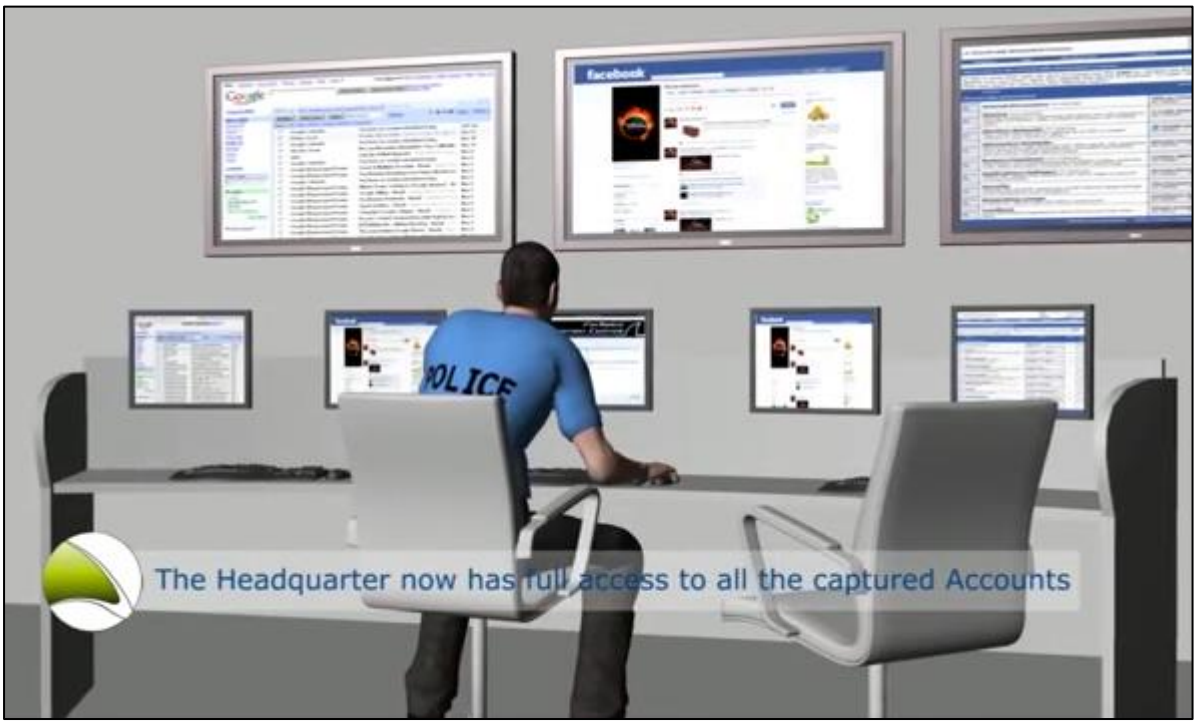
DEALING IN DEADLY SOFTWARE

A Criminological Assessment of the Involvement of Four Surveillance Technology Companies in Gross Human Rights Violations



Augustus 2014

Leonie van Breeschoten

Student Number: 2518980

MSc International Crimes and Criminology

Supervisors: Prof. Dr. Wim Huisman & Annika van Baar

TABLE OF CONTENTS

DEALING IN DEADLY SOFTWARE

A Criminological Assessment of the Involvement of Four Surveillance Technology Companies in Gross Human Rights Violations

INTRODUCTION

Authoritarian regimes have, by their very nature, always aimed to exert a tight control over their population; influencing public opinion and limiting dissent are often perceived as essential to staying in power. Consequently, authoritarian governments tend to employ far-reaching measures to silence dissenting voices, with human rights organisations reporting imprisonment, torture and even murder of dissidents. For many authoritarian leaders controlling their populations has taken a new turn now that technology is playing an all-encompassing role in many people's lives. Every activity of dissidents in cyberspace[1] can be monitored: their emails and texts can be read, their phone calls or Skype conversations can be listened to, and their movements can be tracked through GPS. Additionally, for the first time in history technology enables governments to scan the entire online or mobile networks in order to identify dissidents of whom it was previously unaware. Technology has not lead to a change in the behaviour of authoritarian governments, but it has provided new means, and thereby has made the process much more efficient. Had States not had access to surveillance technology, they would not be able to identify dissidents as easily, and fewer people would fall victim to gross human rights violations (GHRV)[2] at the hands of their governments.

Technology is not simply 'out there' for everyone to do with whatever they want. Technological tools, both software and hardware, are designed by people to serve specific needs. Many companies are specialised in providing governments with surveillance technology, and thereby facilitate[3] the crimes of the States. Due to the nature of the products and the

[1] In this article I refer to 'cyberspace' when discussing the main 'place' that is being surveilled with surveillance technology. The term was coined by the science fiction writer William Gibson, and refers to the "consensual hallucination" where our communications by means of information and communication technology (ICT) seem to exist. It includes the internet, but also, for example, telephone communications.

[2] 'Gross human rights violations' refers to the most serious violations of human rights. Although no official list exists that enumerates which crimes are seen as most serious, the United Nations Sub-Commission on Prevention of Discrimination and Protection of Minorities holds GHRV to "include at least the following: genocide; slavery and slavery-like practices; summary or arbitrary executions; torture and cruel, inhuman or degrading treatment or punishment; enforced disappearance; arbitrary and prolonged detention; deportation or forcible transfer of population; and systematic discrimination, in particular based on race or gender."

[3] For readability purposes and because I deem an in-depth legal analysis outside of the scope of this article, I have used terms like 'facilitating' 'enabling' 'aiding' 'involvement' and 'complicity'

demands of customers, corporations often cannot but have been aware of the potential harmful consequences of their products.

The study of corporate involvement in GHRV and international crimes[4] is a new development in criminology, and lies at the crossroads of the study of GHRV/international crimes and the study of corporate crime. To my knowledge no study focussing specifically on the involvement of surveillance technology companies exists. In this article I aim to work towards filling this gap, by exploring the etiology of the involvement in GHRV of four companies; namely Nokia Siemens Networks/Trovicor, FinFisher, Amesys and Area. I will firstly explore the research question *how does the sale of surveillance technology enable GHRV?* In order to do so the following topics will be explored: the social and historical context of surveillance technology, the nature of the surveillance technology industry, the current possibilities of surveillance technology, and the 'dual use' of surveillance technology (that it can be used for both harmful and non-harmful purposes). Following I will explore the legal framework in order to answer *is selling surveillance technology that is used to enable GHRV crime?* As the answer is negative form a purely legal perspective, I will consequently set out why I maintain that the behaviour can still be seen as 'crime' for criminological purposes and thus allow for a criminological assessment. Following I will apply a well-known theory of 'regular' corporate crime -namely James William Coleman's theory that corporate crime occurs as a result of the confluence of appropriate motivation and opportunity- to the four cases, in order to answer the question *how can the involvement of Nokia Siemens Networks/Trovicor, FinFisher, Amesys and Area in GHRV be explained, using Coleman's theory of motivation and opportunity?* In order to answer this question I will firstly set out the criminological framework, and provide a summary of the cases, after which I will conduct the analysis. Lastly there will be a discussion and conclusion.

SURVEILLANCE TECHNOLOGY

SOCIAL AND HISTORICAL CONTEXT

Our dependence on cyberspace has increased tremendously in a relatively short period of time. Was it in the 1960s only used by a select group of people, nowadays it plays an all-

interchangeably here. For an overview of the (legal) differences between the terms see: International Commission of Jurists (2008).

[4] In this article I will use the concept GHRV rather than international crimes (war crimes, crimes against humanity and genocide). The acts being discussed here can potentially qualify as both; however, because I consider the legal analysis beyond the scope of this article, I prefer to talk about GHRV, which has fewer legal requirements (for example with regards to scale). Additionally, as the corporations discussed in this article facilitate crimes committed by a State, I prefer using a body of law that deals with State responsibility over one dealing with individual criminal responsibility.

encompassing role in our lives. Consequently the stakes for governments to be able to control it have increased tremendously (Deibert and Rohozinski, 2012, p. 21). Four phases of cyberspace regulations by governments are identified by Deibert et al. in their research on trends and patterns shaping information controls around the world: the *open commons* phase (1960s to 2000), the *access denied* phase (2000-2005), the *access controlled* phase (2005-2010), and the *access contested* phase (2010 and beyond). These phases of regulations apply both to authoritarian and democratic governments, be it to different extents. The *open commons* phase refers to the time when there were hardly any governmental regulations over cyberspace, and when it was expected that it would remain open commons. It was perceived as too new and too different, which made that States could not reach it. Consequently, ICT was seen as a force that would inform, empower and liberate citizens. During the *access denied* phase States began to try to exert their control over cyberspace by erecting filters that block access to certain information. During the subsequent *access controlled* phase States started using more 'offensive' methods, such as computer network attacks, espionage, and aggressive propaganda. These mechanisms are more subtle and nuanced than completely blocking certain information, and technological and non-technological measures (such as law enforcement or legal measures) supplemented each other. The last phase, *access contested*, is only just beginning. In this phase cyberspace is no longer seen as a separate space, but as something that is intimately linked with all other aspects of our lives. As a result it is perceived as another terrain than can be controlled, over which advocates for open access, governments, and corporations strive for control. In this phase governments are committed to developing offensive actions in cyberspace against adversaries (Deibert et al., 2012, pp. 6-18).

Surely, in a number of revolutions, such as the 2004 Ukrainian Orange Revolution, ICTs have been an immense aid to protesters. Yet according to Lange (2014) this is due to the fact that the government had simply been unprepared for it at the time (p. 55). Morozov (2011) and Lange (2014) both maintain that –especially authoritarian- governments responded to the notion that ICTs aid dissidents by increasing their ability to surveil and hack their citizens' activities in cyberspace, leaving it more and more unlikely that ICTs can aid dissidents to the same extent in the future (pp. 9-14; p. 59). Still, even though it has become clear that the notion that cyberspace is and should remain open, cannot be touched by governments, and will lead to democratisation is unrealistic, it continues to prevail (Morozov, 2011; Deibert et al., 2012, pp. 6-8; Lange, 2014, p. 48).

THE SURVEILLANCE TECHNOLOGY INDUSTRY

The precise size of the surveillance technology industry is unknown as data about surveillance companies is mostly very difficult to obtain because the mass surveillance industry is highly secretive (Lange, 2014, p. 48; Deibert and Rohozinski, 2012, p. 34). The Spyfiles, a project from WikiLeaks and partners,[5] has currently identified 160 surveillance technology companies, but this is not a complete list. It should also be noted that this does not mean that all these surveillance technology companies are also involved in GHRV; their products could also be used for legitimate purposes in countries that are not authoritarian (see section on dual-use below).

In the previous section I have set out how the demand of States for surveillance technology has increased now ICTs play such an important role in many people's lives and States have seen how ICTs can aid dissidents if not controlled. The production and design of surveillance technology is, however, not only driven by market demands. As Deibert and Rohozinski (2012) note, companies in the surveillance technology business are also a "constitutive force that shapes and affects the realm of the possible," and create new products and possibilities States may never even have thought of (p. 34).

Corporations sell surveillance technology to governments, law enforcement agencies and intelligence organisations, but also telecommunications operators and internet service providers are important customers (Fuchs, 2013, pp. 1346-7). In reality also sales to the second group can enable governments, law enforcement agencies and intelligence organisations to surveil dissidents; telecommunications operators and internet service providers are in most countries (authoritarian and non-authoritarian) obliged to enable law enforcement agencies to intercept traffic. Moreover, in many authoritarian countries telecommunications operators and internet service providers are State-owned or controlled (Deibert et al., 2012).

CURRENT POSSIBILITIES OF SURVEILLANCE TECHNOLOGY

Surveillance technology can roughly be divided in two types of surveillance: mass surveillance technology and targeted[6] surveillance technology. Mass surveillance technologies indiscriminately scan entire networks and thus have the ability to *identify* potential threats, for example by searching for the use of specific words, or by mapping who communicates with

[5] The Spyfiles are a project from WikiLeaks, Bugged Planet, Privacy International and six media organisations: Bureau of Investigative Journalism, l'Espresso, La Republica, ARD, The Hindu, and The Washington Post.

[6] Targeted surveillance (or interception) is often referred to as lawful surveillance. These terms are not exactly interchangeable, as 'lawful' refers to what is allowed by law, and 'targeted' to the fact that only pre-determined targets are surveilled. In practice, however, this often comes down to the same, as in many countries only targeted surveillance is lawful.

other known criminals or dissidents. The data from the entire network can also be stored and analysed at a later time, would anyone become a suspect in the future. Targeted surveillance technology enables those conducting the surveillance to collect more data on previously identified 'targets'. Next to monitoring a target's internet and telephone behaviour through collecting data at the level of the internet or telephony provider, data is collected by hacking into a device (computer or smartphone) or network known to belong to the target. Hacking into the device of the target can be done remotely, for example by sending the software disguised as something else (in an e-mail, or as an update for a programme like iTunes or Adobe Flash Player) so the target installs it by accident, or by locally installing the software (e.g. from a CD or USB, or over the local network), which thus requires physical proximity to the device (FinFisher suggests to have this done by housekeeping staff; FinFisher, n.d., p. 6). Once a device is infected, it is possible to monitor everything done with it. This makes it possible to read data thought to be encrypted (such as Skype communications), as the data is intercepted on the device itself, before it is encrypted. Moreover, once hacked into a device, it is also possible to read or copy the data on the hard drive, log which keys the target presses, track the location of the target through GPS, and remotely turn on webcams or microphones, and thus collect data on the 'real-life' activities of targets in proximity to the infected device. It is even possible to change e-mails sent by a target while they are on their way to the recipient. Additionally, by using voice recognition to scan phone networks, or facial recognition to scan through photographs or surveillance videos, governments can collect even more data on a specific target. Typically a variety of products are coupled to monitoring centres where the collected data is stored, monitored and analysed. The analysis is largely done by the technology, and employees are only presented with 'red flags' (Wikileaks, n.d.; Cohn, Timm and York, 2012, p. 2; Valentino-Devries, 2011; Trovicor, n.d.; FinFisher, 2014; Amesys, n.d.; Area, 2012).

DUAL-USE

Surveillance technology is not necessarily used to identify dissidents and enable GHRV, it can also be used to identify criminals or terrorist and enable their capture; it thus has a dual-use. Traditional dual-use products can be used for both civilian and military purposes; the chemical thiodiglycol, for example, can be used to make textile but also to make chemical weapons. Surveillance technology, on the other hand, has only one application, which is arguably neither civilian nor military as it is applied to serve a governmental need, rather than a civilian one, but oftentimes outside of a military context (Brown and Korff, 2012, p. 37). The difference between surveillance technology being used for 'normal' or harmful purposes lies not in the technological functionality of the product, but in the people targeted. Many surveillance

technology companies focus on the fact that that they only sell their products to governments and law enforcement, which use it for 'lawful interception.'[7] However, lawful interception refers to what is lawful in the country where the technology is employed, but this does not necessarily have to be in accordance with human rights standards. As Marietje Schaake (2013), member of the European Union parliament, asked: "how lawful can interception be without the rule of law?" The same act can constitute law enforcement in an authoritarian State, but a human rights violation in a liberal one. In China, for example, 'crime' is defined broadly to include political dissent. Therefore imprisonment of a dissident is law enforcement according to the Chinese. Is the imprisoned then a criminal, or a victim of human rights violations (Mackinnon, 2012, p. 197)?

LEGAL REGULATIONS

In the current instance it is the State that is the primary perpetrator of the GHRV, and the corporation is facilitating this by providing surveillance technology; as such it can be seen as corporate-facilitated State crime.[8] Corporate facilitation of State crimes can be regulated in two ways: the corporate complicity in crimes committed by another –the State or a State official- can be addressed, or the contribution –the sale of surveillance technology- can be prohibited on its own, most notably through trade regulations. Additionally, the international context in which these products are sold means that there are several legal frameworks that could regulate this; it can be done internationally, by the State in which the company is based (the home-State), or by the State with which the company does business (the customer-State). Below I will discuss the regulations per legal framework.

INTERNATIONAL REGULATIONS

There are no mechanisms under international law that deal directly with the involvement of corporations in GHRV or international crimes, neither as primary nor as secondary perpetrator. Although in the human rights framework corporations are to respect human rights, they are not subject to any binding legal obligations. States have an obligation to

[7] This was also the approach explicitly taken by Trovicor, FinFisher and Area on their websites.

[8] The term 'corporate-facilitated State crime' was coined by Matthews (2006, p. 119) as an addition to two categories of State-corporate crime proposed by Kramer and Michalowski: State-facilitated corporate crime, and State-initiated corporate crime (as cited in: Kramer, Michalowski and Kauzlarich, 2002, p. 271). In contrast to State-facilitated or State-initiated corporate crime, where the corporation is the primary perpetrator, and the crimes occur as the State failed to regulate (State-facilitated) or directed or approved the acts (State-initiated), the primary perpetrator of corporate-facilitated State crime is the State, whose "illegal or socially injurious actions […] are knowingly facilitated by the voluntary actions of a corporation" (Matthews, 2006, p. 119).

protect against human rights violations, which thus includes those committed or aided by companies (Ruggie, 2011). An increasing number of (home-) States are taking steps to do so, however, there is little that can be done to enforce this obligation on States that do not honour their human rights obligation. As for international crimes, the main court prosecuting it –the International Criminal Court- solely has jurisdiction over natural persons, and cannot hold corporations accountable (Rome Statute, 2010, article 25). Theoretically it could prosecute individuals within a company, but until now it has not taken this approach.

The prohibition of the trade of surveillance technology (or other products) is primarily regulated on a national level. States can make international agreements, but the obligations would not directly affect the corporations but rather oblige States to ensure corporations respect these import and export agreements. This will be discussed further in the next section.

HOME-STATE REGULATIONS

Following a greater focus on human rights and an increase in obligations for States, prosecutions of corporations or corporate officials for their –often extraterritorial- involvement in GHRV or international crimes are increasingly taking place. However, these are still exceptional (Huisman, 2010, p. 42). So far, no corporation has ever been convicted for its involvement in GHRV or international crimes, although a number of individuals have been convicted for their involvement in the course of their corporate activities (Huisman, 2010, p. 49). None of these convictions were related to surveillance technology; yet, at the time of writing two surveillance technology companies are being investigated in France. The first is Amesys, which is accused of complicity in torture performed by the Libyan government, and the second is Qosmos, which is accused of complicity in human rights abuses by the Syrian government.[9] It should be noted, however, that both cases originated from a criminal complaint filed by human rights NGO's,[10] and were not instigated by the country's public prosecutor. Individuals and NGO's have also started a number of civil proceedings against surveillance technology companies, most notably in the United States under the Alien Tort Claims Act. Although settlements have been reached, none of these cases were won by the plaintiff.[11]

[9] For an overview of developments on the cases see the website of the Business and Human Rights Resource Centre: http://business-humanrights.org/

[10] Namely La Fédération internationale des ligues des droits de l'Homme (FIDH) and la Ligue des droits de l'Homme (LDH).

[11] Xiaoning et al. v. Yahoo! Inc, et al.: settled for unknown amount; Saharkhiz et al. v. Nokia Corporation et al.: dropped by the plaintiffs following "a reconsideration of the legal environment" (Farivar, 2010); Du Daobin et al. v. Cisco Systems, Inc. et al.: dismissed as the Court maintained that it was a political rather than a judicial decision whether certain products can be exported, and that it did not have the jurisdiction to assess whether a foreign sovereign engaged in violations of international law, which would be necessary to find that Cisco had assisted; Doe et al. v. Cisco Systems, Inc. et al.: pending.

Besides punishing corporate involvement in GHRV after it has taken place, home-States can also attempt to prevent future violations, most importantly through export regulations. It should be noted, however, that export regulations are generally not designed with the aim of preventing domestic corporations from contributing to GHRV, but rather to prevent that other States have access to certain goods. Yet by extension this also prohibits corporate involvement in GHRV through the sale of goods and services. It is up to States to determine which items are subject to export regulations, though this can also be done multilaterally (notably through the European Union, or the (non-binding) Wassenaar Arrangement on Export Controls for Conventional arms and Dual-Use Goods and Technologies, to which 41 States are party). However, as pointed out by Maurer, Omanovic and Wagner (2014), the export of surveillance technology products is currently not adequately regulated in the countries they examined (the United States, Germany, the United Kingdom and the European Union). They maintain that this is largely because export regulations have not kept up with new technology (p. 2). To illustrate: it was only in December 2013 that the first two types of surveillance technology products were added to the Wassenaar Arrangement.[12] The majority of surveillance technology products can thus be exported without consequence, and this holds especially true for newly designed products, as new laws to regulate will always lag behind. Yet even if all surveillance technology products would be included on export control lists, the particular dual-use nature of the products makes it very difficult to adequately assess what the end-use of the products will be. As described above, surveillance technology differs from 'regular' dual-use technology in that its technological functionality is the same when used to enable GHRV or for legitimate law enforcement. This means that it does not suffice for export authorities to assess who the end-user will be (e.g. a producer of textile or of chemical weapons); rather, the adherence of another State to human rights standards needs to be assessed. This is easily done when export restrictions are part of broader sanctions against a country internationally fallen out of grace – as was done by both the European Union and the United States when they explicitly included surveillance technology in the embargoes against Syria and Iran (Council Regulation, 36/2012; Council Regulation 264/2012; Executive Order 13628)- however, States might be more hesitant to prohibit the export of surveillance technology to human rights violating States with which they uphold friendly relations or on which they rely for import.

[12] Namely "intrusion software" (hacking equipment) and "IP network communications surveillance systems or equipment."

CUSTOMER-STATE REGULATIONS

The description 'customer-State' already indicates that the relation between the State and the company here goes beyond that of mere legislator and subject; the State relies on the company to deliver surveillance technology. As the customer-State has an interest in acquiring these products, it almost never creates legal barriers to the import of the products (Huisman, 2010, p. 42). Additionally, it is also extremely unlikely that the complicity of corporations in the crimes of the State will be addressed. State crime almost always remains unlegislated and unpunished -after all, the State is both the legislator and the perpetrator- (Kauzlarich, Kramer and Smith, 1992, pp. 50-1) it is not surprising that this extends to the complicity of corporations in these crimes.

CRIMINOLOGY WITHOUT CRIMINALITY?

As shown above, corporate involvement in GHRV by selling surveillance technology is not adequately prohibited. This raises the question why a criminological assessment would be called for; after all, is this really 'crime'? I maintain that the conduct of surveillance technology companies –as well as of most other instances of corporate-facilitated State crime- differs from 'regular' corporate crime in two ways; a) the acts by the primary perpetrator are not clearly criminal, but do cause social harm; and b) as the corporation is the secondary perpetrator, it is often very difficult to establish whether their conduct contributed or will contribute to the crime of the perpetrator, however, often it is certain that they took a foreseeable risk. Below I will argue that these points make a criminological assessment appropriate.

Firstly, providing authoritarian States with surveillance technology, even if not legally prohibited, does enable social harm. Crucial here is that, as described above, what is 'crime' is defined by States, and this often means that State crime, social harm caused by States, remains outside of the definition of crime. Should harm by the powerful then be omitted from criminological scrutiny simply because they have the power to decide what is legal? Critical criminologists did not think so, and searched for alternate ways to define crime rather than relying on the State-defined definition. An influential alternative was posed by Schwendinger and Schwendinger (1970) who interpreted crime as violations of internationally accepted human rights norms, and urged criminologists to depart from the State-defined definitions in order to "no longer […] be the defenders of order but rather the guardians of human rights" (p. 149).

The above mainly relates to why the acts of the State should be seen as crime, but as the corporations discussed here are not the primary perpetrators, the question remains whether their involvement can also be seen as 'criminal' and therefore can be subjected to criminological

analysis. In national law there are broadly two requirements in order to establish corporate complicity in crimes committed by another actor (although this differs between jurisdictions): a) there has to be some sort of *causation or contribution* between the acts of the corporation and the crime of the perpetrator, and b) the corporation had to have *knowledge or foreseeability* that the crime would occur (International Commission of Jurists, 2008[13]). Problematically, the first aspect, causation or contribution, is very difficult to establish in most instances of corporate-facilitated State crime, as customer-States (but sometimes also home-States) often refuse to cooperate, and the geographical distance between a prosecutor (or journalist, scientist or other investigator) obstructs evidence collection. Moreover, linking the use of products provided by a corporation to a specific crime (e.g. showing that it was a certain surveillance technology product that facilitated the torture of a certain individual) can be very difficult.[14] However, I would argue that in order to allow for a criminological assessment only knowledge or foreseeability should be taken into account, while causation is irrelevant, because the results of the corporations' behaviour lie outside of their control. They delivered the bombs, but whether these will eventually be dropped, and whether these will hit a lawful or unlawful target, is out of their hands. Had the products malfunctioned, forgotten about, or had the government simply decided not to use them, the companies would not have been complicit, but their behaviour would have been exactly the same. Gobert and Punch (2003) set out this argument, and maintain that a defendant's (criminal) responsibility should not be assessed by the results of his behaviour, as the "actual results may be affected by events, circumstances and fortuities beyond a defendant's control" (p. 144); rather, they argue, the focus should be on the risk taken, as this more strongly reflects the defendant's culpability or moral blameworthiness. Following this logic I maintain that it should not be the extent to which a corporation's actions caused or contributed to the GHRV of a State that determines whether a corporation did something 'criminal;' no, rather, it should be the risk taken by the company – determined by the knowledge

[13] The ICJ lists three factors indicative of the likelihood that a corporation will be held legally accountable for complicity in GHRV; causation/contribution, knowledge and foreseeability, and proximity. Here I have only discussed the first two because I maintain that proximity is indicative of whether the other two requirements can be established, rather than that it is a legal requirement on its own.

[14] A notable case where this was done very successfully was in the Dutch criminal case against the businessman van Anraat, who was found guilty of complicity in war crimes by the Iraqi government against the Kurds by delivering the chemicals that were used in chemical weapons. Documentary evidence and witnesses established his knowledge that the chemicals would be used for chemical weapons, but in order to establish causation it had to be proven that (some of) the chemicals he sold had ended up in the bombs that were used in the war crime against the Kurds. The prosecution successfully showed through a mathematical scenario created by an expert witness that following the substantive amount of Thiodiglycol he provided and the methods in which the Iraqis produced mustard gas it could be assumed that the chemicals supplied by him ended up in ammunition filled with mustard gas (District Court of The Hague, 23 December 2005, Case No. AX6406; Court of Appeal of The Hague, 9 May 2007, Case No. BA6734 (available in English at http://ljn.rechtspraak.nl); Dutch Supreme Court, 30 June 2009, Case No. BG4822 (only available in Dutch)).

or foreseeability that their acts contribute to harm– that makes the acts of the corporation 'criminal.' As I have set out in the first chapter, this risk is inherent in the sale of surveillance technology to authoritarian States.

CRIMINOLOGICAL FRAMEWORK

In this article I intent to use James William Coleman's integrated theory of white-collar crime (1987) to explain the involvement of four surveillance technology companies in GHRV. I use Coleman's -often used- theory[15] because he applied the concepts of motivation and opportunity to white-collar crime. As no integrated theory for corporate involvement in GHRV exists white-collar crime-theory is a logical place to start, as corporate involvement in GHRV is a type of white-collar crime.

Coleman (1987) maintains that "criminal behaviour results from a coincidence of appropriate motivation and opportunity" (p. 408). He takes an interactionist approach to motivation as he assumes that white-collar criminals are not deviant in their biological makeup or socialisation, and holds motivation "to consist of a set of symbolic constructions defining certain kinds of goals and activities as appropriate and desirable and others as lacking those qualities" (p. 409). He identifies two aspects of motivation: a) neutralisation techniques and b) the culture of competition. Neutralisation techniques are techniques that allow white-collar criminals to maintain a non-deviant self-image while their behaviour violates societal expectations. By telling themselves that their behaviour was acceptable -for example because no one was hurt, because it was not their responsibility, or because their behaviour was necessary- white-collar criminals can engage in criminal activity while continuing to be opposed to breaking the law (or violating human rights norms) (Coleman, 1987, pp. 410-414; Sykes and Matza, 1957). The initial attractiveness of the behaviour of white-collar criminals lies, according to Coleman (1987), in the culture of competition; the prevailing worldview which adjudicates successes and failures to the individual's actions and abilities, and thereby links them to one's self-worth. This leads to a desire for wealth and success on one hand, and a fear of failure on the other (pp. 414-20). However, Coleman also names a second cultural force: normative restraints, meaning social norms (like honesty, fair play, ethical codes within businesses and a desire to

[15] There are two notable variations on this theory; Kauzlarich and Kramer (1998; see also Kramer, Michalowski and Kauzlarich, 2002) separate three catalysts for action: motivation or performance emphasis, opportunity structure, and the operationality of social control. Rothe and Mullins (2009), who applied these catalysts to international criminal violations, separate this last catalyst into constraints, elements that can make the crime riskier or less successful (such as public opinion), and controls, elements that offer complete blockage (such as laws and/or regulations). I maintain that in Coleman's framework these extra catalysts are integrated in motivation and opportunity; controls and constraints influence the perception of risk of opportunities, and are part of the symbolic construct influencing motivation.

follow the law) which diminish the motivations originating in the culture of competition (pp. 420-4). Coleman further defines opportunity as "a potential course of action, made possible by a particular set of social conditions, which has been symbolically incorporated into an actor's repertoire of behavioural possibilities" (p. 409). He identifies four factors determining the attractiveness of opportunities, namely a) the perception of gain; b) the perception of risk; c) the compatibility of the opportunity with previously held ideas, rationalisations and beliefs; and d) the availability of alternate opportunities (pp. 424-34).

In the next sections I will firstly set out four cases, after which I will attempt to explain their behaviour through Coleman's theory.

CASES

CASE SELECTION

Following the extreme secrecy surrounding these types of sales (Lange, 2014, p. 48) it is impossible to determine how many surveillance technology companies have enabled GHRV, and thus to know the number of potential cases. Consequently I selected the cases based on two criteria; first, in order to avoid including cases where a corporation was rumoured to have sold to authoritarian States but had not actually done so, I only included companies that had admitted to have sold to authoritarian countries (NSN/Trovicor, Amesys and Area), or against which detailed evidence was available (FinFisher). The second selection criteria I used was rather practical; I included the four cases with the greatest availability of data (especially data that originated from the companies themselves, such as press-statements, interviews, or human rights policies), in order to have sufficient data to base my analysis on. Ultimately I selected Nokia Siemens Networks/Trovicor, FinFisher, Amesys and Area.

NOKIA SIEMENS NETWORKS/TROVICOR

The first accusations against Nokia Siemens Networks (NSN) for involvement in GHRV were issued in 2008, when an Austrian website reported the sale of surveillance equipment to Iran (Rhoads and Chao, 2009). As NSN (2010a) declared later, it had sold mobile networks to two leading Iranian mobile network operators in 2008, and those networks included "lawful interception capability" and a monitoring centre. After the merge of Nokia and Siemens in 2007 it was decided to exit the monitoring business, according to the company partly due to an increased risk of human rights violations. Consequently Intelligence Solutions, the unit responsible for developing monitoring centres, was sold to Perusa Partners Fund in March 2009, which renamed it Trovicor. When the protests in Iran truly broke out in June of that year,

wide-scale allegations against NSN and Trovicor appeared, as well as a 'No to Nokia' boycott, a lawsuit against NSN in a U.S. court (which was later dropped), and inquiries by the European parliament (Katz, 2010). As NSN continues to refer former customers to Trovicor, the 'No to Nokia' boycott also targeted NSN, even though it no longer owned Intelligence Solutions; activists maintained that by selling Intelligence Solutions NSN had continued to profit from its products that enable GHRV rather than prevent future violations (Greenberg, 2010). NSN does continue to be involved in lawful interception of mobile communications, as the capability to intercept communications over a network is intrinsic to providing the network itself (Rhoads and Chao, 2009). According to its website, code of conduct and human rights policy NSN strives to resolve conflicts between local law and international human rights standards in favour of human rights, even if this may result in loss of business (Nokia Solutions and Networks,[16] 2013a; Nokia Solutions and Networks, 2013b; Nokia Solutions and Networks, 2014).

Trovicor (n.d.) markets "solutions for communication networks intelligence, cyber and infrastructure security and target and mass communication analysis" by selling "monitoring centres, analytic tools, and beyond" (Trovicor, 2012b). Surveillance technology is thus at the core of its business. Trovicor is one of the biggest surveillance technology companies, with a current turnover of €54,4 million, of which €2,4 million was profit in 2010 (Trovicor, 2012a). According to its website Trovicor's mission is "making the world a safer place" (Trovicor, n.d.). In its Code of Business Conduct Trovicor (2013) mentions respect for human rights as one of its business ethics goals, but does not include concretely what this would entail (while it does do so for other topics). Moreover, Trovicor (2013) stresses that it "complies with all relevant laws in every jurisdiction," but does not address how to deal with conflicts between local laws and human rights. The company focusses on the fact that it sells exclusively to governments and law enforcement. Moreover, it maintains to have sold to over a 100 countries worldwide (Trovicor, 2012b) – it is difficult to imagine these all to be non-authoritarian. Next to accusations of involvement in GHRV in Iran Trovicor has specifically been accused of having done so in, among others, Syria, Egypt, Bahrain, Yemen, and Tunisia (Timm, 2012).

FinFisher

The Germany company FinFisher was established in 2007 as part of the British Gamma Group. Since October 1st, 2013, it is independent and privately owned (FinFisher, 2014). It creates "innovative cyber tools" which can take full control over the computers and mobile phones of targets, and thus enable the monitoring of online and offline activities of suspects, as

[16] In 2013 Nokia completed the acquisition of Siemens' part of NSN, and the name was changed in Nokia Solutions and Networks.

well as extract passwords, files, or track them (FinFisher, 2014). FinFisher software can be installed on a target's computer or phone in a number of ways, but FinFisher became heavily criticised when it became known that it sent fake updates for popular software, such as iTunes in order to trick suspects into installing FinFisher (Valentino-Devries, 2011). During the Egyptian revolution in the spring of 2011 a FinFisher invoice and promotion materials sent to the Egyptian authorities were found by human rights activists who had broken into the headquarters of the State's security service. They also found evidence that the Egyptian government had used a five-month free trial version of the product (McVeigh, 2011). Later in the same year WikiLeaks (2011) leaked multiple FinFisher promotion materials, including videos and brochures explaining how the product enables breaking into computers and mobile phones of targets.[17] Marquis et al. (2013), researchers at Citizen Lab, an interdisciplinary laboratory located at the University of Toronto, identified FinFisher's Command & Control servers in 36 countries, in all parts of the world.[18] The Organisation for Economic Cooperation and Development is currently looking into Gamma's involvement in GHRV in Bahrain, following a complaint by five human rights organisations (United Kingdom National Contact Point for the OECD, 2013). The OECD can investigate the complaints, determine whether its guidelines have in fact been violated, and issue recommendations on how to avoid further breaches, but cannot impose any punishment (Privacy International, 2013). Both Gamma and FinFisher continue to be unwilling to deny or confirm whether they have sold to Bahrain (United Kingdom National Contact Point for the OECD, 2013). The FinFisher (2014) website does not mention potential human rights conflicts, but only stresses the company's compliance with respective laws and regulations.

AMESYS

Amesys is a French company, founded in 1979 as i2e Technologies, and acquired by the French computer company Bull in 2010. For Amesys the surveillance technology industry is a large part of their business, but not the exclusive part, as is the case for Trovicor and FinFisher; surveillance technology is seen as part of the broader 'Homeland Security Industry' (which, for example, also includes border control systems, or system jamming equipment), one of the two "key areas of excellence" alongside 'Critical Systems' ("equipments that –if they would fail- would expose people, goods or the environment to a major risk") (Bull, 2010). Similar to

[17] See: http://wikileaks.com/spyfiles/list/company-name/gamma.html and http://www.youtube.com/watch?v=oNsXKPHBR3s

[18] Namely Australia, Austria, Bahrain, Bangladesh, Brunei, Bulgaria, Canada, Czech Republic, Estonia, Ethiopia, Germany, Hungary, India, Indonesia, Japan, Latvia, Lithuania, Macedonia, Malaysia, Mexico, Mongolia, Netherlands, Nigeria, Pakistan, Panama, Qatar, Romania, Serbia, Singapore, South Africa, Turkey, Turkmenistan, United Arab Emirates, United Kingdom, United States, Vietnam.

FinFisher, Amesys became accused of involvement in GHRV when during the Arab Spring intelligence headquarters were stormed, in this case in Libya. The scene was investigated by the Wall Street Journal in August 2011, and Amesys's products were found, including manuals and a poster explaining the far-reaching nature of Amesys's products; it said: "whereas many internet interception systems carry out basic filtering on IP address and extract only those communications from the global flow (Lawful Interception), EAGLE Interception system analyses and stores all the communications from the monitored link (Massive Interception)." (Sonne and Coker, 2011). In an presentation, leaked by Wikileaks' Spyfiles, the company makes the same claim (Amesys, 2008). In September 2011 Bull released a press-statement in which it explained to have signed a contract with the Libyan government in 2007, "when the international community was in the process of diplomatic rapprochement with Libya." The company pointed out that it provided analysis hardware, but only for a "small fraction of the Internet lines installed at that time (a few thousand)" (Bull, 2011). Rumours circulate that this sale was aided by French government officials, including Nicolas Sarkozy (at the time minister of interior), yet how substantive these claims are is difficult to say (Manach, 2011a). Two human rights NGO's, FIDH and LDH, filled a complaint for Amesys' complicity in torture with the French judiciary on October 19, 2011. The investigation was halted in April 2012, when the Paris prosecutor issued an order not to open the investigation as it maintained that the facts could not qualify as criminal acts. In January 2013, however, the Appeal's Court decided to allow the judicial proceedings to go ahead (FIDH, 2013).

In March 2012 Bull announced to be negotiating the sale of Amesys's EAGLE systems, as it was "non-strategic" and 'only' represents less than 0,5% of Bull's revenues (about €65 million of their total €1,3 billion revenue)(Bull, 2012). In January 2013 EAGLE was divested to Nexa Technologies, the CEO of which is Stéphane Salies, who, according to his LinkedIn, is also former vice-president of the security and critical systems business line at Bull, and previously general manager at Amesys and i2e (Salies, n.d.; Reporters without borders, 2013, p. 6).

AREA

The Italian company Area (2012) "develops and markets monitoring systems for lawful monitoring activities" to law enforcement, governments and military agencies. In November 2011, during the escalation of the Syrian civil war, Bloomberg News reported that the company was building a monitoring centre in Syria. It based its data on an interview with an anonymous Area employee, who was thereby breaking confidentiality (Elgin and Silver, 2011). The Bloomberg News item was met with public outcry, and led to protests outside Area's headquarters in Milan (Silver and Elgin, 2011), and the European Union explicitly including

surveillance technology in products prohibited to export to Syria (Council Regulation, 36/2012). Area initially refused to comment on their business with Syria specifically, but declared that the company always complied with all laws and export regulations (Elgin and Silver, 2011). Following it issued a statement in which it said that Area "is against all forms of repression and disapproves of any use of technology for violating human rights" (Silver and Elgin, 2011). Three weeks later Area announced to exit the project due to "lack of improvement in the conditions of the country" (Silver, 2011). However, nothing on its website or in its ethics code indicates that this is also taken into account for future sales. In fact, while its ethics code (2010) includes a provision on corporate social responsibility, this is only seen as applying vis-à-vis its employees, not towards society as a whole.

ANALYSIS

Below I will apply Coleman's theory of motivation and opportunity to the four cases, in order to attempt to explain this particular type of corporate involvement in GHRV. I will firstly discuss the two aspects of motivation -neutralisation techniques and the culture of competition- before moving on to opportunity.

MOTIVATION

Neutralisation techniques

NSN, Trovicor, FinFisher, Amesys and Area all issued statements when accused of involvement in GHRV. NSN (2010a) admitted that "we should have understood the issues in Iran better in advance" (p. 3), but said so only after it had sold its monitoring unit to Perusa, and thus was no longer involved. The other companies initially refused to confirm or deny involvement, by relying on confidentiality, but issued general comments on how their business activities are in line with human rights or why these sales would be legitimate. A number of neutralisation techniques can be identified in these statements. Even though these statements were issued after the acts, this does not mean they were only invented as after-the-fact rationalisations; if a corporation had maintained to be doing nothing wrong in the first place, it would not need to justify its actions afterwards. Therefore, it is often held that many statements issued after the conduct had happened can still be seen as reflective of techniques that neutralised disapproval of others in advance (Sykes and Matza, 1957; Coleman, 1987; Huisman, 2010).

Coleman (1987) maintained that six neutralisation techniques were most common among white-collar criminals: denial of harm; maintaining that the laws are unnecessary or unjust; appeal to necessity; transfer of responsibility to a large and often vaguely defined group; denial of responsibility when adhering to expectations of others; and maintaining that the extra

money was deserved (pp. 410-414). My research indicates that a number of these were not employed in these particular cases, or only partly, while also two other neutralisation techniques that were not explicitly discussed by Coleman were employed; namely denial of victim, and appeal to higher loyalties. This does not contradict Coleman's theory, as he acknowledged that also other neutralisation techniques are being used, and his interactionist approach allows for the use of different neutralisation techniques in different situations, as different industries and different 'crimes' would lead to different social expectations.

Neutralisation techniques discussed by Coleman that were not employed by the companies examined were: maintaining that the laws are unnecessary or unjust; appeal to necessity; and maintaining that the extra money was deserved. It is logical that no claims were made that the laws were unnecessary or unjust – after all, there are no laws prohibiting this particular type of conduct. It was also to be expected that the last technique, maintaining that they deserved the extra money, was not employed by the companies, as it applies to occupational crime (crimes committed by individuals for themselves during their occupation) rather than corporate crime (crimes committed for the corporation). Perhaps it is more surprising that no evidence was found indicating that the conduct was neutralised by maintaining it was necessary to achieve vital economic goals or to survive. A possible explanation for this is that appealing to necessity does admit the wrongfulness of the conduct; it was wrong *however* it was necessary. Yet the corporations here mainly maintained that their conduct was not wrong to begin with, thus making this neutralisation technique obsolete.

I would argue that surveillance technology companies most importantly justified their involvement in GHRV by denying responsibility. However, rather than maintaining that they were not responsible as they were merely responding to expectations of others (Coleman, 1987, p. 413) the companies mainly claimed not to be responsible because the harm was caused by forces outside of their control (Sykes and Matza, 1957, p. 667). This is mainly done by maintaining that the responsibility lies with the customer-States rather than with the corporations; as put by Amesys "the use of the equipment [Amesys] sells is exclusively the responsibility of its clients" (Manach, 2011b). NSN's response to the lawsuit by two Iranian dissidents follows the same logic: "the Saharkhizes allege brutal treatment by the Government in Iran, but they have not sued that government. Instead, they are seeking to blame Nokia Siemens Networks for the acts of the Iranian authorities" (2010b). This reasoning is often coupled with the argument that the technology sold is inherently neutral, which thus absolves the companies from responsibility for the ultimate use. Martin Muench, Gamma and FinFisher official, maintained that "Software doesn't torture anybody" (Satter, 2013) and that because "a can of fizzy drink or a car battery can be abused and used as an implement of torture, it is of no

surprise to anyone if our products can be abused too" (Knight, 2012). However, as set out earlier, contrary to a fizzy drink these products do not have to be 'abused' to be an implement of torture, rather this can be achieved through their normal functioning. Besides, also the foreseeability of the 'abuse' make this an unrealistic comparison - though an effective neutralisation technique. In addition, corporations also tend to transfer responsibility to the home-States. Jerry Lucas, the organiser of the Intelligence Support Systems conference, an exclusive get-together for customers and producers of surveillance technology, maintained that it is "just not my job to determine who's a bad country and who's a good country. That's not our business, we're not politicians… we're a for-profit company" (Gallagher, 2011). FinFisher took a similar position, stating that "we use the export controls authorities in the UK, Germany and USA to determine to whom we can sell our products. They in effect act as our 'moral compass'" (Knight, 2012), thereby maintaining that governments have the responsibility to decide which sales are allowed, rather than the corporation. It is a powerful neutralisation technique, as it not just places the responsibility outside of the corporation, but places it with an outside authority which indeed *has* a responsibility to prevent GHRV.

A related technique, transfer of responsibility to a large and often vaguely defined group by claiming that "everybody else is doing it too" (Coleman, 1987, p. 413), is also applied, though to a lesser extent. This approach is for example taken by Area; when confronted with its sales to Syria, the company responded that it got the contract "subsequent to an international tender process" in which "leading international suppliers, both European and non-European" participated (Business and Human Rights Resource Centre, 2011). Thereby it implies that as other companies were eager to engage in the same sales, it would be unfair to merely condemn Area, who eventually got the contract.

Another frequently employed neutralisation technique is denial of the victim; maintaining that the victim was not really a 'victim' but somehow deserved it (Sykes and Matza, 1957, p. 668). Many companies maintain that their technology is exclusively used against criminals, and ignore the fact that in many countries dissidents are considered criminals under local law. Trovicor (n.d.), for example, uses the slogan "making the world a safer place." Area maintains that its products are used in the "fight against terrorism, child pornography as well as organized crime" (Business and Human Rights Resource Centre, 2011), FinFisher (2014) states that its products help "identify, locate and convict serious criminals" and according to Amesys's EAGLE system's manual (Amesys, 2009), it is "designed to help law enforcement agencies and intelligence organization to reduce crime levels." When it is recognised that surveillance technology could be used against dissidents, companies sometimes blame victims for their own suffering. Perusa, owner of Trovicor, maintained that "citizens in semi-democratic or

undemocratic countries should refrain for their own safety from using such forms of communication for activities that could bring them into conflict with a regime in power" (Buse and Rosenbach, 2011). Besides the fact that this statement disregards the right to privacy or freedom of speech, this reasoning is also very unrealistic. Contrary to those working in the surveillance technology business most dissidents are not and cannot be aware of the means of governments, and thus of the risk they are taking when they use ICTs.

Moreover, companies often appeal to higher loyalties or emphasise the positive effects of their products (Huisman, 2010, p. 35). They experience competing social norms, and focus on adhering to one norm to justify sacrificing the other. In this instance contributing to GHRV is justified by a focus on spreading technology, as this, in line with an open commons-approach to technology, is believed to enable freedom and democracy. NSN (2010b), for example, stated in a response to the lawsuit issued by Iranian dissidents that "mobile communications are a powerful tool in the promotion of human rights and the rule of law. They have done far more to empower those who fight for democracy than to empower oppressive governments," and maintained that its products and services "directly contribute to the exercise of such fundamental rights as free expression and political participation" (Nokia Solutions and Networks, 2013b, p. 3). For NSN the harmful consequences of their products, such as enabling torture, are outweighed by the believed positive consequences of giving access to better means of communications.

Lastly, in their statements companies tend to lessen the harm caused. This is related to the often-employed neutralisation technique 'denial of harm', but rather than maintaining that as no harm was done no crime was committed (Coleman, 1987, pp. 410-1; Sykes and Matza, 1957, pp. 667-8), the harm is framed in such a way to portray it as as unimportant as possible. Rather than discussing their products' potential use for GHRV, companies focussed on violations of the right to privacy or freedom of speech. Although those rights are related in this context – without a violation of the right to privacy a government might not have been able to identify the dissident and thus to commit GHRV against him- framing it as solely a privacy issue, rather than an issue of more serious human rights, makes it easier to justify involvement.

Culture of competition and normative restraints

Yet while neutralisation techniques enable people to engage in behaviour they actually do not find acceptable, the initial motivation for this behaviour should be found elsewhere; according to Coleman (1987) in the culture of competition. Coleman sees the culture of competition as a society-wide phenomenon in contemporary industrial capitalist societies, where the pursuit of economic self-interest has become central, and thus provides a structural

motivation. The demand for success, and, conversely, a fear of failure, are powerful symbolic structures which, according to Coleman, are central to the motivation of economic behaviour (pp. 414-8). However, normative restraints, such as honesty, fair play, ethical codes within businesses and a desire to follow the law, pose restraints on what people are willing to do in their financial self-interest. It follows that when these normative restraints are not strong enough -which is also largely dependent on the context and aggravated by the segmentation of social life in industrial society (which makes that people are primarily exposed to the norms of a subgroup)- the initial motivation to commit the crime prevails (pp. 420-4).

It is difficult to determine whether, and to what extent, the culture of competition exists and provides a motivation to become engaged in GHRV to the corporations discussed here; as a society-wide phenomenon it potentially applies to all people and in all companies, and as such is not necessarily related to the economic situation of a company. I found little evidence of the corporations indicating that a desire for economic profit underlies their sales to authoritarian governments, however, this does not necessarily have to mean it does not play a role. Arguably, the fact that the primary motivation of corporations is to make money is so prevalent and accepted in society, that it does not need to be pointed out. A number of journalist articles (e.g. Buse and Rosenbach, 2011; Manach, 2011a) do seem to *assume* that the corporations became involved in GHRV out of a desire for wealth. They do not really seem to maintain that corporations should not be driven by financial self-interest, but rather imply that this is taking the pursuit of gain too far. This strongly corresponds with Coleman's notion that striving for economic success is a society-wide phenomenon, seen as acceptable as long as it operates within certain normative boundaries.

However, from the data at hand it seems that the initial motivation at least partially stems from another factor; namely the intellectual challenge the work poses, which encourages employees to constantly strive for innovation and technical perfection. In the words of FinFisher's Martin Muench being able to control cyberspace "is a cat and mouse game" between governments and surveillance technology corporations on the one hand, and dissidents, criminals, privacy advocates and corporations creating virus scans on the other (Silver, 2012). "Ever-changing and varied threats" (to States) constantly need to be tackled through "innovative approaches" (Bull, 2010, p. 6; see also Deibert et al., 2012, p. 10). In the surveillance technology industry there is a continuous intellectual challenge to outwit the mice, which encourages employees to constantly strive for innovation. Trovicor (n.d.) and Area (2012) emphasise this aspect in the job vacancies on their websites, as selling points to attract new employees.

Theoretically normative restraints would restrain a desire to engage in 'crime', irrespective of whether this desire originates in the culture of competition, a strive for innovation, or –what I think most likely- a combination of both. As surveillance technology has actually been sold to authoritarian States, it appears that normative restraints are not powerful enough to restrain the motivation in these cases. The most important explanatory factor for this is, in my opinion, the fact that the desire to follow the law does not function as a normative restraint here; this desire can be adhered to while also conducting these sales. Other restraints - most importantly a desire not to do harm and to contribute to GHRV- are likely to remain, but are not strong enough to completely restrain the motivation. This, I would argue, is influenced by two industry-specific factors; first, there is a large emotional and geographic distance between the corporate employees and the victims, which makes the relation between the conduct and the GHRV less clear, and thus this normative restrain less influential (this aspect also plays a role in the opportunity structure, and will be discussed in more detail there). In addition, employees within surveillance technology companies have to adhere to far-reaching confidentiality; Trovicor (2013), for example, prohibits its employees even from informing their family and friends whereto they travel on business trips, as to keep it secret with whom it conducts business. As a result employees only discuss their corporate activities with people from the same subculture, which severely limits the chances of them being exposed to the condemnation of outsiders. It seems that within the subculture of the corporation, the business activities are primarily discussed in two ways: a) in technical terms; the functioning of the products is discussed, without needing to relate this to people, and b) in crime-fighting terms; when relating the products to people these people are projected as criminals – for example illustrated by Trovicor's (n.d.) slogan "making the world a better place". Normative restraints are thus strongly influenced by the (corporate) subculture, and as a consequence, in these cases, not strong enough to restrain the initial motivation to offend.

Moreover, it seems that societal norms do not only restrain but can also supplement the initial motivation; the idea that technology is a force for democracy and thus ought to be spread supports the motivation to sell surveillance technology to authoritarian States. NSN strongly focusses on this aspect, for example by maintaining that they sold to Iran because "we believe providing people, wherever they are, with the ability to communicate is preferable to leaving them without the choice to be heard" (Rhoads and Chao, 2009). This view is also held more broadly in society, the European Parliament, for example, praised the spread of ICTs in its digital strategy (2012) as it maintains ICTs to be "fostering revolutionary changes in societies." As such, I would argue, societal norms do not only function as restraints, but can also encourage motivations.

OPPORTUNITY

Yet even when an actor is extremely motivated to commit an offence, without the opportunity to do so there will be no crime. For Coleman (1987) there are four factors that determine the attractiveness of opportunities for an actor or group of actors: the perception of gain; the perception of risk; the compatibility of the opportunity with previously held ideas, rationalisations and beliefs; and the availability of alternate opportunities (pp. 424-5). In this instance there is only one major alternate opportunity available, namely to exclusively sell surveillance technology to States unlikely to use it to enable GHRV.

As much wealth and success is to be made in the surveillance technology industry, the perception of gain is probably very high. Amesys, for example, points out that when it added dual-use technologies to their business-activities in 2004, it achieved an average annual growth of 27%, and in 2008 40% of their €100 million turnover came from dual-use technology. The products it sold to Libya specifically, yielded it €26,5 million (Manach, 2011a). Important to note, however, is that there are no precise numbers indicating which percentage of surveillance technology products are sold to authoritarian countries, and how gain would be affected if companies were only to sell to non-authoritarian countries. It seems reasonable to expect authoritarian States to be responsible for a large portion of the surveillance technology sales, as they have the greatest interest in being able to surveil and hack their citizens' activities in cyberspace, but this is mere speculation. Yet irrespective of the size of this percentage, the perception of gain for the alternate opportunity is much smaller, not only because a number of potential clients are omitted, but also as it would even *cost* the companies money. Without concrete trade regulations indicating which customers pose a risk and which do not, the companies themselves would have to invest money and resources in making this assessment.

Additionally, while the gain is high, there is hardly any risk in selling surveillance technology to authoritarian governments. Laws are, according to Coleman (1987) "the most basic of all forces shaping the distribution of opportunities" (p. 425) and the absence of laws prohibiting the sale of surveillance technology to countries likely to abuse it, makes the risk of punishment virtually zero. It should of course be noted that Amesys is currently being investigated; however, I maintain that as this was the very first prosecution of its kind, and even the prosecutor was not eager to take on the case, it was an unforeseen risk that had not influenced the perceived opportunity structure. The way in which companies have responded now these legal risks -as well as social risk, such as public rejection- have become clearer is very telling; Bull/Amesys and Gamma divested their surveillance units following investigations (a criminal investigation in the case of Amesys and OECD investigations regarding Gamma).

Afterwards the sale of surveillance technology was continued by smaller companies, which operated exclusively in the surveillance technology industry. This suggests that the nature of the company is related to the risks it is willing to take; companies that engage in a number of business activities, like Gamma, Amesys and NSN (which had sold its intelligence unit just prior to allegations, according to the company itself partly due to an increased risk of human rights violations), can easily divest their surveillance technology units and focus on other areas when the risks become more pronounced. For companies specialised in surveillance technology, like Area, Trovicor and FinFisher this is not an option, which probably makes them willing to accept higher risks. Additionally, also the type of customers on which a company relies is likely to play a role here. NSN relied on governments, other companies, and consumers to buy its products, while the other companies solely sold to governments and/or businesses. Arguably this made NSN much more vulnerable to public pressure, and thus selling surveillance technology had a higher social risk for it. This could explain why NSN decided to exit the monitoring business; the company itself maintains to have done this primarily for human rights concerns, but this argument is not very convincing as NSN sold Trovicor to Perusa rather than dissolve it, and continued to refer former customers to it. It thus had done nothing to prevent the products it once created from continuing to enable future GHRV, but at the same time it had decreased its own risk, as it is no longer directly involved. Notably, however, the company still suffered public condemnation through journalistic articles and a public boycott *after* it had divested its surveillance unit. Consequently NSN maintained that "as a result of these credible reports [of the use of its products in Iran], Nokia Siemens Networks halted all work related to monitoring centers in Iran in 2009" (NSN, 2010c) and that the issues raised in the Bloomberg News article on its sales with Iran led it to be "the first telecommunications equipment provider to adopt a human rights policy specifically addressing the issues of new technologies and privacy, access to information, and freedom of expression" (NSN, 2011). I found no evidence of companies or non-authoritarian governments putting pressure on corporations to refrain from selling to authoritarian States; rather, democratic and non-democratic governments visit the same ISS conferences to get in contact with surveillance technology companies (ISS World, n.d.), which indicates that democratic governments are doing little to condemn these types of sales.

With the data at hand we cannot know to which extent the opportunity of developing and selling surveillance technology to authoritarian governments is compatible with previously held ideas, rationalisations and beliefs of the individual actors. However, a similar tension as with the normative restraints is likely to apply here, where at the one hand technology is seen as a force of good, while on the other hand people are mostly opposed to doing harm. I think the first mostly prevails here, as the fact that their actions contribute to harm is not something

employees have to think about, following the emotional and geographic distance between the corporation and the victims (Huisman, 2010, p. 23). When this becomes more visible the opportunity might no longer be compatible with previously held ideas and beliefs. This seems to have been the case for the Area employee who broke confidentiality when he gave an interview regarding the company's sales with Syria (Silver and Elgin, 2011). Although the business with Syria had been ongoing for a while, it was only after the outbreak of the civil war in the country, when the behaviour of the State against its citizens had become more visible, that he decided to give an interview. The changing situation in Syria had also changed the opportunity structure.

DISCUSSION & CONCLUSION

With the current research I have attempted to explore the etiology of the involvement in GHRV of four companies; Nokia Siemens Networks/Trovicor, FinFisher, Amesys and Area, by answering three questions; *how does the sale of surveillance technology enable GHRV? is selling surveillance technology that is used to enable GHRV crime?* and *how can the involvement of Nokia Siemens Networks/Trovicor, FinFisher, Amesys and Area in GHRV be explained, using Coleman's theory of motivation and opportunity?*

The question *how does the sale of surveillance technology enable GHRV?* was dealt with in the first part of this article. I set out how States, both authoritarian and democratic, have increased their interest in being able to control cyberspace now that is playing an all-encompassing role in people's lives. Especially for authoritarian States –known to also have employed far-reaching measures to silence dissenting voices in the past– the stakes to do so are high. Surveillance technology companies have created a variety of products to meet these demands, but have also created products that go beyond the demand and even the imagination of States, and thus have shaped the realm of the possible. Through surveillance technology the identification and surveillance of dissidents has become easier than ever before; entire mobile or online networks can be scanned in order to identify dissidents of whom the government was previously unaware. Moreover, devices (computers or smartphones) of previously identified targets can be hacked, giving access to everything stored on it or done with it, and providing the opportunity to remotely turn on the camera or microphone. However, although surveillance technology enables the identification and surveillance of dissidents, it can also be employed for the identification of criminals, and it thus has a dual use. In contrast to 'regular' dual use technology, however, the technological functionality of surveillance technology remains exactly the same when used for 'normal' or harmful purposes. The difference between the two uses lies rather in the people targeted, which is largely determined by the definition of crime in a country, and the extent to which the State respects human rights.

In order to answer the second question, *is selling surveillance technology that is used to enable GHRV crime?* I looked at two ways in which it can be regulated; namely by addressing corporate complicity in crimes by others, or by prohibiting the corporate contribution on its own through trade regulations. I further looked at three legal frameworks; international regulations, home-State regulations, and customer-State regulations. I found that the sale of surveillance technology is not adequately regulated at the moment. At the international level there are no regulations regarding (involvement in) GHRV or trade that are directly binding on corporations; this is to be ensured by States. Customer-States, however, do not effectively regulate this, following their clear interest in obtaining these products from the corporations. Home-State regulations are the most far reaching; local laws dealing with corporate complicity in GHRV or international crimes have led to a number of criminal and civil cases against (surveillance technology) corporations, and also trade regulations tend to be more extensive in home-States. However, though home-State regulations are most significant, these also do not adequately address corporate involvement in GHRV at the moment. I have argued, however, that the absence of adequate legal regulations should not exclude these acts from criminological scrutiny, as the use of surveillance technology does cause social harm, and the corporations took a foreseeable risk by selling this.

In the last part of this article I have aimed to explore the question *how can the involvement of Nokia Siemens Networks/Trovicor, FinFisher, Amesys and Area in GHRV be explained, using Coleman's theory of motivation and opportunity?* Coleman maintained that corporate crime occurs as the result of the confluence of appropriate motivation and opportunity. Motivation, according to him, is influenced by two aspects: neutralisation techniques and the culture of competition, of which the latter is restrained by social norms he calls normative restraints. Opportunity, according to Coleman, is determined by four factors; perception of gain, perception of risk, compatibility with previously held ideas, rationalisations and beliefs, and the availability of alternate opportunities. When applying his theory to the four cases I found a number of factors that influenced the companies' motivation and opportunity structure. First, they operate in a climate where much profit can be gained by conducting business with clients likely to use their products to enable GHRV. This increases the attractiveness of the opportunity to become engaged in GHRV, but is also a motivating factor on its own in our capitalist society. Furthermore, the absence of laws also affects both opportunity and motivation; the absence of risk increases the attractiveness of the opportunity, while the intrinsic opposition to breaking the law does not function as a normative restraint to the desire to gain wealth and success. Other types of risks, such as public condemnation, do not strongly influence the perception of risk of the majority of these companies, as they do not sell to

consumers but solely to States and other companies (in this regard NSN is an exception). These factors taken together create a situation where there is both initial motivation and opportunity. Neutralisation techniques allow people to engage in GHRV while still maintaining a non-deviant self-image. A number of neutralisation techniques can be identified in the statements of the companies assessed here; firstly, responsibility is often denied and transferred, either to the customer-State, which actually commits the GHRV, to the home-State, which does not legislate, or to the industry as a whole, as 'everyone' does it. Secondly, the companies discussed here 'denied' that there were victims, by maintaining that their products were used to catch criminals rather than dissidents. They further neutralised their behaviour by focussing on the positive effects of technology on democracy and human rights, and by lessening the harm by solely focussing on the violation of the right to privacy or freedom of speech rather than on more serious violations of human rights such as torture or murder.

Coleman's theory mostly fit the cases quite well, except for one aspect; Coleman maintains that the primary motivating force of human behaviour stems from the culture of competition, which makes that people mostly engage in harmful behaviour based on economic self-interest. From the cases it seemed, rather, that many people within these companies are also engaging in this behaviour because they find the work very interesting; the cat and mouse game between dissidents and governments asks for continuous innovation and poses an interesting intellectual challenge to employees. Striving for innovation and technical perfection is also put forward as an alternative motivational force by van Baar and Huisman (2012) in their study of Topf & Söhne, the corporation that build the ovens used by the Nazis in the Holocaust; although a difference is that in their case study the motivational factor to strive for better products originated in the internal competition *within* the company –a desire of the engineers to design better ovens than their colleagues- while here the surveillance technology companies' strive for innovation originates from the challenge posed by aiming to outwit the mice. With regards to Coleman's theory, I would argue that it is too simplistic to reduce human behaviour to one primary motivating force. It seems more likely that a number of motivating forces exist, including the culture of competition, as well as a desire to engage in work that is intellectually challenging and to strive for innovation and technical perfection. Depending on the context different motivating forces might be more influential. Following this reasoning it is unsurprising that the culture of competition is the most prevalent motivating force for 'regular' corporate crime, as corporations normally work out of an economic interest, and it is mostly quite clear that a violation of the laws leads to an increase of gain (or reduction of losses). This link is less clear in cases of corporate-facilitated State crime, primarily because the behaviour is not obviously 'crime.' The absence of clear laws, paired with the large emotional and geographical

distance between corporate employees and the victims, and a corporate focus on achieving technical possibilities rather than viewing technology as a means to an end, enables employees not to have to think of the consequences of their acts; which, to relate it to Bauman (1989), replaces their moral responsibility for a technical responsibility. In such a context, I would argue, an initial desire for intellectually challenging work, and a strive for innovation and technical perfection, is a significant motivating factor.

An aspect very prevalent in both the motivations and opportunities structure is the absence of laws. Arguably the adoption of clearer regulations regarding corporate involvement in GHRV or trade in surveillance technology by home-States might lead to a deduction in the prevalence of this conduct; as it would decrease the attractiveness of the opportunity, and constrain the motivation. However, considering the fast-changing nature of technology, the dual-use of the products and the international character of the involvement, creating adequate legal regulations will be extremely difficult, if not impossible. A less far-reaching approach might be to adopt very detailed guidelines (either internationally or nationally) which include country specific information, intended to help corporations to assess the human rights situation in customer-States. This would at least make it easier for companies *wanting* to avoid selling to customers likely to use it for GHRV, as they currently have to make this assessment themselves. Of course, as the current behaviour results from a combination of factors, it is unlikely that regulations or guidelines would prevent the sale of surveillance technology to authoritarian States altogether, but it might become less widespread than it is now. Additionally, a greater societal focus on the harms caused by selling these products, for example through journalistic or NGO initiatives, could also decrease the prevalence of these activities. According to NSN this played a role in its decision to halt all work relating to monitoring centres in Iran, and adopt a human rights policy. It is likely, however, that only companies relying on 'regular' consumers are receptive of this type of pressure, while many surveillance technology companies exclusively sell to States or States and other companies. Public attention or pressure can also have other effects; it decreases the emotional distance between corporate employees and the victims, which might reduce the prevalence as well, as it makes it more difficult to employ neutralisation techniques such as blaming the victim, increases the importance of certain normative restraints as it becomes clearer that norms are violated, and decreases the compatibility of the opportunity with previously held ideas, rationalisations and beliefs. Arguably this happened when the civil war in Syria broke out and reporting on the country's treatment of dissidents increased, and an Area employee decided to break confidentiality and give an interview.

Nonetheless, it should be kept in mind that the generalizability of my conclusions is limited following the small-scale of the research and the use of purposive sampling. It would be interesting to have further research into the etiology of surveillance technology companies, which ideally also includes interviews with the employees, although it is unlikely that the corporations will welcome data collection. Hopefully the criminal investigations into Amesys will make data accessible that otherwise would have remained confidential. It should also be kept in mind that Coleman's theory assumes that white-collar criminals do not differ in their biological makeup or socialisation. It would be interesting to have further research focussing on whether this is actually the case. In other fields of criminology research it has been found that while it was long assumed that a certain organisational culture was criminogenic, and thus caused the antisocial behaviour of the employees, this relation was actually spurious, with people predisposed for delinquent behaviour applying for those jobs. Apel and Paternoster (2009) show this in a case study of the relationship between youth employment and delinquency, and argue that "disentangling causation from selection should be a research priority for the study of white-collar crime" (p. 15). A process of self-selection could be an (additional) explanatory factor here, as it might be that people more inclined to become engaged in GHRV are more likely to apply for a job in the surveillance technology business rather than in another technology business. Additionally, further research into the extent to which the intellectual challenge of the work and the strive for technical perfection is a motivational force, both in surveillance technology companies or in other instances of corporate-facilitated State crime, might lead to a better understanding of the etiology of corporate involvement in GHRV.

REFERENCES

Amesys (2008). *From lawful to massive interception: Aggregation of sources.* Retrieved from: https://wikileaks.org/spyfiles/files/0/21_200810-ISS-PRG-AMESYS.pdf

Amesys (2009). *Eagle Glint operator manual.* Retrieved from: https://www.wikileaks.org/spyfiles/files/0/99_AMESYS-EAGLE-GLINT-Operator_Manual.pdf

Amesys (n.d.). Official website: http://www.amesys.fr/index.php/

Apel, R., & Paternoster, R. (2009). Understanding "criminogenic" corporate culture: What white-collar crime researchers can learn from studies of the adolescent employment-crime relationship. In: S. S. Simpson, D. Weisburd (eds.), *The criminology of white-collar crime* (pp. 15-33). New York: Springer.

Area S.p.A. (2010, March 3). *Ethics Code.* Retrieved from its website: http://www.area.it/wp-content/uploads/2013/01/CodeOfEthics.pdf

Area S.p.A. (2012). Official website: http://www.area.it/

Bauman, Z. (1989). *Modernity and the holocaust.* Cambridge: Polity Press.

Bull (2010, October). *A comprehensive security offering to tackle ever-changing and varied threats.* Bull Direct n. 48 [company newsletter]. Retrieved from: http://www.bull.hu/adatok/bulldirect_no48_2010_10_eng.pdf

Bull (2011, September 1). *Amesys press release.* Retrieved from: http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=673289&lang=en

Bull (2012, March 8). *Bull Group signs exclusive agreement with a view of selling the activities relating to the Eagle software system of its subsidiary Amesys.* Retrieved from: http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=718165&lang=en

Brown, I., & Korff, D. (2012). *Digital freedoms in international law: Practical steps to protect human rights online.* Retrieved from the Global Network Initiative: http://globalnetworkinitiative.org/content/digital-freedoms-international-law-0

Buse, U., & Rosenbach, M. (2011, December 8). The transparent state enemy: Western surveillance technology in the hands of despots. *Der Spiegel.* Retrieved from: http://www.spiegel.de/

Business and Human Rights Resource Centre (2011, November, 30). *Area response to Human Rights First article re surveillance technology and oppressive regimes.* Retrieved from: http://www.business-humanrights.org/media/documents/area-response-re-surveillance-technology-oppressive-regimes-30-nov-2011.doc

Cohn, C., Timm, T., & York, J. C. (2012). *Human rights and technology sales: How corporations can avoid assisting repressive regimes.* Retrieved from the Electronic Frontier Foundation: https://www.eff.org/files/filenode/human-rights-technology-sales.pdf

Coleman, J. W. (1987). Toward an integrated theory of white-collar crime. *American Journal of Sociology, 93*(2), 406-439.

Council Regulation (EC) 36/2012, concerning restrictive measures in view of the situation in Syria. OJ L16/1.

Council Regulation (EC) 264/2012, amending Regulation (EU) No 359/2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran. OJ L87/26.

Deibert, R., & Rohozinski, R. (2012). Contesting cyberspace and the coming crisis of authority. In: R. Deibert, R. Rohozinski, J. Palfrey & J. Zittrain (Eds.), *Access contested: Security, identity and resistance in Asian cyberspace* (pp. 21-42). Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). Access contested: Toward the fourth phase of cyberspace controls. In: R. Deibert, R. Rohozinski, J. Palfrey & J. Zittrain (Eds.), *Access contested: Security, identity and resistance in Asian cyberspace* (pp. 3-20). Cambridge, MA: MIT Press.

Doe I et al. v. Cisco Systems, Inc. et al., No. 5:11-cv-02449-JF-PSG, U.S. California Northern District Court.

Du Daobin, et al. v. Cisco Systems, Inc. et al., No. 8:11-cv-01538-PJM, U.S. Maryland District Court.

Elgin, B., & Silver, V. (2011, November 4). Syria crackdown gets Italy firm's aid with U.S.-Europe spy gear. *Bloomberg News.* Retrieved from: http://www.bloomberg.com/

Executive Order 13628 (2012, October 9), authorizing the implementation of certain sanctions set forth in the Iran Threat Reduction and Syria Human Rights Act of 2012 and Additional Sanctions With Respect to Iran. Federal Register 77/198.

European Parliament (2012) Resolution on a digital freedom strategy in EU foreign policy. P7_TA-PROV(2012)0470

Farivar, C. (2010, November 18). Nokia Siemens lawsuit dropped by Iranian plaintiffs. *Deutsche Welle.* Retrieved from: http://www.dw.de/

FIDH (2013, January 15). *Amesys case: The investigation chamber green lights the investigative proceedings on the sale of surveillance equipment by Amesys to the Khadafi regime.* Retrieved from: http://www.fidh.org/

FinFisher (2014). Official website: http://www.finfisher.com/

FinFisher (n.d.). *FinFisher: Governmental IT intrusion and remote monitoring solutions.* Presentation available at: http://info.publicintelligence.net/Gamma-FinFisher.pdf

Fuchs, C. (2013). Societal and ideological impacts of deep packet inspection internet surveillance. *Information, Communication & Society, 16*(8), 1328-1359.

Gallagher, R. (2011, November 1). Governments turn to hacking techniques for surveillance of citizens. *The Guardian.* Retrieved from: http://www.theguardian.com/

Gobert, J. & Punch, M. (2003). *Rethinking corporate crime.* London: Butterworths.

Greenberg, A. (2010, October 15). Nokia Siemens denies lingering ties to Iran surveillance. *Forbes.* Retrieved from: http://www.forbes.com/

Huisman, W. (2010). *Business as usual? Corporate involvement in international crimes.* The Hague: Eleven International Publishing.

ISS World (n.d.). Official website: http://www.issworldtraining.com/index.html

International Commission of Jurists (2008). *Report of the ICJ Expert Legal Panel on corporate complicity in international crimes: Corporate complicity & legal accountability. Volume 1:*

Facing the facts and charting a legal path. Retrieved from: http://www.refworld.org/docid/4a78418c2.html

Katz, E. (2010, October 13). Holding Nokia responsible for surveillig dissidents in Iran. *Electronic Frontier Foundation.* Retrieved from: http://www.eff.org/

Knight, B. (2012, September, 19). German spyware business supports dictators. *Deutsche Welle.* Retrieved from: http://www.dw.de/

Kauzlarich, D., Kramer, R. C., Smith, B. (1992). Toward the study of governmental crime: Nuclear weapons, foreign intervention, and international law. *Humanity and Society,* 16(4), 543-563.

Kauzlarich, D., & Kramer, R. C. (1998). *Crimes of the American nuclear state: At home and abroad*. Boston: Northeastern University Press.

Kramer, R. C., Michalowski, R. J., & Kauzlarich, D. (2002). The origins and development of the concept and theory of state-corporate crime. *Crime & Delinquency,* 48(2), 263-282.

Lange, S. (2014). The end of social media revolutions. *The Fletcher Forum, 38*(1), 47-68.

MacKinnon, R. (2012). Corporate accountability in networked Asia. In: R. Deibert, R. Rohozinski, J. Palfrey & J. Zittrain (Eds.), *Access contested: Security, identity and resistance in Asian cyberspace* (pp. 195-216). Cambridge, MA: MIT Press.

Manach, J. M. (2011a, October 13). Doing business with Gaddafi: Making millions and risking lives. *OWNI.* Retrieved from: http://www.owni.eu/

Manach, J. M. (2011b, December 1). Spyfiles: Revelations of a billion dollar mass surveillance industry. *OWNI.* Retrieved from: http://www.owni.eu/

Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J. (2013). *For their eyes only: The commercialization of digital spying.* Retrieved from Citizen Lab: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Matthews R. A. (2006). Ordinary business in Nazi Germany. In: R. J. Michalowski & R. C. Kramer (Eds.), *State–corporate crime: Wrongdoing at the intersection of business and government* (pp. 116–33). New Brunswick: Rutgers University Press

Maurer, T., Omanovic, E., & Wagner, B. (2014). Uncontrolled global surveillance. *New America Foundation, Digitale Gesellschaft, & Privacy International.* Retrieved from: http://newamerica.net/

McVeigh, K. (2011, April 28). British firm offered spying software to Egyptian regime. *The Guardian.* Retrieved from: http://www.theguardian.com/

Morozov, E. (2011). *The net delusion: How not to liberate the world.* London: Penguin Books.

Nokia Siemens Networks (2010a, June 2). *Statement to the public hearing on new information technologies and human rights.* Retrieved from its website: http://nsn.com/news-

events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights

Nokia Siemens Networks (2010b, August 20). *Update: Response to the lawsuit filed by Isa and Mehdi Saharkhiz against Nokia Siemens Networks.* Press Statement retrieved from: http://nsn.com/news-events/press-room/statement-to-activist-sues-nokia-siemens-networks

Nokia Siemens Networks (2010c, September 28). *Clarifcation on Nokia Siemens Networks' business in Iran.* Press Statement retrieved from: http://nsn.com/news-events/press-room/clarification-on-nokia-siemens-networks-business-in-iran

Nokia Siemens Networks (2011, August 23). *Telecoms and human rights.* Press Statement retrieved from: http://nsn.com/news-events/press-room/statements/telecoms-and-human-rights

Nokia Solutions and Networks (2013a). *Code of Conduct.* Retrieved from its website: http://nsn.com/about-us/sustainability/our-approach/code-of-conduct

Nokia Solutions and Networks (2013b). *Human rights policy.* Retrieved from its website: http://nsn.com/about-us/sustainability/ethics-and-human-rights

Nokia Solutions and Networks (2014). Official website: http://www.nsn.com/

Privacy International (2013, February 3). *Briefing note on OECD complaints against Gamma International and Trovicor in the UK and Germany.* Retrieved from: https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2013_02_01_oecd_briefing_note.pdf

Reporters Without Borders (2013). *Enemies of the internet: 2013 report.* Retrieved from: http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf

Rhoads, C., & Chao, L. (2009, June 22). Iran's web spying aided by Western technology: European gear used in vast effort to monitor communications. *The Wall Street Journal.* Retrieved from: http://online.wsj.com

Rome Statute of the International Criminal Court (amended 2010).

Rothe, D. L., & Mullins, C. W. (2009). Toward a criminology of international criminal law: An integrated theory of international criminal violations. International Journal of Comparative and Applied Criminal Justice, 33(1), 97-118.

Ruggie, J. (2011, March 21). Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. UN Human Rights Council A/HRC/17/31

Saharkhiz, et al. v. Nokia Corporation, et al., No. 1:10-cv-912-AJT-TRJ, U.S. Virginia Eastern District Court.

Salies, S. (n.d.). LinkedIn account: https://www.linkedin.com/pub/st%C3%A9phane-salies/9/45b/703 (accessed 26 June 2014).

Satter, R. (2013, March 13). Researchers find German-made spyware across globe. *R&D.* Retrieved from: http://www.rdmag.com/

Schaake, M. (2013, May 5). *In defense of digital freedom.* Retrieved from her own website: http://www.marietjeschaake.eu/2013/05/in-defence-of-digital-freedom/

Schwendinger, H., & Schwendinger, J. (1970). Defenders of order or guardians of human rights. *Issues in Criminology*, 5(2), 123-157.

Silver, V., & Elgin, B. (2011, November 9). Area SpA may exit Syrian monitoring project. *Bloomberg News.* Retrieved from: http://www.bloomberg.com/

Silver, V. (2011, November 28). Italian firm said to exit Syrian monitoring project. *Bloomberg News.* Retrieved from: http://www.bloomberg.com/

Silver, V. (2012, November 9). MJM as personified evil says spyware saves lives not kills them. *Bloomberg News.* Retrieved from: http://www.bloomberg.com/

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 664-670.

Timm, T. (2012, February 21). Spy tech companies & their authoritarian customers, part II: Trovicor and Area SpA. *Electronic Frontier Foundation.* Retrieved from: http://www.eff.org/

Trovicor (2012a). *Jahresabschluss zum geschäftsjahr vom 01.01.2010 bis zum 31.12.2010.* Retrieved from: http://buggedplanet.info/images/d/de/TROVICOR-20101231.pdf

Trovicor (2012b). *Paris expo flyer.* Retrieved from: http://www.wikileaks.org/spyfiles/docs/TROVICOR-2012-PariExpo-en.pdf

Trovicor (2013). *Code of Business conduct.* Retrieved from its website: http://www.trovicor.com/

Trovicor (n.d.). Official website: http://www.trovicor.com/

United Kingdom National Contact Point (2013, June). *Initial assessment by the UK National Contact Point for the OECD guidelines for multinational enterprises: Complaint from Privacy International and Others against Gamma International UK Ltd.* Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208112/bis-13-947-complaint-from-privacy-international-and-others-against-gamma-international-uk-ltd.pdf

Valentino-Devries, J. (2011, November 21). Surveillance company says it sent fake iTunes, flash updates. *The Wall Street Journal.* Retrieved from: http://online.wsj.com

Van Baar, A., & Huisman, W. (2012). The oven builders of the holocaust: A case study of corporate complicity in international crimes. *British Journal of Criminology 52*(6), 1033-1050.

Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies: *List of dual-use goods and technologies and amunitions list* (amended 2013).

Wikileaks (2011). *The Spyfiles: Gamma.* Retrieved May 27, 2014, from: http://wikileaks.org/spyfiles/list/company-name/gamma.html

Wikileaks (n.d.). *The Spyfiles.* Retrieved May 27, 2014, from https://wikileaks.org/the-spyfiles.html

Xiaoning et al. v. Yahoo! Inc, et al., No. 4:07-cv-02151-CW, U.S. California Northern District Court.