allowed national law to develop protections for corporations. An example is that under national or domestic law, corporate actors may use shell corporations to help shield the parent company from legal liability[67]. While this hasn't played out yet in the realm of cyber weapon development, such loopholes would ultimately dismantle any attempt at regulation of cyber weapon exports.

Another possible angle towards the prosecution of corporations comes in the form of the Corporate Manslaughter Act of 2007[68]. This focuses again on the individual culpability of high-level managers in offenses to force the liability of corporations into legitimate claims. Price makes an interesting contribution to this discussion in the context of corporate liability, where he argues that the insistence on individual culpability of high-level managers, should be seen as an indication of corporate structure, i.e. the effect this has on directing employees' work within the organization[69]. Sullivan similarly argues that it is legally justifiable to claim that a corporation is guilty of a criminal conspiracy based on this emphasis of high-level management culpability[70].

---

[63] Kolieb, J. (2020). Don't forget the Geneva Conventions: Achieving responsible business conduct in conflict-affected areas through adherence to international humanitarian law. *Australian Journal of Human Rights, 26*(1), 142-164.

[64] Grear, A., & Weston, B. (2015). The Betrayal of Human Rights and the Urgency of Universal Corporate Accountability: Reflections on a Post- Kiobel Lawscape. *Human Rights Law Review, 15*(1), 21-44

[65] Van der Wilt, H. (2013). Corporate Criminal Responsibility for International Crimes: Exploring the Possibilities. *Chinese Journal of International Law, 12*(1), 43-77.

[66]Pieth, M. (2018). Corporate Compliance and Human Rights. *Criminal Law Forum, 29*(4), 595-601.

[67] Simon, Penelope. *International Law's Invisible Hand and the Future of Corporate Accountability for Violations of Human Rights.* Journal of Human Rights and the Environment, Vol. 3 No. 1, March 2012 pp. 5-43

[68] This is an act of national legislation within the U.K. parliament.

[69] Price, Luke. *Finding Fault in Organizations-Reconceptualizing the Role of Senior Managers in Corporate Manslaughter.* Legal Studies, Vol. 35 No. 3, pp. 385-407.

[70] Sullivan, G. (1996). The Attribution of Culpability to Limited Companies. *The Cambridge Law Journal, 55*(3), 515-546.

While this act is at the national level, Price's examination of the culpability tied to the corporate structure is of particular interest when considering breaches of international law, especially when these corporations often work across multiple jurisdictions. In fact, precedent set by the Nuremberg Trials has laid the groundwork for individual criminal liability within organizations under international criminal law[71]. In an effort to define corporate cooperation and subsequent benefits from dealing with military dictatorships, Kaleck distinguishes three different strategies of these such corporations:

> "(a) cases in which corporations profit from state vio- lence, (b) cases in which the regime's human rights abuses are facilitated by providing the necessary means and (c) cases in which corporations directly support repression without direct economic benefit[72]."

The example used was of the Shell Corporation's complicity in the death of the Ogoni 9 by the Nigerian government. This case was eventually settled in in a civil lawsuit, where Shell was found to be complicit and ordered to pay $15.5 million to the victims[73]. While this wasn't an example of criminal liability it was a step towards legal prosecution of corporate entities under Rome Statute violations. While Kaleck's example didn't touch on ICL, Farrell suggests two modes of attribution that would be especially useful within the corporate context, co-perpetration and aiding and abetting. The first deals mainly with the accused committing a criminal act in concert with another individual; while the second is more about business dealings that perpetuate the situation or profit from it[74]. While the *mens rea* for aiding and abetting is unclear from Farrell's explanation as he relies mainly on the results from the Frans Van Anraat case, wherein knowledge of the ultimate outcome (the use of materials supplied by Anraat to make chemical weapons which were ultimately used on civilians) was unnecessary under Netherlands law to obtain a guilty verdict. This issue of knowledge however would again be somewhat subsided in the realm of cyber weapons as they are highly targeted in their development stage. Stewart goes to the far other end of this conversation by suggesting that traditional mode of liability are essentially meaningless as attribution requirements of the Rome Statute are not enforced within domestic legislation of the states party to the treaty[75]. What all this leaves us with, is an increasingly complex mosaic of domestic and international law with respect to corporations and their liability.

---

[71] Bryk, L., & Saage-Maaß, M. (2019). Individual Criminal Liability for Arms Exports under the ICC Statute. *Journal of International Criminal Justice, 17*(5), 1117-1137.

[72] Kaleck, W., & Saage-Maaß, M. (2010). Corporate Accountability for Human Rights Violations Amounting to International Crimes. *Journal of International Criminal Justice, 8*(3), 699-724.

[73] Ibid

[74] Farrell, N. (2010). Attributing Criminal Liability to Corporate Actors. *Journal of International Criminal Justice, 8*(3), 873-894.

[75] Stewart, J. (2012). The End of 'Modes of Liability' for International Crimes. *Leiden Journal of International Law, 25*(1), 165-219

Chapter 3: Methodology

A. Methodological Approach

The aim of this research was to explore an under-developed area of legal scholarship surrounding the regulatory mechanisms involved in the defense industry and how they relate to the advent of cyber weapons and dual use technology. The main assumptions underpinning the rationale of my approach was that the majority of arms trades were done in manners consistent with legal trade; this turned out to be a somewhat false assumption as the illicit arms trade deal does present a factor that I only accounted for briefly in the literature review portion.

The main research questions driving me were then, how is the small arms trade regulated at a national and international level, and to what extent do these succeed in halting illegal trade from established defense industry companies? As the research progressed it was naturally necessary to add additional elements to those questions including the impact of non-conventional weapons on regulatory schemes.

To this end the quantitative data needed was limited, I only required sufficient data, particularly surrounding the registration of imports and exports affiliated to items listed in the Wassenaar Arrangement. As a result, the majority of my research was of the qualitative sort, surrounding case studies and treaty interpretation. The treaties and other international legal documents were analyzed with a teleological approach in accordance with articles 31 and 32 of the Vienna Convention on Law of Treaties, paying special attention to the intention of treaties such as the Arms Trade Treaty and the aim of the Wassenaar Arrangement. This sort of analytical approach was necessary to help discern the *opino juris* of the international community on these issues. Given my western academic background, my research was infused with prejudices of stricter government controls as a normality, as such this could have skewed the results as one of my case studies involved a legal system where that may not be the case.

B. Methods of Data Collection

As this was primarily a qualitative analysis, the results are largely more dependent on the approach I took in selecting cases to study. Unfortunately, there are limited cases involving corporations that develop and sell cyber weapons (even in the altered definition I presented in chapter 1). To this end, selecting cases became a matter of analyzing the business practices and relevant court documents relating to any corporation I found dealing in cyber weapons. This method produced few results, but two very promising

examples of a future trend. In relation to the qualitative analysis of existing international legal documents, my options were somewhat more open; however, I limited them to the existing structures of small/nuclear/chemical/biological weapons controls and export controls (strictly at an international level). The reason for choosing the international level for export controls was to try and determine if there was an attempted harmonization of national export controls in relation to the non-proliferation of dual-use technologies and cyber weapons. This could have been done at the national level, but would have been a multi-year study, so for simplicity and a general overview I only analyzed the international level.

For the quantitative data I needed, the Wassenaar arrangement has a database, updated annually of entries made by countries who either imported or exported the technologies or equipment listed in the arrangement. To this end it made the research more streamlined; however, I did not have a way to verify if the data was correct or complete without looking into the licenses granted by each individual country for export/import. This would have resulted in the same issue as only analyzing the international level of legal documents, so I took the data collected from their database at face value. Considering it was only used to demonstrate the growth in technology trade and had no bearing on the results, I did not consider this a big enough issue for the time investment needed to validate the data.

C. Methods of Analysis

The method of analysis I most used could be described at "thematic," in that I was searching for trends in both case law and international law development that would point to a solution for regulation of cyber weapons. This involved categorizing all the legal documents into two distinct relevant areas: international controls on arms trade (or non-proliferation), and international control on defense industry corporations. The aim of such a method was to produce both sets independently and then identify areas where they merge as potential entry points to new international law.

For the case studies, as my methods for data collection were somewhat limited, I resigned to a similar thematic approach, attempting to each case into either of the two areas above while cross-classifying them in either the fields of human rights law or international criminal law given their violations. This method proved rather unsuccessful as the cases I found had an easier basis in human rights law, despite the allegations of one involving crimes against humanity.

D. Evaluation and Justification of Methodological Choices

The methodological approaches I took were inherently necessary as this was such an underdeveloped sub-field of law that traditional case analysis and treaty interpretation would have resulted in an incomplete pictures of the factors at play, namely the interplay of cyber weaponry, defense industry corporations, and conventional/non-conventional

weapon treaties. It was precisely the nature of cyber weapons that resulted in this non-standard approach of separating treaties into different categories and looking for inflection points where they merge. The addition of case law as examples were necessary to highlight the struggle of current international and domestic laws to reconcile these two different categories in the cyber context.

Chapter 4: Results

A. The Wassenaar Arrangement

The role of the Wassenaar Arrangement in international law has not yet been fully realized, partially because of the non-binding legal nature of the arrangement, and partially because it has not attained the same level of universal recognition as other treaties such as the Chemical Weapons Convention[76]. The stated aim of the arrangement is:

> "The Wassenaar Arrangement has been established 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 destabilizing accumulations. The aim is also to prevent the acquisition of these items by terrorists."

Clearly the aim of this arrangement is for conventional arms control; however, there are other international treaties with greater political support that will be discussed later, such as the Arms Trade Treaty. So the question remains of why adhere to this agreement? Well the answer is defined in the purpose as "dual-use goods." This is a term that is often thrown around in legal discourse surrounding weapons, but is not fully articulated. It becomes clear however, when you look deeper into the list of "dual-use goods and technology/munitions." For the purposes of this research, one section is of particular interest, 4. D. 4.:

> *"Software" specially designed or modified for the generation, command and control, or delivery of "intrusion software".*
>
> *Note 4.D.4 does not apply to "software" specially designed and limited to provide "software" updates or upgrades meeting all the following:*
>
> *a. The update or upgrade operates only with the authorisation of the owner or administrator of the system receiving it; and*
> *b. After the update or upgrade, the "software" updated or upgraded is not any of the following:*
>
> *1. "Software" specified by 4.D.4.; or*
> *2. "Intrusion software"*[77].

This article in particular highlights the first concerted international effort to limit the exports or imports of software that can be considered a cyber weapon under the definition I laid out. The software described in article 4. D. 4. Can readily be described as spyware. In fact, even with the exception of upgrades, the arrangement makes clear that such code can only operate with the

[76] The Wassenaar arrangement is the successor to the Coordinating Committee for Multi-Lateral Export Controls, a cold-war era committee. The arrangement however, currently consists of only 41 member states.

[77] Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List (December 2020).

express permission of the owner. This shows a strong commitment to banning software that can violate ICCPR article 17, the right to privacy, as owners of any technology must be fully aware of whatever updates come onto their system, and "intrusive" software such as surveillance viruses are strictly prohibited. Former versions of this list had much more simplified version of this software requirement, originally positioned in section 5. D. 1. E., it prohibited dual-use software that could "perform policing functions[78]." The ambiguities of that wording could mean surveillance software or any number of police activities from remote data gathering, to facial recognition; however, with the new distinction of intrusive software, the arrangement is clearly moving towards a prohibition on exports and imports of viruses. It's possible that this is in response to the growing realization of tech companies like Israel's NSO that sell their surveillance software to state actors.

Also present in the updated list that was notably absent in the previous versions is the prohibition on imports of technology used to create intrusive software. A small section of it reads:

> *4. E. 1. "Technology" as follows:*
> *a. "Technology" according to the General Technology Note, for the "development", "production" or "use" of equipment or "software" specified by 4.A. or 4.D*
> *c. "Technology" for the "development" of "intrusive software[79]."*

It remains unclear and undefined what technology they are referring to in this section. Technology for the development of intrusive software could be something as simple as a common laptop, though it's likely they are referring to something more military-grade. Still it underscores the rising importance of non-proliferation of cyber weapons through export/import monitoring. All of the above restrictions can be categorized as attempting to prohibit the spread of software or technologies that can enable a state government or non-state actors within a state's territory to carry out a CNE attack. Recall that this is specifically related to espionage or cyber-crime activities.

There are special designations at the end of the list of prohibited technologies that bear consideration. In terms of cyber weapons, these are the ones that can cause CNA attacks, and they are designated under the 'very sensitive' list, although presumably this just means a greater obligation to report such imports/exports.

> *5.A.1.h. Counter Improvised Explosive Device (IED) equipment and related equipment...*
> *5.D.1.a. "Software" specially designed for the "development" or "production" of equipment, functions or features specified by Category 5 – Part 1 of this List[80].*

The importance of a 'kinetic' consequence for a cyber-attack is clearly of greater importance to

[78] Wassenaar Arrangement List 2019.
[79] Wassenaar Arrangement List 2020
[80] Ibid.

the party member of this arrangement. Still the entire arrangement is not legally binding and so carries no obligations; however, it is the best example of *opinio juris* towards the proliferation of cyber weapons to date, and given the control angle (the reliance on import/export notifications or license revocations) this is a viable strategy to deal with PMCs who develop and sell their products, either for CNE or CNA attacks.

B. The Case of Amesys

Amesys, standing for Advanced Middle Eastern Systems, was a tech company operating out of France in the early 2000s to the mid 2010's. They specialized in surveillance technology and operated as a PMC, distributing their technology globally to assist governments and military operations. In 2007, Amesys contracted with the Libyan government, Muammar Gaddafi's regime, to provide technology and setup an advanced surveillance center for the purposes of intercepting communication, and processing and analyzing data of the citizens of Libya. Subsequently this surveillance center was used in the systematic capturing and torturing of Libyan citizens by the Gaddafi regime.

On October 19th, 2011, the FIDH (International Federation for Human Rights, in France) and the LDH (French League on the Rights of Man) formally filed a criminal complaint against the French head-quartered company Amesys for assisting in the alleged crimes against humanity that happened in Libya. The specific basis for the complaint was stated as follow:

> "The application of the United Nations Convention against Torture 1984, and the principle of extraterritorial jurisdiction enshrined therein, gives French judges jurisdiction over crimes committed outside of France, regardless of the nationality of the perpetrator or the victim. In this instance, however, the fact that Amesys had its headquarters in France at the time that the alleged crimes were perpetrated, was enough to give the French courts jurisdiction over acts of torture committed outside France where the main perpetrators were non-French nationals – namely, agents of the Libyan State, who used surveillance equipment supplied by Amesys, who was thus rendered accomplice to their crimes, to the detriment of Libyan victims[81]."

Here it was made clear that the surveillance technologies supplied by Amesys were being used as evidence for the complicity of Amesys in crimes against humanity and violations of the right to privacy. Whether or not the legal basis was valid, this is an example of a complete lack of 'due diligence' on Amesys' part, it's hard to say that this level of oversight was intentional, but the company certainly did nothing to avoid the abuse of its technologies.

In the preliminary investigation done in 2011, the violations of the rights to privacy were

[81] FIDH report on the Amesys trial.

ultimately dropped after investigators established:

1. the Eagle equipment did not require authorisation to be exported because it was not considered war equipment; and
2. it did not need to obtain the special clearance usually required for communication interception equipment because it was not going to be used on national soil, but exclusively destined to be exported[82].

The issue of lack of export controls for PMCs has been made clear, whether from lack of political will or economic fear; however, Amesys was not classified as a PMC it was merely a tech company that offered dual-use technology. This case continued to garner public attention and soon a media firestorm erupted, which pushed the French government in 2013 to propose changes to the Wassenaar arrangement to include dual-use technologies such as those sold by Amesys. The proposal was accepted by all 41 states and the results of which led to the 2014 banning by the Germany government of dual-use technologies to Turkey "on the basis that the equipment could be used to listen in on exchanges over the Internet and, potentially, to breach fundamental liberties[83]."

This was not the end of litigation for Amesys however. The allegations of violations of the rights to privacy, supported by a lack of export controls, were dropped; however, they still had to contend with violations of crimes against humanity. In March 2016, new evidence surfaced, consisting of dozens of documents from Gadaffi's security services that reportedly showed the regime's extensive use of the surveillance technologies provided by Amesys to track, arrest, and torture political opposition. In light of this, Amesys was formally assigned the status of "assisted witness" for complicity in the torture committed in Libya between 2077 and 2011. What the specific legal consequences of being labeled an "assisted witness" are I am unaware of, but in the time between its designation and 2017, Amesys restructured itself into NEXA Technologies, continuing in the same practice it had been[84]. In November of that year, a report by French media showed a similar connection between NEXA Technologies and the repressive Al-Sissi regime in Egypt as between Amesys and Gaddafi in Libya. As of 2020, there was a judicial request by French courts to investigate key witnesses in connection with NEXA's dealings in Egypt.

The Amesys case is an interesting one, in that it's one of the first times a corporation has been accused or tried on the basis of a Rome Statute violation. This can't be done at the international level, as the Rome Statute itself doesn't recognize corporations as a legal entity; but many countries around the world have adopted Rome Statute crimes into their national legislations, which opens up the possibility of holding corporations like Amesys or NEXA Technologies accountable for their repeated violations of international law. It is an interesting exercise to consider the requirements of a Rome Statute violations, specifically in the sale of cyber weapons or technologies. As article 7, regarding crimes against states:

[82] Ibid. page 13.
[83] Ibid.
[84] Trial International

> 1. *For the purpose of this Statute, "crime against humanity" means any of the following acts when committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack*[85]*:*

The important factor when considering complicity for arms dealers, in this case surveillance technology dealers, was whether or not their "knowledge" of the situation rose to the level required by law. Certainly one could argue that their failure in CSR responsibilities does not absolve them of liability, but the specific threshold for knowledge within this article is something that will have be discussed at length within the international community, given the highly targeted nature of cyber weapons.

C. The NSO Case

One of the most prescient examples of software firms exploiting human rights and profiting from it, is the case of the Israeli tech firm "NSO." Most of the controversy surrounding NSO is in the production and alleged sale of their "Pegasus" software. It is a highly advanced spyware virus that can infiltrate phone systems and allow whoever is controlling it to listen in on conversations and track movements. As per the Wassenaar Arrangement (the 2019 version), this software is considered dual-use and has the function of being able to "carry out policing activities[86]."

It's important to note at this point that Israel is not a party to the Wassenaar Arrangement; however, several countries that have been linked to the use or sale of "Pegasus" are, including India and Mexico. The example highlighting the effects of Pegasus however, concern the activities of the Saudi Arabian government in relation to the extrajudicial killing of Jamaal Kashoggi in October of 2018. As per the United Nations special report investigating the incident, there was evidence that Kashoggi was being tracked, prior to his killing, by the Saudi government using the "Pegasus" software. This information comes from a Canadian academic research lab "Citizen Lab":

> *68. On 1 October 2018, Citizen Lab, a Canadian academic research lab, reported that the cellphone of Saudi political activist Omar Abdulaziz had been infected with Pegasus spyware which is produced and sold by NSO Group.*[87] *Citizen Lab attributed the infiltration to a Pegasus operator linked to Saudi Arabia. Pegasus had allowed the Saudi-linked operator to access Mr. Abdulaziz's phone contacts, photos, text messages, online chat logs, emails, and other personal files. The operator also had the ability to use the phone's microphone and camera to secretly view and eavesdrop on Mr. Abdulaziz*[88]*.*

---

[85] Rome Statute

[86] Wassenaar Arrangement List 2019. Specifically, section 5 D. 1 e. which relates to dual-use software.

[87] https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/ .

[88] Annex to the Report of the Special Rapporteur on *extrajudicial, summary or arbitrary executions.* OHCHR regular sessions, session 41.

While this was not specifically targeted at Jamaal Kashoggi, it was instrumental in tracking his movements prior to the killing. Mr. Abdulaziz himself gave an interview to the special rapporteur wherein he laid out the extent to which "Pegasus" had infiltrated his communications and what actions he had taken:

> *70. In December 2018, Mr. Abdulaziz filed a lawsuit in Israel against the NSO Group alleging that the company helped Saudi authorities to infiltrate his phone and spy on Mr. Khashoggi.*[89] *The lawsuit claims that in the months before the killing, the Saudi authorities had access to Mr. Khashoggi's communications with Mr. Abdulaziz by infecting Mr. Abdulaziz's phone with Pegasus spyware. NSO Group has denied the allegations. Mr. Abdulaziz has also filed lawsuits against Twitter and the American consultancy firm McKinsey & Company*[90].

And this was not found to be an isolated incident. As early as August 2018, Amnesty International reported that Yahya Assiri, the director of ALQST, a human rights advocacy organization in Saudi Arabia had been targeted with the Pegasus software[91]. This clearly shows a pattern of human rights violations by the Saudi Government, using NSO's products. Where the issue of derogations comes in the form of article 7 of the International Covenant on Civil and Political Rights, NSO's marketing of its product points to an attempted diminishing of its own liability. According to NSO's personal webpage, the aim of their software is to be "used exclusively by government intelligence and law enforcement agencies to prevent crime and terror[92]." Since terrorism can be used as an effective example of a danger to national security, NSO is specifically trying to market its product as an effective tool in defense of national security, exempting it from allegations of human rights abuses because the derivations would be justified. This is similar to the reasoning used in the Heckler and Koch case described above, essentially using an end-user license agreement to absolve the company of liability. While there isn't currently access to NSO license agreements, a fair assumption would be that the company explicitly states in the contract that "Pegasus" is to be used on in defense of national security.

However, as can readily be seen from the Kashoggi case, the Saudi Arabian government will use such technologies in defense of its own interests which does not amount to a viable cause for derogations of human rights. Further, Kashoggi wasn't the first case of this as demonstrated earlier in the year by Amnesty International's report. With this information, NSO Group Technologies should have been forced to adhere to Corporate Social Responsibility principles and conduct a due diligence evaluation of its product's use by the Saudi Government. However, due to weak regulatory control of NSO's export license in Israel, and the non-binding nature of CSR principles, NSO was allowed to continue operation.

---

https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session41/Documents/A_HRC_41_CRP.1.docx

[89] https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html.

[90] Ibid. page 14.

[91] Ibid.

[92] NSO Group Technologies website. https://www.nsogroup.com/about-us/

D. Arms Trade Treaty

The Arms Trade Treaty has often been touted as good foundational example for a potential cyber weapons treaty. There are many facets of regulatory control proposed within the treaty itself, several of which may be compatible with cyber weapons. Starting with Article 2, the scope of the treaty is laid out in explicit terms, listing the different weapons that are bound under the text. While cyber weapons cannot be described as any of the items listed therein, paragraph 2 is especially important to look at:

> *2. For the purposes of this Treaty, the activities of the international trade comprise export, import, transit, trans-shipment and brokering, hereafter referred to as "transfer[93]".*

In the example of private military corporations and their regulatory framework within U.K. legislation, it becomes clear that the giving of technical assistance is also considered as a "transfer." The Arms Trae Treaty however takes a more traditional approach from the aspect of transfers of physical property. This is an issue that would need to be resolved with relation to the non-physical nature of cyber weaponry. As more and more states gravitate towards the regulation of "technical assistance", that concept should find its way into international law, at which point the non-physical nature of cyber weapons will no longer be an issue.

The stated aim of the Arms Trade Treaty was towo-fold; to establish the highest possible standards for international regulation of conventional arms, and to prevent and eradicate the illicit trade of conventional arms. In order to achieve this, it's essential for international cooperation and transparency. The issue when applying this same aim to a potential cyber weapons treaty was highlighted earlier, namely that the main mode of operation for cyber weapons is stealth and anonymity. So the transparency element so prevalent in the Arms Trade Treaty will only apply to export/import claims, which makes the (currently non-binding) obligations of the Wassenaar Arrangement all the more prevalent.

The last point of discussion, and perhaps the most important is the applicability of Article 6 of the Arms Trade Treaty, the prohibitions. This covers prohibitions on trade to areas that have arms embargoes enforced by the United Nations, or prohibitions on trade that would lead to other breaches of international obligations or Rome Statute violations. These obligations are central to the stated aim of the treaty and would need to be included in a cyber weapons treaty. In consideration of the considerable logistical issues of governmental oversight for cyber weapon development within their territory, it would be prudent to ensure the aim of Corporate Social Responsibility principles, particularly due diligence, be encoded into any regulatory framework in this sector.

[93] Arms Trade Treaty. Page 3.

Chapter 5: Conclusion

The results of this research were skewed by the availability of court documents and relevant cases. While that is no excuse for the lack of foundational legal elements, I think it does speak to the overall nature of this section of international law; that it remains very much within the context of domestic legislation as international cooperation and transperancy is highly limited. Efforts have been made to effect international regulatory control in the trade of dual-use cyber technology and cyber weapons, most notably the Wassenaar Arrangement, these attempts remain in the category of soft law. As shown from the United Kingdom's approach towards private military corporations and their value to the host state's economy, weak regulatory functions are the norm. While there have been notable exceptions, particularly in reference to Amesys in France, and the curtailing of Heckler and Koch's activities in Mexico by German courts, these remain in the realm of civil law suits, similar to the outcome of Shell's violations of human rights in Nigeria. Further, when countries with less liberal ideas instilled in their domestic legislation, corporations like NSO Group Technologies are allowed to continue operations with essentially impunity. Still, the strongest mode for international control is in export licenses.

In terms of potential international treaty frameworks, I didn't even address the Chemical Weapons Treaty in my personal research simply because of the conclusions Geers drew from his analysis of it. Simply put there are too many points of development for cyber weapons to the effect that governmental regulation even at the ISP level is a logistical impossibility. This same logistical impossibility was pervasive throughout my analysis of the Arms Trade Treaty and the Wassenaar Arangement; however, where they differ, and where potential success might be found is in their mode of control. From the Wassenaar Arrangement it's clear that the mode of control is export licenses and restrictions on governmental imports of certain technologies. With the Arms Trade Treaty, the mode of control is essentially to enact the concept of due diligence into binding domestic law. This combination supports what I contend to be the best chance at regulating cyber weapons, a cocktail of export/import controls and legally enforceable CSR principles that force obligations on states to oversee the activities of corporations within their jurisdiction and when necessary to prosecute under ICL and human rights law violations. Evidence for the efficacy of this has been shown through the Amesys case and the related developments it percipitated in the Wassenaar Arrangement. The success of which culminated in the halting of dual-use exports from Germany to Turkey. This could be taken as an example of a shift in *opinio juris* towards state responsibility in the oversight of corporate CSR adherence.

Ultimately, I have attempted to argue that the Wassenaar Arrangement as well as the prosecution of companies like Amesys and NSO are leading towards a tighter regulatory scheme involving cyber weapons and their distribution. While it will never reach the efficacy of the Chemical Weapons Treaty due to logistical impossibilities, incremental steps are being taken to curtail the proliferation of these technologies, and when misused, corporations are being held accountable, if only currently in civil lawsuits.

Considerations for further research:

My research focused primarily on the interplay between corporations and states through export licenses in the context of cyber weapons. The areas involving ICL violations and their applicability to cyber weapons was something I was lacking and deserved more detail than I can

give; however it was slightly outside the scope of this research anyways. One area that I alluded to and needs to be developed further is the "knowledge" requirement in the Rome Statute and the nature of cyber weapons themselves. I couched it as cyber weapons being "highly targeted" in their development, meaning that the developer must have specific knowledge of what the weapon will be used for in order for it to be developed properly. Whether or not this reaches the level required by the Rome Statute is something I leave to future scholars on the subject.

A wider comparison of domestic legislation could also be attempted to show the development of restrictions on PMCs in their host countries. Largely this could be shown again through export licenses and governmental documents such as the Green Papers I examined in relation to the U.K. Although the interplay with cyber technologies specifically might not be clear from that context, it would show a shift towards greater CSR accountability at the national level. I only delved into this area briefly but it could have profound implications on the potential shift of CSR from soft law to hard law.

Bibliography:

1. Michael N. Schmitt. *Tallinn Manual 2.0*. Cambridge University Press. February 2017. DOI: https://doi.org/10.1017/9781316822524
2. Maitra, A. (2015). Offensive cyber-weapons: Technical, legal, and strategic aspects. *Environment Systems and Decisions, 35*(1), 169-182
3. Mele, Stefano. Legal Consideration on Cyber Weapons and their Definitions. Journal of law and cyber warfare. Vol. 3 No. 1 pp. 52-69 2014
4. Koblentz, G., & Mazanec, B. (2013). Viral Warfare: The Security Implications of Cyber and Biological Weapons. *Comparative Strategy, 32*(5), 418-434.
5. UN General Assembly. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction. Geneva, 3rd September 1992. Available at: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVI-3&chapter=26
6. Geers, K. (2010). Cyber Weapons Convention. *The Computer Law and Security Report, 26*(5), 547-551.
7. UNGGE on the developments in ICT on national security and international affairs. (A/RES/70/237).
8. Nuclear Test Ban Treaty, July 26, 1963; Treaties and Other International Agreements Series #5433; General Records of the U.S. Government; Record Group 11; National Archives.
9. Roscini, M. (2014). Cyber Operations as Nuclear Counterproliferation Measures. *Journal of Conflict and Security Law, 19*(1), 133-157.
10. O'Connell, Mary Ellen. Cyber Security Without Cyber War. Journal of Conflict and Security Law. Oxford University Press, 2012
11. Sleat, M. (2018). Just cyber war?: Casus belli , information ethics, and the human perspective. *Review of International Studies 44*(2), 324-342.
12. Orji, Uchenna Jerome. Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation? 2015 7th International Conference on Cyber Conflict. NATO CCDCOE Publications
13. Walker, Clive and Whyte Dave (2005). Contracting Out War?: Private Military Companies, Law and Regulations in the United Kingdom. International and Compartive Law Quarterly, 54, pp 651-689
14. Export Control Act (U.K. Legislation, apologies for the lack of proper citation at this time)
15. White, N. (2016). Regulation of the Private Military and Security Sector: Is the UK Fulfilling its Human Rights Duties? *Human Rights Law Review, 16*(3), 585-599.
16. Musa, S. (2017). The Saudi-Led Coalition in Yemen, Arms Exports and Human Rights: Prevention Is Better Than Cure. *Journal of Conflict and Security Law, 22*(3), 433-462.
17. Wheeler, S. (2015). Global production, CSR and human rights: The courts of public opinion and the social licence to operate. *The International Journal of Human Rights, 19*(6), 757-778.
18. Byrne, E. (2007). Assessing Arms Makers' Corporate Social Responsibility. *Journal of Business Ethics, 74*(3), 201-217.
19. Green, R. (2000). Legally Targeting Gun Makers: Lessons for Business Ethics. *Business Ethics Quarterly, 10*(1), 203-210.

20. Federal Ministry of the Interior, 1986. War Weapons Control Act. As last amended by Article 3 of the law of 11 October 2002, Federal Law Gazette I, p. 3970
21. NPR Publication (Again, apologies for the lack of proper citation at this stage). https://www.npr.org/2019/02/21/696561255/heckler-koch-fined-4-2-million-over-assault-rifle-sales-in-mexico?t=1618240329383
22. Cooper, N. (2006). What's the point of arms transfer controls? *Contemporary Security Policy, 27*(1), 118-137.
23. Hansen, S. (2016). Taking ambiguity seriously: Explaining the indeterminacy of the European Union conventional arms export control regime. *European Journal of International Relations, 22*(1), 192-216.
24. Koutrakos, P. (2010). The Notion of Necessity in the Law of the European Union. *Netherlands Yearbook of International Law, 41*, 193-218.
25. Heidenkamp, H., Louth, J., & Taylor, T. (2013). IV. The Regulation and Control of Defence Businesses. *Whitehall Papers, 81*(1), 98-137.
26. Ambos, K., & Momsen, C. (2018). Introduction: Human Rights Compliance and Corporate Criminal Liability. *Criminal Law Forum, 29*(4), 495-497.
27. Ambos Kai. *The Foundation of Companies' Criminal Responsibility Under International Law*. Criminal Law Forum 29(4). Copyrite Springer Nature B.V. 2018. 498-566.
28. Kolieb, J. (2020). Don't forget the Geneva Conventions: Achieving responsible business conduct in conflict-affected areas through adherence to international humanitarian law. *Australian Journal of Human Rights, 26*(1), 142-164.
29. Grear, A., & Weston, B. (2015). The Betrayal of Human Rights and the Urgency of Universal Corporate Accountability: Reflections on a Post- Kiobel Lawscape. *Human Rights Law Review, 15*(1), 21-44
30. Van der Wilt, H. (2013). Corporate Criminal Responsibility for International Crimes: Exploring the Possibilities. *Chinese Journal of International Law, 12*(1), 43-77.
31. Pieth, M. (2018). Corporate Compliance and Human Rights. *Criminal Law Forum, 29*(4), 595-601.
32. Simon, Penelope. *International Law's Invisible Hand and the Future of Corporate Accountability for Violations of Human Rights.* Journal of Human Rights and the Environment, Vol. 3 No. 1, March 2012 pp. 5-43.
33. Price, Luke. *Finding Fault in Organizations-Reconceptualizing the Role of Senior Managers in Corporate Manslaughter.* Legal Studies, Vol. 35 No. 3, pp. 385-407.
34. Sullivan, G. (1996). The Attribution of Culpability to Limited Companies. *The Cambridge Law Journal, 55*(3), 515-546.
35. Bryk, L., & Saage-Maaß, M. (2019). Individual Criminal Liability for Arms Exports under the ICC Statute. *Journal of International Criminal Justice, 17*(5), 1117-1137.
36. Kaleck, W., & Saage-Maaß, M. (2010). Corporate Accountability for Human Rights Violations Amounting to International Crimes. *Journal of International Criminal Justice, 8*(3), 699-724.
37. Farrell, N. (2010). Attributing Criminal Liability to Corporate Actors. *Journal of International Criminal Justice, 8*(3), 873-894.
38. Stewart, J. (2012). The End of 'Modes of Liability' for International Crimes. *Leiden Journal of International Law, 25*(1), 165-219.
39. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Public Documents 2: Dual-Use Goods and Technologies and Munitions List. Wassenaar Arrangement general secretariat. December 2020.

40. Karim Lahidji. *FIDH Report on the Amesys Trial*. FIDH's Litigation Action Group. Oak Foudnation. November 2014. https://www.fidh.org/IMG/pdf/report_amesys_case_eng.pdf
41. Trial International. https://trialinternational.org/latest-post/amesys/
42. UN General Assembly, **Rome Statute** of the International Criminal Court (last amended 2010), 17 July 1998, ISBN No. 92-9227-227-6, available at: https://www.refworld.org/docid/3ae6b3a84.html [accessed 8 May 2021]

Appendix 4. Non-exclusive licence

Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I, Ian Heimgartner

1.Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

Corporate Liability in the Production and Sale of Cyber Weapons,
(title of the graduation thesis)

supervised by Alexander Antonov,
(supervisor's name)

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

---

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*