2014

Towards an integrated EU ICT security policy: What are the political and technical obstacles of securing the European IT infrastructure against espionage and surveillance and how can they be overcome?

Mario Schulze

11045426

Academy of European Studies & Communication Management

ES3-3B, The Hague University of Applied Sciences

June 21st 2014

Dissertation supervisor: Paul G. Nixon

Executive Summary

This research paper concerns itself with the technical and political obstacles of securing the EU cyber space against espionage and surveillance both amongst the member states and particularly those emerging from foreign powers. The scope of the research is limited to signals intelligence (SIGINT) related measures used by states to retrieve intelligence about state and non-state actors.

One major finding is that both mass surveillance and espionage are difficult to address from a legal point of view. International human rights law, is supposed to guarantee a right to privacy, however has no extraterritorial applicability for states, which made sense during the 1970s, but not in the age of cloud computing and social media. Espionage during peace time on the other hand is not even addressed by international public law.

Mass surveillance is also difficult to prevent because a lot of popular internet services are located in the USA and are thus subject to laws that require them to release user data to authorities under conditions which do not meet European data safety standards.

A particular issue in regards to European states counter-espionage capabilities is that these are underdeveloped due to a lack of competence in signals intelligence matters. This could be a direct result of the reliance on NATO and UKUSA signals intelligence sharing, which meant that European states gained cheap access to security related information, however, without considering that the means used to obtain this information could be turned against them in the form of espionage programs.

The author comes to the conclusion, that the EU member states should seek closer inner European collaboration in intelligence matters and particularly SIGINT sharing. The strategy vis-à-vis the US intelligence apparatus should be reconsidered and should not just comprise elements of collaboration, but also such of counter-intelligence. Subsequently, the creation of a European SIGINT agency under the provision of voluntary member state participation is recommended. In regards to tackling the problem of mass surveillance, the author finds that by requiring foreign enterprise to comply with EU Law even when operating abroad and by subsequently imposing direct and indirect financial penalties on enterprise in case of non-compliance, the EU and its member states have already taken appropriate steps in the recent past. However, the situation could be further improved through investment in research and development of domestically produced, safety-related IT products and services.

CONTENTS

TERMINOLOGY

Term	Description
DNI	DNI is “the intelligence from intercepted digital data communications transmitted between, or resident on, networked computers” (Richelson, 2005).
DNR	Short for Dial Number Recognition, it describes a technique used for telephone monitoring and tapping (Farivar, 2013).
Metadata	Although different types of metadata exist for different purposes, the word describes in the widest sense data that is used to catalogue other data. In a movie file e.g. metadata contains information such as the file name, length of the video stream, the date of creation and other information that make it possible to identify the resource (NISO, 2001).
SIGAD	A SIGINT Activity Designator is a label used to identify the signal collection station responsible for establishing a signal intelligence (SIGINT). “The first two letters indicate the country and can be US for the United States, UK for the United Kingdom, CA for Canada, AU for Australia and NZ for New Zealand. Then comes one letter indicating what sort of staff runs the station, which can be M for Army, N for Navy, A for Air Force, J for Joint services (mainly military), F for Joint services (mainly civilian), D for Detachment or C for Civilian staff. After a hyphen follows a unique number which identifies the particular facility” (SIGINT Activity Designators (SIGADs), 2014)
SIGINT	Signals intelligence – contracted SIGINT – is the interception of a signal, which can be communication between people (COMINT), devices (ELINT) or a combination thereof (SIGINT Activity Designators (SIGADs), 2014).
Upstream collection	Refers to methods used to harvest data directly from “fibre-optic cable networks that carry much of the world’s Internet and phone data” (Washington Post, 2013)

INTRODUCTION

On June 6th 2013 local time, the British newspaper “The Guardian“ revealed that it had received classified NSA documents by an insider of the agency. A first report revealed that the National Security Agency had, on a large scale, collected the phone records of customers of major US telecommunications company Verizon (Greenwald, NSA collecting phone records of millions of Verizon customers daily, 2013). This first report alone set into motion a wave of new reports by newspapers around the world, which then subsequently revealed a much larger picture of surveillance and espionage carried out by the US intelligence agency and subsequently raised the question of how European politics should react to such acts, especially when committed by a military ally.

The question of how the European IT infrastructure can be protected against these types of state executed attacks of course can be answered in a multitude of ways depending on personal perspective. Espionage and surveillance may at first glance constitute two separate topics, however, regardless of their different purposes, both represent instances of intelligence gathering normally carried out by a secret service and as the paper will show have become interconnected.

The paper strives to answer the main research question in four steps. Step one aims to identify the sources of all threats to information security in the EU. In a second step this work will explore the correlation between these threats and the European countries’ policies regarding SIGINT collection and counterintelligence. Thirdly, the existing defence mechanisms will be scrutinized regarding their advantages and disadvantages. Lastly, based on the data collected, the author will then make a recommendation regarding possible moves to improve information safety within the EU.

The main question of this research requires a pragmatic answer, which is why mass surveillance will not be scrutinized regarding its ethical implications. Since, however, the advantages and disadvantages of mass surveillance have ethical implications in themselves (security vs liberty) the paper will simply orient itself towards case law of the European Court of Justice. In its most recent decision regarding the legality of the retention of user metadata by European communications service providers, the court ruled that surveillance techniques even for the legitimate purpose of national security are incompatible with the European Covenant on Human Rights (ECHR) so long as they occur “without any differentiation,

limitation or exception being made in the light of the objective of fighting against serious crime" (European Court of Justice, 2014). This ruling will subsequently form the ideological basis for evaluating all mass surveillance related data.

Moreover, the topics of mass surveillance and espionage are undoubtedly highly complex issues from a technical point of view, which is why this paper cannot give any in-depth solution, but will rather try to give pointers about what should be the focal points of attention when it comes to tackling this part of the problem. As to the scope of this research it shall be clarified that due to page limit constraints not all forms of espionage can be covered, but only such that are performed strictly by use of the global ICT infrastructure. This limitation concerns e.g. special usage scenarios of military grade technology such as radio pathway attacks, which do not rely on traditional means of cable based intercommunication.

The methodology used for this research mainly consisted of desk research, with the majority of sources being either academic journals, official press releases or main stream press articles. More traditional print media was not deemed appropriate for this research since IT brings about massive changes within short periods of time, thus quickly rendering older publications regarding SIGINT obsolete especially where this information describes techniques only developed by the secret services within the past few years. Similarly, as of the time of writing the EU was reforming or even terminating old and introducing new data protection laws, so that literature on these laws was either not up to date or not yet available. What is more, informed contributors of articles on mass surveillance and espionage such as Glenn Greenwald, author of the Guardian, published their information for free and everything that could have been considered novelty in books such as "No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State" was quickly picked up on in the articles of commentators. An interview with an employee of the EU Directorate-General for Communications Networks, Content and Technology was conducted for this research as well, however, did not yield too many conclusive results. Furthermore, the interviewee made it clear that he was only giving his personal opinion and not official statements, which somewhat limits the academic relevance of the interview.

RESULTS

ESPIONAGE AND SURVEILLANCE CAPABILTIES

USA

The United States' most important civil SIGINT body is the National Security Agency (NSA). The main mission of the agency is to "collect (including through clandestine means), process, analyse, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions". In addition to these offensive security tasks, the agency provides for the protection of the US's national IT infrastructure against attacks and is obliged to report to the Director of National Intelligence about any IT security relevant events (US National Security Agency, 2011).

UNDERWATER WIRETAPPING

The NSA deploys at least four principal wiretapping programs in order to monitor global internet traffic. These upstream collection type programs are named OAKSTAR, STORMBREW, BLARNEY and FAIRVIEW. Depending on the scale on which wiretapping is carried out, the technical requirements of such programs can be enormous. Indeed, even with dedicated filtering techniques applied, the gear used in these usage scenarios must be capable of processing the data flow of entire nations, which can amount to several terabits of data per second (the world's largest internet exchange DE-CIX located in Frankfurt handled 3.2 terabits per second peak traffic as of 2014), before storing the remaining amount of data deemed significant for analytical purposes.

What all four of these NSA programs have in common is that they intercept data sent from one foreign (non-US) communication node to another (United States Government, 2012). The data intercepted by the NSA therefore does not need to be destined for the US but is in many cases just supposed to transit through the switch of a US telecommunications provider. Furthermore, these programs are referred to as umbrellas, which means that they collect the information gathered by a number of different SIGADs. As to the location of the different programs, "it is assumed that FAIRVIEW, BLARNEY and STORMBREW are for

collection within the US and the programs under the OAKSTAR umbrella are intercept facilities elsewhere in the world" (Slides about NSA's Upstream collection, 2014).

OAKSTAR, firstly, comprises the greatest number of SIGADs. At least two of its eight Signal Intelligence Activity Designators are known to provide SIGINT data originating from European IT infrastructure. The names of these two designators are MONKEYROCKET (US-3206) and YACHTSHOP (US-3247). MONKEYROCKET is designed to collect DNI metadata and content from the Middle East, Europe and Asia (see figure 2). It is thought to have been created primarily for counter-terrorism purposes. YACHTSHOP, which has global reach is said to collect metadata using the infrastructure of a foreign communications partner only known by the codename BLUEANCHOR. All intelligence gathered from YACHTSHOP is fed into the MARINA called NSA database used for storing global internet metadata (see figure 1). The remaining six SIGADs under the OAKSTAR umbrella (see figure 3) are largely thought to intercept data coming from or destined for European networks as well, given that the other end of the connection is under surveillance. However, not all OAKSTAR labelled SIGADs have reached operational status as of yet (Slides about NSA's Upstream collection, 2014).

The second umbrella program, STORMBREW consists of only two SIGADs, one of which carries the same name as the umbrella itself. This STORMBREW SIGAD (US-983) can monitor DNR as well as DNI data, whereby DNI data collection requires previous FISA and FAA court authorization (also see section "Legal Basis" for details). Leaked NSA documents furthermore reveal the inclusion of a key corporate partner "with access to international cables, routers, and switches" (Slides about NSA's Upstream collection, 2014). This partner has meanwhile been identified by Matthew Aid, a NSA historian, as US telecommunications provider Verizon (Heil, 2013). The other SIGAD only known as MADCAPOCELOT (US-3140) can collect DNI metadata using NSA storage backend technologies such as XKeyScore (XKS), PINWALE and MARINA (Slides about NSA's Upstream collection, 2014).

FAIRVIEW, the third umbrella is a mass surveillance program with only one SIGAD allocated to it. As with STORMBREW, the Snowden documents speak of collaboration with a domestic key corporate partner without actually revealing the identity of said company, which according to Matthew Aid is AT&T. According to the Snowden documents the domestic corporate partner is supposed to establish contractual agreements with foreign internet providers to enable NSA surveillance. FAIRVIEW became known through an article by

Brazilian newspaper “Globo” which claimed that the program was responsible for stealing “email and telephone records of millions of Brazilians” (Greenwald, The NSA's mass and indiscriminate spying on Brazilians, 2013). FAIRVIEW, however, appears not to be confined to one geographic region.

Lastly there is BLARNEY, a program which is said to have been in existence since 1978 when it was still operated under the name “project SHAMROCK”. BLARNEY collects DNI metadata and like STORMBREW is executed under the control of FISA and FAA. According to the German magazine “Der Spiegel”, BLARNEY, with the help of an US telecommunications provider, is used to specifically grab foreign government data and is supposedly one of the US President’s main sources of information. The targets surveyed by BLARNEY comprise “diplomatic establishment, counter-terrorism, foreign government and economic” players (SPIEGEL, 2013).

PRISM

Prism is a complex surveillance program deployed for the direct interception of user data from nine hefty-weight US internet companies. As can be seen in figure 4, the list comprises such well-known names as Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. The slide moreover reveals which data types are collected by the PRISM program. Unlike the majority of known upstream programs that are currently in use, PRISM data collection is not limited to the gathering of metadata type information. Depending on the source, the data collected by PRISM may include the contents of e-mail, voice and video chat, video, photos, stored files, VoIP, transferred files, video conferencing, logins, social networking and other custom data types. According to the data that can be seen in figure 5, and according to the interpretation provided by the New York Times, the collected data is first filtered for relevant contents, and then sorted by type of content. In a last step, before passing on the data to the relevant data analysis and storage tools, all records of US citizens must be removed since the NSA is only legally allowed to collect data of people residing outside of the USA (The Washington Post, 2013). Some of the companies involved were quick to deny any involvement in the surveillance of their customers, however various media reports found that the firms had collaborated with the NSA (Rushe, 2013). While the businesses were not always legally required to do so, they were apparently given monetary incentives for their compliance (MacAskill, 2013; Nolan, 2013). On the other hand, companies who do not comply with the NSA’s requests to release information are apparently

subject to fines. Yahoo states that in 2007 the US government coerced the company to collaborate by threatening “the imposition of $250,000 in fines per day”. Yahoo appealed to the Foreign Intelligence Surveillance Court because it held that the NSA’s request was unconstitutional, but was turned down and forced to share the data with the authorities (Agencia EFE, 2014).

THE LEGAL BASIS

Nationally, monitoring of NSA activity is legitimized through the Foreign Intelligence Surveillance Act of 1978 (FISA) in which rights are granted to the executive branch of government that allow it to order surveillance against selected foreign targets. Only the president may, through the Attorney General, order surveillance of a target without a court order for a maximum of one year or for 15 days after a declaration of war. All other applications made by a Federal officer to the Attorney General require court authorization. The court in question is the United States Foreign Intelligence Surveillance Court, which too is established under the FISA. Eligible targets for surveillance according to 50 U.S. Code § 1801 include foreign powers such as “a foreign government or any component thereof, whether or not recognized by the United States”, “a faction of a foreign nation or nations, not substantially composed of United States persons” (political parties), “an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments” (ministries and other authorities), “a group engaged in international terrorism or activities in preparation therefor”, “a foreign-based political organization, not substantially composed of United States persons” (NGOs, unions), “an entity that is directed and controlled by a foreign government or governments” (state owned business such as public transport, waterworks, electricity companies) or “an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction”. Only the first three types of targets named on this list can be surveyed without a warrant. Eligibility for targeting furthermore extends to all “agents” of these foreign powers. The applicants are to ensure to provide so-called minimization procedures, which guarantee that no data about or intended to be sent to US citizens is intercepted, stored or published. Ensuring that foreign citizens, who cannot be associated with foreign powers as defined by FISA, are not targeted does not form part of this procedure unless these persons have been granted permanent residence in the US (50 U.S. Code § 1801 - Definitions, 2008; 50 U.S. Code § 1802 - Electronic surveillance authorization

without court order, 2008; 50 U.S. Code § 1805 - Issuance of order, 2008; 50 U.S. Code § 1811 - Authorization during time of war, 2008). FISA was last amended in 2008 and several new provisions such as a release from liability for telecommunications companies collaborating with the secret services were added (Text of the FISA Amendments Act of 2008, 2008).

RUSSIA

Surveillance and spying activities in foreign countries are carried out by Russia's Sluzhba Vneshney Razvedki (SVR), which together with the domestic intelligence service Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii (FSB), is a successor organization to the Komitet gosudarstvennoy bezopasnosti (KGB). Unlike the NSA, the FSB and SVR are not dedicated SIGINT collectors, but like FBI and CIA also carry out human intelligence (HUMINT) missions.

Not much detailed information is available about either of the agencies' SIGINT programs. The little information publicly known was provided by former agents of these services such as Alexei Filatov. It is generally agreed that the FSB's wiretapping techniques largely resemble those of the NSA, however without providing the same quality results. When asked in an interview by the Russian TV broadcaster MIR-TV about "why Russian officials and pro-Kremlin analysts were so up in arms about PRISM, the NSA foreign -espionage program that Snowden leaked, Filatov answered that Russian officials were just envious about the huge capabilities gap between the NSA and Russia's equivalent intelligence agencies" (Bohm, 2013).

The Moscow Times also reports that Russia's relatively low success in terms of global surveillance can be attributed to the infrastructural disadvantage it suffers compared to the USA. Most major internet services are hosted on servers on US soil and therefore make it more feasible for the NSA to grab data as it is directed through the domestic grid. The Russian intelligence services thus could likely be more successful in their endeavours if globally popular services were hosted in Russia, since technology for surveillance similar to PRISM was generally available (Bohm, 2013).

Even though there is no detailed record of SVR foreign surveillance and espionage programs it can at least be estimated what capabilities such programs would have by looking at the FSB's domestic surveillance agenda. Its umbrella program, which is called System for Operative Investigative Activities (SORM) was divided into three subdivisions by the names

SORM-1, SORM-2 and SORM-3. “SORM-1 intercepts telephone traffic, including mobile networks; SORM-2 monitors Internet communication, including VoIP (Voice over Internet Protocol) programs like Skype; and SORM-3 gathers information from all types of communication media”. SORM is said to be around since the mid-1980 and works similar to the US wiretapping systems. By attaching a dedicated splitting device to an internet service provider’s infrastructure, the FSB gains access to all the information passing through the company’s cables. Nevertheless, there also appear to be differences to the US data collection system. While the NSA is legally compelled to seek binding agreements with providers before it can commence its surveillance activities, the FSB can not only enforce this cooperation, but is even legally entitled to order an internet service provider to install the FSB’s surveillance devices on its network at the provider’s own expense. Notwithstanding its enormous data collection capabilities however, the FSB is apparently also strongly limited in its analysis capabilities for shortage of manpower (Blyth, 2013).

According to data leaked from private US intelligence gathering company Stratford, Russia is – regardless of all technological and logistical backlogs - still seen as one of the main threats to the US’s economic and military secrets, even though in recent times China’s attacks on US IT infrastructure are seen as somewhat more potent. Russian attacks generally target the retrieval of information and communications technologies -- military and dual-purpose; developments relating to alternative energy systems; medical and pharmaceutical developments; and business-related and macroeconomic information (Stratfor, 2011).

CHINA

China in the past has repeatedly been accused of political and economic espionage by a number of governments. Quite unusually, the country lacks a civil foreign intelligence bureau. Economic and political espionage and surveillance in the exterior are said to be carried out by an arm of the Chinese armed forces, even though China denies all such reports, saying that the country was a victim of hacker attacks itself and that all military resources were used for defensive capabilities. However, there is evidence that suggests otherwise.

In 2007 German officials reported they had stopped the transfer of 160 gigabytes worth of data after Chinese hackers had infiltrated the computer networks of the Chancellery and three German ministries using a trojan. The officials were unable to provide concrete

evidence because the hackers used a South Korean proxy server as a disguise for the attack (SPIEGEL, 2007). However, the country has not only been subject to attacks against its political organs. The German economy is said to lose 50 bn. Euro per year to industrial espionage and China, which is said to employ millions of agent for cyber espionage, together with Russia, is suspected to be the main source of these losses (Connolly, 2009).

The US has been voicing similar complaints against China. In recent times, two particular units, known as Unit 61398 and Unit 61486 of the 2nd China Army received press in the USA for stealing trade secrets and high tech blueprints. The groups used so-called 'spear fishing attacks' to gain access to the networks of high profile US companies such as Coca-Cola and RSA. Unlike in Germany, security professionals were able to trace back the origin of the attacks to the headquarters of the two military units based in Shanghai (Perlroth, 2014; Sanger, Barboza, & Perloth, 2013).

INTELLIGENCE GATHERING CAPABILITIES OF THE EU

The European External Action Service (EEAS) can be seen as the most high-level EU authority in terms of intelligence since it is directly subordinated to the EU High Representative (HR). The EEAS is an autonomous diplomatic service with limited intelligence gathering capabilities, which was created and legitimized through the Lisbon Treaty. Intelligence gathering takes place in the Intelligence Centre (IntCen, formerly Joint Situation Centre (SitCen)) called arm of the institution. IntCen used to be an independent authority before being incorporated by the EEAS on January 1st, 2011. The purpose of IntCen is to collect information from "Member States' security and intelligence services, open sources (media, websites, blogs etc.), diplomatic reporting, consular warden networks, international organizations, NGOs, CSDP missions and operations, EU Satellite Centre, visits and fact-finding missions" and to then report back to its customers, which comprise the HR and EEAS, "the various EU decision making bodies in the fields of CSFP/CSDP and CT, as well as to the Member States". It is important in this sense to point out that IntCen cannot produce any information on its own but is dependent on third parties for the exercising of its powers (European External Action Service, 2012). A research report on the IntCen revealed that member country officials were dissatisfied with the quality of the reports provided by the institution. "Many member state representatives have claimed that they receive the same level of information and analysis but faster through magazines (e.g. Time, the Economist, Newsweek) or open source news providers. The added value is, however, the information put forward by SitCen has been checked" (Cross-border Research Association).

In addition to an autonomous SIGINT collection agent, the EU also lacks a common intelligence policy that could serve as a basis for meaningful corporation in this area. Safety and security are a national matter and many if not most states in the EU insist on their sovereignty in this area. One notable exemption to this rule is the Common Foreign and Security Policy (CFSP), which includes a Common Security and Defence Policy (CSDP).

Cooperation in SIGINT matters and intelligence within the EU is thus mainly based on bilateral cooperation between the national agencies (Cross-border Research Association) and even then is limited in its scope. Beyond UK-US cooperation: “What is not as well recognized is the scale of other less complete exchanges that have developed with other Western countries and between them. The result is a patchwork of bilateral and multilateral arrangements of all kinds and all degrees of intimacy. The patchwork is unusual in its secrecy, but otherwise is not unlike the intergovernmental arrangements that have developed in other specialized areas” (Herman, 1996, p. 203).

EU ANTI-ESPIONAGE AND DATA SAFETY INITIATIVES

The EU recently introduced a wealth of new legislation that aims to improve data security for government, business and individuals. After recognizing that a number of states in Europe still had not developed a national cyber security strategy, the union in 2013 introduced the EU Cyber Security Strategy. Under the provisions of the strategy, the EU member states are obliged to report attacks on their national IT infrastructure to the European Commission. Along with the strategy itself, the Commission subsequently published a list of companies whose protection would need special attention, amongst them online retailers, search engines, ISPs and cloud service providers. The strategy moreover requires the EU governments to establish dedicated agencies responsible for ensuring information safety by coordinating the monitoring of attacks on national infrastructure as well as providing technical assistance to business. Examples of such agencies which are already operative are the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) in France, the British Communications-Electronics Security Group (CESG; a subsidiary of the GCHQ), the Spanish Instituto Nacional de Tecnologías de la Comunicación (INTECO) as well as the Bundesamt für Sicherheit in der Informationstechnik (BSI) and the Nationales Cyberabwehrzentrum (created specifically to respond to attacks on government computers) in Germany. On the supranational level these national organs will be assisted in their missions by the European Union Agency for Network and Information Security (ENISA).

Even though generally considered to be a step in the right direction, the strategy has drawn some criticism because “member states will have to audit ‘critical infrastructure’, including off-site cloud storage facilities ‘for all services, no matter if they are in Europe’”. The general consensus is that this is hard to put into practice without member states creating binding agreements with the relevant service providers abroad, especially however since such agreements would have to be created with service providers of all scopes and not just the most critical ones. The main goal however lies in compelling EU enterprise which have acted secretively in the past (e.g. for the fear of loss of reputation) to share their knowledge about security breaches in their infrastructure (Hall, 2013; Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013).

In 2014 the EU followed up with a reform of the 1995 Data Protection Directive, which was turned into an EU regulation in the process. The most important changes included: The complete harmonization of EU member privacy law, the introduction of single authority responsible for supervising business compliance, the introduction of penalties of up to 2% of a company’s global annual turnover in case of non-compliance with EU privacy standards, an obligation for big enterprises to appoint a Data Protection Officer (whereas small and medium business was exempt) and the ‘right to be forgotten, which allows individuals to have their personal data erased if this does not contradict public interest (European Commission, 2014). Companies moreover have to report data breaches to EU authorities within 72 hours. The regulation applies for every enterprise that offers products or services to citizens in an EU member country.

TECHNICAL CHALLENGES

DANGERS DERIVED FROM FOREIGN MADE HARD- AND SOFTWARE

Unfortunately there are also issues which the EU cannot immediately solve through new legislation. One of these problems is the ongoing reliance of European industries on networking products from abroad, which may pose an attack vector for secret services when these products are installed in a critical environment.

The manufacturers of most networking gear used in Europe come from China (Huawei, ZTE) and the USA (Linksys, Cisco, Netgear). Both China and the US frequently accuse each other’s domestic network hardware manufacturers of producing manipulated hardware, in the case of China particularly for the purpose of facilitating industrial espionage.

Although neither state has gone as far as applying embargos, a US congressional panel made it clear that they held the notion that Chinese networking companies Huawei and ZTE posed a threat to national security. More precisely, the panel argued that “the firms failed to allay fears about their association with China's government and military”. The panel went on to recommend excluding any Huawei or ZTE equipment or component parts from being used by government contractors. Both companies denied the accusations (BBC, 2012). Ironically, the Snowden files later revealed the NSA breaking into Huawei company networks (Jopson, Hornby, & Clover, 2014) and a separate report found that the NSA had regularly intercepted and manipulated US made servers and switches by Cisco destined to be delivered abroad for use in critical infrastructure (BBC, 2014).

Software engineered in the US is equally suspected to be manipulated. Especially newer versions of Microsoft’s popular operation system Windows are said to have a preinstalled backdoor to facilitate NSA access. The German data security agency BSI therefore recommended government agencies not to install Windows 8 on government computers (Beuth, 2013). China’s government, having similar fears, started replacing Windows computers with a custom government developed version of Linux and advised businesses to follow suit (O'Brien, 2013). Starting September 2013 reports surfaced that the NSA was also striving for control over all encrypted internet data. To achieve this, the agency used “supercomputers, technical trickery, court orders and behind-the-scenes persuasion”, the report says. US technology companies say they have been coerced by court order to build master keys and backdoors into their crypto-products so it would be easier for the NSA to decrypt encrypted data. The report warns that by weakening the cryptographic strength of their products the companies were not only opening the door to the NSA but to any entity capable of exploiting such backdoors. In cases where the NSA is unable to implement backdoors or crack code through supercomputing it compels companies who secure their data to allow pre- or post-encryption access to data. US “Safe e-mail” provider Lavabit was one of a number of companies closing their business for good when they were put under massive government pressure to collaborate with the NSA. Ladar Levison, the founder of the company, addressed the public in the aftermath, stating: “Without Congressional action or a strong judicial precedent, I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States” (Perloth, Larson, & Shane, 2013).

INFRASTRUCTURAL

Another issue to data security is the current layout of the internet. Although the internet does not have a central point of control, it would be fallacious to call the internet a completely decentralized structure. This is because the number of internet services and the available bandwidth in each country is not the same anywhere in the world. To the contrary; especially at the early beginnings of the internet the USA almost had a monopoly on bandwidth and services. This situation has not completely relaxed itself until this day and only during the millennium years, the US started to route considerably less global traffic to other regions than before. The US have always appreciated this tactical advantage and continue to hold onto it, because aside from the economic advantage that an effective infrastructure poses it also considerably facilitates surveillance (Markoff, 2008).

Slide 6 shows the bandwidth through which Europe was connected to other regions of the world as of 2011. It demonstrates clearly that as of now the bandwidth between Europe and the economically growing Asia and South America regions is still marginal compared to the bandwidth the US supplies there. This is a problem because the internet is designed in a way which forces data to follow the fastest link to its location instead of following the geographically most approximate route. As a result, traffic which is often not even sent to a destination in the US is still routed through US switches.

Even though this problem has been recognized by European politics little has been done so far to improve the situation. With one exception: in the wake of the NSA scandal, the EU together with the Brazilian government has started the process of increasing the capacities between Europe and the South American continent through a new submarine cable between Portugal and Brazil in the hope of bypassing this problem (Emmott, 2014). It is as of now, however, unlikely that many other similar projects will be initiated in the near future (Frederix, 2014).

POLITICAL CHALLENGES

THE COSTS OF SIGNALS INTELLIGENCE GATHERING

European countries also face political problems which prevent an immediate reaction especially to US espionage and surveillance. For example, extensive surveillance, as it is carried out by the NSA requires a huge input of resources. Like in a major enterprise, financially this involves above all wages for personnel, acquisition and maintenance of gear and premises, research and development as well as remuneration of contractors. Determining the budget used for generating signal intelligence by the individual secret

services proves challenging because these budgets are typically not made public due to safety concerns. Enemy services could use such data to identify areas of priority and adapt their strategies accordingly (Gellman & Greg, 2013). As a consequence, the United States, like many other nations keeps the financial data of its secret services classified, so that normally it would be next to impossible to make an educated guess about the country's SIGINT related expenses. However, the Snowden documents also revealed precisely this information so that according to NY Times reports the NSA budget for 2013 was probably worth around $10.8 billion (Shane, 2013). Moreover, this number only reflects the amount of direct costs incurred by the agency. National security experts like Jeffrey T. Richelson estimate that the precise figure might be even higher, considering that the number mentioned in the report "omits much of the support it [the NSA] receives from military personnel who carry out eavesdropping on its behalf". At any rate, $10.8 billion is an astronomical number compared to the respective $730 million Germany's BND (Bundesministerium der Finanzen, 2013) and $887 billion France's DGSE (Sénat, 2014) spent on foreign intelligence altogether (these numbers includes, for instance, costs for HUMINT missions, which do not form part of the NSA's mission). Both services are obliged to release information over their spending, albeit the allocation of the BND's funds remains fully classified, whereas the French Senate's DGSE financial report merely breaks down the budget into staff related and operative costs. The biggest spender within the EU remains to be Britain's GCHQ. The budget of the agency is said to be set at around $1.6 billion (Shipman, 2014), which is the lion's share of the $3.3 billion heavy Single Intelligence Account (SIA) also used for funding the MI5 and MI6. In conclusion, even assuming that the BND and DGSE would invest their respective annual budgets exclusively in SIGINT related tasks (which they do not), the combined budget of the secret services of the three major economies in the EU would as of 2013 still only make up about 30 per cent of that of the NSA (while those countries' combined BIP is roughly 55% of that of the US).

NATO COOPERATION VS EU INTEGRATION

A compelling way of overcoming financial and logistical impasses on the national level of course is the pooling of resources. In post WWII times, for the European states, two options for collaboration in security matters emerged.

The first choice, the NATO, quickly established itself as the leading coalition for military collaboration in Europe, which only appears natural given the important role that its

member state USA played in terms of guaranteeing the independence of its Western European allies vis-à-vis the Soviet Union. The second option, military integration solely within the community of Western European states at first did not materialize. Initiatives to create a joint European army existed especially within the early days of the Western European Union (WEU), however, these efforts faded off over time as European federalists struggled to overcome the resistance of intergovernmental forces who insisted that security should remain within the control of the national executive authorities. This attitude only began to change very slowly, but following massive EU enlargement finally manifested itself in the creation of the European Defence Agency (EDA, since 2004) as well as the EU Battlegroup (since 2007) under the CSDP. Regardless of this concession, the right to national self-determination in the area of defence and security remains firmly enshrined in Article 4, Paragraph 2 of the Lisbon Treaty, thus giving states the possibility to opt out of the EU's CSDP entirely. A look into the past, which reveals how differently the EU member states have positioned themselves in the face of mayor military conflicts such as the 2003 Iraq War and the 2011 Libya intervention show why the outlook for a standing European army is so uncertain. This, together with the fact that NATO has proved successful to fulfil its principal purpose of securing the independence and safety of the European state community against external threats today leaves a rather marginal role to the various CSDP bodies when compared to their transatlantic counterparts. A withdrawal of the UK from the CSDP, which is currently being reviewed, would most likely further jeopardize EU integration in the realm of military security.

The future of military collaboration has serious implications for the way signals intelligence is shared in the future. The emergence of irregular warfare tactics such as guerrilla warfare and terrorism, which are often financed through clandestine means such as money laundering and drug trafficking have blurred the lines of what is military and non-military intelligence and of what is an internal or external threat. Accordingly, SIGINT collection and sharing can, depending on the exact circumstances (e.g. time, location and cause of a threat), occur through both military and civil organs and be either unilateral, bilateral or multilateral in nature. It is exactly in this crucial area that the EDA has not been mandated with any capabilities. As can be derived from the official EDA fact sheet: "So far no Member State has indicated a willingness to pursue ISR [Intelligence, Surveillance and Reconnaissance] related Pooling & Sharing initiatives in the EDA framework. EDA is

prepared to continue to work on the capability, but substantive progress on fulfilling this key requirement will require commitment by Member States and the availability of a Lead Nation".

The same is not true for NATO, which has established itself as an important forum for SIGINT, HUMINT and IMINT (image intelligence; intelligence collected through satellite imagery) exchange in which the US takes a leading role. This leading role can be dated back to Cold War times, when intelligence gathering became of paramount importance for learning about the intentions as well as the military and particularly nuclear warfare capabilities of the enemy. Although the dependence resulting from reliance on vastly US governed intelligence sharing were recognized by the EU member states, only few attempts were made to actually bring about change and were then mostly limited to unilateral and bilateral IMINT programs by Germany, France, Spain and Italy (Villadsen, 2008).

THE CIVIL DIMENSION

The dependence on the US, however, cannot only be felt in the military but also in the civil realm. Cooperation in intelligence matters amongst EU member countries is rare and is for the most part limited to bilateral agreements. The EU intelligence agency IntCen shows to be a rather half-hearted attempt of multilateral cooperation judging by the privileges it has been granted and the disappointing results the agency appears to have yielded as a consequence.

It is not unlikely that such intra-EU intelligence efforts are actually deemed redundant by the member states due to the existence not only of the NATO but also the "Five Eyes", which originally constituted a coalition of secret services of five Anglophone countries, namely the USA, the UK, Australia, Canada and New Zealand. The Five Eyes grew from the UKUSA agreement forged between Britain and the US during WWII. The first major SIGINT project under the UKUSA agreement was ECHELON, a satellite surveillance program which initially was destined to spy on the Warsaw Pact before becoming upgraded to a global surveillance program. With the emergence of the internet as a means of mass communication, new programs such as the already mentioned BLARNEY, OAKSTAR, FAIRVIEW, STORMBREW and PRISM were developed; Britain's GCHQ in close collaboration with the NSA contributed its own wiretapping program "Tempora".

In addition to the five core members, the Five Eyes also have European and other Western third-party members, which run their own respective programs and aid the NSA in carrying out surveillance abroad. The group of European intelligence partners again are

divided in the “Nine Eyes”, consisting of the core members plus Denmark, France, the Netherlands and Norway on the one hand and the “Fourteen eyes”, consisting of the “Nine Eyes” plus Germany, Belgium, Italy, Spain and Sweden on the other hand. The Fourteen Eyes moreover are called “SIGINT Seniors Europe” (SSEUR) for official purposes and as of 2014 constitute the biggest community of SIGINT collectors worldwide. It is not exactly known in how far the collaboration between the different layers varies, but the GCHQ is said to have a huge saying in which other European services are allowed into the inner circle of the “Nine Eyes”, which reportedly gave France’s DGSE the edge over Germany’s BND (MacAskill & Ball, Portrait of the NSA: no detail too small in quest for total surveillance, 2013).

Possibly due to simultaneous NATO collaboration, the SSEUR in the past have been wrongly perceived as an intelligence alliance by some of the third-party members, judging by the reactions amid 2013 reports of NSA spying on EU government leaders. However, UKUSA does not entail a formal provision that would prohibit or even condemn mutual espionage or surveillance even amongst the core members. Both former and current US officials therefore were quick to dismiss the European public outrage over espionage on EU member government leaders as a case of double standards, saying that the affected nations’ secret services were reciprocally targeting the US. Although there have been reports about an existing commitment by the Anglophone governments not to spy on each other’s government organs, this measure apparently merely constitutes a gentlemen’s agreement rather than binding legislation.

Irrespective of this diplomatically rather distanced approach that the core members seem to pursue especially vis-à-vis the third-party members, there is no lack of incentives particularly on part of the NSA to retain this form of loose collaboration. Aside from the direct and indirect financial benefits provided through the agency, political observers also assume the existence of strong technological support that goes beyond the aforementioned compensation for underdeveloped SIGINT infrastructure on part of the EU member states. In this regard, particularly voices from within Germany’s BND have admonished that the European countries heavily depend on the US in terms of SIGINT data analysis (SPIEGEL, 2013). What is more, while the data collection methods deployed by intelligence services in countries like France, Sweden and Germany are similarly advanced in the sense that they can process a high bandwidth of data, unlike the US and the UK, the aforementioned states find it difficult to exploit collected information due to limitations in the area of deciphering encrypted data (López, 2013).

INTERNATIONAL AND EUROPEAN LAW REGARDING MASS SURVEILLANCE

Because this research is addressing and challenging the legitimacy of acts carried by government, these should also be looked at from the point of view of international law. In the case of mass surveillance this means taking a closer look at International Human Rights Law (IHRL) as a guideline for what is permissible for non-European states and additionally the European Convention on Human Rights for the respective European signatories.

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) lays down that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation” (Office of the High Commissioner for Human Rights, 1976).

Firstly, a major issue lies in defining what constitutes an “arbitrary” or “unlawful” interference. Even the word “interference” can be interpreted quite differently. The American Civil Liberties Union (ACLU) criticizes this legal uncertainty and admonishes that the General Comment to Article 17 ICCPR does not take into account the developments in IT during the past decades.

With regards to the definition of the word “unlawful”, “General Comment 16 makes clear at [3] that the prohibition on unlawful interference means that interference can only occur ‘on the basis of law.’ However, that law must also be consistent with ‘the provisions, aims and objectives of the Covenant.’” Since this provision is intended as a “measure of legal protection against the possibility of interference through executive acts and discretion”, US mass surveillance which is carried out through executive order and therefore bypasses approval by the Foreign Intelligence Court may indeed qualify as unlawful (American Civil Liberties Union, 2014). Furthermore, the ACLU argues with regards to “arbitrary” interference, that surveillance law must pass a proportionality test. Case law shows that European courts in the past have ruled quite strictly when evaluating the proportionality of data collection law. As already stated in the introduction, the ECJ sacked the EU’s Data Retention Directive, which required EU telecommunications providers to retain call detail records of all of their customers. The court held that such action was not proportional given the resulting interference to the right to privacy, Article 8 ECHR. Given the ECJ’s ruling it is very unlikely that the US mass surveillance programs, particularly PRISM would be considered “lawful” at least from a European view of Human Rights Law.

Lastly though, even if mass surveillance programs meet the definition of what is unlawful and arbitrary interference, there remains one last issue which concerns the

applicability of HRL. Since it believes that the obligations derived from the covenant have to be interpreted as strictly territorial, the US judiciary e.g. does not consider mass surveillance to be in breach of Article 17 of the ICCPR as long as the offending state does not exert effective control over an affected territory (Schaack, 2014, pp. 54-55).

This understanding of the applicability of human rights law is in stark contrast to the opinion of various international human rights courts and expert bodies, who argue that this would contravene the objectives of the Convenant (Schaack, 2014, pp. 61-62). Given the fact that many other states in the world have foreign mass surveillance programs of their own, it is unlikely that the US's position will be challenged.

INTERNATIONAL AND EUROPEAN LAW REGARDING ESPIONAGE

The legal situation regarding espionage is rather simple compared to that of mass surveillance. Simply put, International Public Law does not prohibit foreign governments to spy on EU member states. "Unlike [for] espionage in times of war, public international law does not contain any specific rules with respect to espionage in times of peace". As an effect, peace time espionage falls under the "Lotus Principle", which holds that a state by virtue of being sovereign, can "engage in any activities that are not expressly prohibited by international law" (Talmon, 2013).

EU member states are, however, not only bound by International Public Law but also by EU law, which means that given the existence of support for an intra-EU solution, the member states could outlaw espionage amongst themselves. Since the EU ought to guarantee fair competition, which could be hindered especially by economically motivated espionage, such a regulation would definitely have a raison d'être. As of now though, EU Law has not addressed the issue. Whether this will change on the other hand is uncertain.

In summer 2013 soon after the first reports about NSA spying surfaced, and following rather unsuccessful bilateral talks with US officials, Germany started pushing for a "no-spy" agreement on the EU level that would see the member states obliging themselves to "refrain from mutual espionage" as well as from requesting other EU member states to release data about their own citizens where national law does not allow this. The UK and Sweden strongly opposed the move from the beginning, on the basis that the EU had no saying in intelligence matters. In January, regardless of the opposition, there also seemed to be some level of support for such an agreement. However, in recent times things have become quiet around the incentive (The Local, 2014; End the Lie, 2013).

ANALYSIS

When looking at the data collected, what sticks out is that mass surveillance programs like PRISM, OAKSTAR, STORMBREW, BLARNEY and FAIRVIEW demand an extraordinary technological, logistical, and financial effort. Although all programs but PRISM apparently only collect meta-data, the resulting amount of information stemming from these data collection schemes still appears to be so enormous, that in 2011 the NSA felt compelled to commence construction of a new $1.7 billion data center in Bluffdale, Utah, capable of storing 20 terabytes of data per minute (for scale: this amounts to roughly 83.3% of the peak traffic of the world's biggest internet exchange DE-CIX) (Caroll, 2013). In order to gain access to these huge amounts of data, the US requires access to major internet exchange points, in the US and elsewhere in the world.

Since these exchange points are the property of major enterprises, who out of economic self-interest would rather not disclose the personal information of clients to government organisations, the logistical challenge lies in compelling these internet service providers to comply or even deliberately collaborate with the NSA. Even more persuasion is likely necessary to enforce compliance from firms targeted by the downstream program PRISM. Since the user content gathered through this one program is perceived as far more intimate as the meta-data gathered by the upstream collection programs (albeit whether this is true is debatable) the damage to the image of complying companies in the public eye is far bigger.

These technological and logistical efforts come at a cost. It is unfortunately not possible to break down the NSA's budget into its individual assets, so that the exact costs of the wiretapping programs cannot be determined. It should moreover not be ignored that the NSA also fulfils defensive security tasks such as advising US companies in data security matters and developing encryption standards, which take their share of the agency's budget. Even taking this into account though, it should not prove to be too keen a claim that much of the $10.8 billion NSA budget are indeed spent on the running and development of surveillance programs.

Yet, all this alone does not yet explain why as of 2014 the only name appearing in Western media in relation to mass surveillance appears to be that of the NSA. After all, the data suggests that Russia e.g. has developed the SORM programs that appear to work

hugely similar to US surveillance schemes. The existence of comparable surveillance programs in China, be they domestic or foreign, can neither be confirmed nor ruled out with the data available. What speaks in favour of such a theory though is that China has a strong IT infrastructure that would allow it to break common encryption standards relatively easy. In Tianhe-2, which clocks at 33.86 petaflop/s, China possesses the world's fastest supercomputer, and 76 of the 500 world's fastest systems are hosted by the East Asian superpower. Tianhe-2 was installed at the National University of Defense Technology campus and therefore the usage of such facilities for intelligence purposes while still unproven is at least suggested (Knapp, 2014). What speaks against the usage of dragnet surveillance in foreign countries by either Russia's or China's intelligence agents in the relative use this would have either regime. The purpose of such programs after all, be it in a democratic or despotic system, is to provide inner safety against external threats and thus establish the control of the incumbent party. However, a program that would search for threats to the incumbent party rule in the exterior when actually resistance mostly forms domestically would prove useless. The biggest threats to Russia's and China's regimes are nationalist and religious separatist movements in annexed regions as well as political and ideological movements which demand more accountability from the political elites. In Russia such movements can be found in a number of regions such as Chechnya, Dagestan, Tatarstan, Tuva, Bashkortostan, Sakha, Kaliningrad and Primorsky (Kravtsova, 2014). China faces similarly challenging cases of regional instability in Xinjiang, Tibet, Inner Mongolia, and Taiwan (Davis, 2008). Even domestically, China appears to pursue a different route than state governed mass surveillance. Instead of controlling the national data flow through the nation's various internet exchange points, as is the case in Russia, the Chinese People's Party rather coerces enterprise to engage in self-censorship and blocks access to foreign internet forums and services. The effort to survey subversive elements is consequently reduced to a minimum, due to the chilling effects of an ever perceived feeling of observation amongst Chinese internet users.

In the US on the other hand most threats are perceived as coming from outside, and the country nowadays goes to great lengths to reveal these external threats. The mass surveillance programs therefore do not only serve the purpose of observing known suspects, they are also supposed to identify threats that have not yet been unveiled by other means. Indeed, after Western intelligence services collectively failed to prevent the September 11th attacks in New York, which were carried out by terrorists, who for a long time even lived in

and prepared their attacks within different NATO states, this task has become a centre of attention for the NSA.

The conditions for creating mass surveillance programs in the US are ideal. The country hosts major and globally popular internet giants such as Microsoft, Yahoo, Google and Facebook. What is more, since operating such services requires high bandwidth, the country always put a focus on expanding its internet infrastructure. No other region in the world can transfer anywhere as much data, which makes the USA a global data hub and thus through the NSA's upstream programs gives the secret services easy access to information which is not even destined to be sent there. In some cases, however, access through the domestic grid is not possible. The US therefore also delegates certain surveillance tasks to members of the Five Eyes and the SSEUR. This mounted speculation that UKUSA was also used to circumvent limits to domestic surveillance. The German magazine SPIEGEL with reference to Snowden documents declared: "And it appears that the principle that foreign intelligence agencies do not monitor the citizens of their own country, or that they only do so on the basis of individual court decisions, is obsolete in this world of globalized communication and surveillance. Britain's GCHQ intelligence agency can spy on anyone but British nationals, the NSA can conduct surveillance on anyone but Americans, and Germany's BND foreign intelligence agency can spy on anyone but Germans. That's how a matrix is created of boundless surveillance in which each partner aids in a division of roles" (Poitras, Rosenbach, Schmid, Holger, & Stock, 2013).

Especially where partners of the NSA cease to be cooperative, however, the US do not seem to refrain from using clandestine means even against military allies. Germany's BND e.g. from 2004 to 2007 forwarded data it collected from DE-CIX directly to the NASA. The collaboration was, however, terminated when officials in Germany expressed reservations regarding the legality of the program. This would normally suggest that the NSA should not be receiving any more data out of Germany. Indeed, according to German media reports the NSA and the GCHQ have since established backdoor access to the networks of internet service providers "Deutsche Telekom" and "Netcologne" as well as German satellite teleport operators Stellar, Cetel and IABG. "Because Netcologne is a regional provider, it would seem highly likely that the NSA or one of its Treasure Map partners accessed the network from within Germany. That would be a clear violation of German law and potentially another NSA-related case for German public prosecutors" (Müller-Maguhn, Poitras, Rosenbach, Sontheimer, & Grothoff, 2014).

In summary, a country would have to qualify for multiple conditions in order to be considered a threat to information privacy in Europe. Firstly, from a technical point of view it would require an excellent data link with Europe in order to be able to transfer high loads of bandwidth as well as technical gear and qualified staff to constantly decrypt, process, analyse, and store data. Moreover, logistically, to gain access to data which it cannot intercept domestically, a foreign government would need either government or private partners to get access to key foreign internet exchange points or would alternatively have to infiltrate those key points through hard- or software backdoors. Thirdly, a country would need to be both capable and willing to make high annual investments to run its mass surveillance programs. Lastly, the government of such a country would risk to sacrifice established diplomatic and economic ties with infiltrated EU countries for giving inner safety a higher priority.

The infrastructure used for mass surveillance programs, however, cannot only be deployed for finding terrorists and drug traffickers, it can also be a door opener for espionage. One of these espionage programs, which make use of the same infrastructure as the NSA's anti-terror schemes is BLARNEY. As one of the oldest NSA surveillance programs, in recent times it was used to spy on the communications of high level government leaders such as German Chancellor Merkel as well as various other heads of government in Eastern Europe. The 2013 SPIEGEL data about BLARNEY furthermore mentions that access to the Chancellor's communication data was established through a US communications provider whose name remained undisclosed within the official NSA documents. British and US telecommunications providers generally seem to exhibit a strong interest in foreign countries' political organs. For instance, from 2005 on the German lower house, the "Bundestag", contracted Verizon as its communications provider and the "Abgeordnetenhaus von Berlin", which is the state parliament of the federal state of Berlin contracted City of London Telecommunications for its services (Meister, 2014). Whether this was a good idea remains questionable. The collaboration of Verizon with US secret services at least today is well documented (Greenwald, NSA collecting phone records of millions of Verizon customers daily, 2013); similar reports about an incorporation of British telecommunications providers in GCHQ's "Tempora" program exist as well (Ball, Luke, & Garside, 2013). The German Interior Ministry meanwhile announced that German government had decided to terminate the collaboration with Verizon, openly stating that the ties between US communication

companies and US government formed part of the decision (Bundesministerium des Innern, 2014).

There is also evidence that the US uses its surveillance program for economic espionage, such as the report of NSA spying on Brazilian oil giant Petrobras (Watts, 2013). As another example, in an interview with German media, when asked about the purpose of the NSA's upstream programs, whistle-blower Edward Snowden stated: "If there's information at Siemens that's beneficial to U.S. national interests - even if it doesn't have anything to do with national security - then they'll take that information nevertheless" (Kirschbaum, 2014). US economic espionage became a major topic for the EU for the first time as early as 2001. At the time the NSA was using the espionage program ECHELON to eavesdrop on an EADS trade mission in Saudi-Arabia. James Woolsey, a former CIA boss later confirmed that the eavesdropping had taken place, however, justified the act as an attempt to counter the threat of "EU companies indulging in bribery to obtain contracts" (Schmid, 2001). Regardless, whether such allegations regarding bribery by EU enterprise are true or not, US economic espionage may have severe consequences for the EU economy. EADS for instance is in direct competition with US counterparts such as Boeing, Lockheed-Martin and others. Losing a single contract to a competitor in the aerospace industry due to loss of trade secrets can easily result damages worth multiple billion Euros.

Especially economic espionage, however, can also occur without the existence of sophisticated surveillance networks. Especially the emerging BRIC nations, amongst them particularly Russia and China pose a threat to the European economy. Other than the USA, these countries' industries have to compensate a technological backlog and thus are above all interested in technological blueprints and patents rather than trade secrets. As the data shows, they can gain access to this valuable information through technically quite simple measures such as Spear-Fishing attacks. These penetrate the IT infrastructure of governments and enterprise by sending disguised malicious links to staff in key positions - such as network administrators, higher management staff or even CEOs. Preventing these attacks is difficult to manage on a policy level since they exploit the human factor. Even though the European Commission estimates that one in five companies in the EU has become subject to industrial espionage at least once during the past ten years (Barker, 2013), especially small and medium-sized enterprises (SME) in Europe underestimate the risk of economic espionage and often do not take appropriate steps against it.

The EU meanwhile made first attempts to improve the situation around data security in Europe. Although they only tackle the issues of mass surveillance and espionage indirectly, the EU Cyber Strategy and the recently updated Data Protection Regulation could prove to be useful tools against the acts. Through ENISA and the various national data security agencies, the public and private sector in the EU will for the first time closely work on improvements to data security conjointly, by requiring enterprise to report cyber-attacks to competent authorities. By sharing collected information about security breaches across European boarders the data protection authorities could create synergies that ultimate benefit all member states.

Another legislative tool, the March 2014 Data Protection Regulation can be considered a U-turn away from the EU-US Safe-Harbour agreement, which was suspended by the EU Parliament the same month. The Safe-Harbour agreement was an EU decision, which aimed to obligate US enterprise to comply with EU Directive 95/46/EC on the protection of personal data. US companies could simply certify themselves compliant with the directive, and thus more stringent data protection rules by signing up to a list of the US Department of Commerce. The EU Commission in return acknowledged compliance with Directive 95/46/EC, without applying further tests whether that was indeed the case. The independent auditing firm “galexia” who probed the integrity of the decision issued massive criticism. For instance, while the companies had the possibility to let an external auditing firm check for the company’s compliance with the Safe Harbour Principles, this option, although more reputable was mostly not utilised. Beyond that, companies made false claims about the decision, stating that they were certified by the EU Commission or US Department of Commerce. Others (overall 206 companies until 2008) went as far as claiming to be certified without ever having gone through the process of self-certification. Beyond that, even such companies compliant with the directive did not protect all data in a similar manner, but only apply the highest level of protection to particular data types. (5.1. False claims regarding membership, 2008; 5.2. False claims regarding certification, 2008; 5.9. Categories of data protected, 2008). After PRISM became known to the public, the Safe-Harbour agreement finally lost all political support, because it became evident that the NSA coerced US companies to release data of European citizens, thus making them infringe on European data protection law.

The new Data Protection Regulation goes different ways. All companies doing business in the EU, be they foreign or domestic are now automatically and directly

accountable to the Data Protection Authority. Big business has to designate a Data Protection Officer in order to be able to quickly respond to privacy concerns. What should prove most useful are the sanctions that the EU can now impose for non-compliance against foreign companies. After all, the US administration, for instance successfully enforces compliance by domestic companies through a mix of financial repercussions and incentives as well.

International Law on the other is unlikely to play a major part in preventing mass surveillance in Europe. Firstly, this is because IHRL was created during the 1970s when cloud computing, social media and e-commerce were not even thought of, yet, and hence does not deliver a clear answer as to under which exact circumstances mass surveillance becomes arbitrary and unlawful. The most crucial reason though lies in the fact that EU member states (and especially those with ties to UKUSA) survey the internet connections of citizens of foreign states in bulk themselves. Advocating for clearer or extraterritorial applicability of Article 17 ICCPR will thus likely not be on the agenda of most EU member state governments since it runs contrary to their own agenda.

The situation is even clearer when it comes to espionage and IPL. As long as espionage remains the sovereign right of states there is no legal remedy against foreign secret services, with the exception of national anti-espionage laws, which however scrutinize acts of individuals and not states. The exception to this rule is espionage amongst EU member state governments. The UK, in supporting and running programs like ECHELON, BLARNEY and Tempora could be in violation of EU law depending on the country's role in these spying endeavours. An EU parliamentary report on ECHELON found that: "if, on the other hand, the system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member Statesí duty of loyalty and with the concept of a common market based on free competition, so that a Member State participating in such a system violates EC law" (Schmid, 2001). In combination with financial repercussions for non-compliance, a formal agreement or law to combat government sponsored espionage within the EU could have chilling effects states' deliberation to carry out economic espionage.

CONCLUSION

The EU is facing a wealth of different issues in regards to ensuring data protection within the member states. Many of these problems correlate with the close collaboration of EU member states' secret services within the NATO and the UKUSA community. In essence,

experience has shown that the Five Eyes do not respect European privacy and data protection laws. Especially since the terror attacks of September 11th 2001, which caused the creation of US legislation such as the “Patriot Act”, the data of European citizens is collected through arbitrary mass surveillance programs which are merely legitimized through presidential executive order and both NSA and GSHQ appear to access the networks of companies and government agencies at will. Being dependent on US SIGINT competence was acceptable while it appeared that the targets of European and US in terms of SIGINT collection were perfectly aligned in a common goal to combat terrorist and other external threats. Now however that it became clear that the US have objectives that do not match with European states’ self-interests, the EU member states should draw the right conclusions and intensify inner European intelligence collaboration.

This does not mean that the member states should give up on their national secret services, but rather that, like in other areas of competence of the EU, they should consider to pool their financial resources and supplement the national services with a supranational EU body which is capable of carrying out SIGINT operations in areas where European interests align, but where the US proves to be a rival rather than a partner. In other words, the EU should carry out joint counter-espionage. The first mismatch of US and EU interests affects trade secrets. Because European and US American companies are in direct competition, it is tempting for the administration of each side to gain the upper hand through clandestine means. The second mismatch consists in the protection of government secrets, which are a fundamental condition for the sovereignty of the EU as well as the EU member states. Of course espionage threats also originate from other parts of the word such as the BRIC states, but the lesson that has to be learned from the Snowden revelations is that a military alliance does not protect against the strive for dominance of a superpower like the US.

In order to provide this, the member states will need to allow the EU to extend its privileges in the area of safety and security. Through the Common Foreign and Security Policy (CFSP) they have already created a basis for stronger collaboration. Moreover, through IntCen the EU already possesses a minuscule intelligence body, which when equipped with the appropriate resources could bring about greater independence from the Five Eyes in regards to SIGINT collection. Some nations which are strongly rooted within the UKUSA community would likely oppose such plans. This however can be handled through opt-out agreements, as is already the case today with the EU monetary union and the CSDP.

A particular vulnerable spot in the defence of privacy rights are the US enterprises which collect personal data of European citizens. The issue of comparatively lower data protection standards in the US has been tackled through the Data Protection Regulation, which forces US enterprise to comply with and report on the implementation of European data safety standards. However, the problem remains that these companies are legally obliged to cooperate with the US secret services, which is subsequently enforced through both FISA Court orders as well as financial penalties. As the example of Yahoo shows the US administration does not even refrain from imposing fines of an amount that could threaten the existence of its domestic tech companies. Therefore it remains to be seen whether the EU's own penal system for non-compliance with EU privacy law will deter US tech companies from handing over personal data of European citizens. If, however, the financial damage resulting from proceedings and lost revenue due to loss of trust (see Verizon losing its contract with the German Bundestag) would be big enough, it could stir public debate in the US away from the NSA's domestic wiretapping to its operations abroad and ideally lead to stricter data collection regulations for US secret services.

Change should also be promoted regarding the technological and infrastructural backlog vis-à-vis more advanced regions. Firstly, the EU should expand its bandwidth capacities with the BRIC states in order to exacerbate the collection of EU upstream data. Secondly, the EU should provide financial incentives for the development of services and products which can ultimately improve data security, such as domestically produced encryption software, networking gear and operating systems. Because of the growing significance of social media and cloud computing, the EU should also support the creation of European services which could offer an alternative to popular US services.

Lastly, perfect security from espionage and surveillance is not a realistic target for any nation, but the EU member states' aspiration should at least be to level the playing field with the Five Eyes, Russia and China within the years to come. In terms of guaranteeing national security, the current intelligence exchange system provided through UKUSA and NATO already seems to offer everything the states could hope for, which shows not only in the member states reluctance to further integrate on the safety and security level of the EU, but e.g. also in the number of terrorist attacks that have been prevented in the past (SPIEGEL, 2013). It must however also be pointed out that even if the collection signals intelligence is an important factor for ensuring inner safety, it should be every constitutional democratic state's guiding principle not to collect or require allied states to collect information

in a way that gravely interferes with the lives of its citizens and also to remain independent vis-à-vis other states for the sake of remaining capable of acting in this manner. The EU member states have so far failed to guarantee this each on their own.

REFERENCES

50 U.S. Code § 1801 - Definitions. (2008). Retrieved June 8, 2014, from Cornell University Law School web page: http://www.law.cornell.edu/uscode/text/50/1801

50 U.S. Code § 1802 - Electronic surveillance authorization without court order. (2008). Retrieved June 8, 2014, from Cornell University Law School web page: http://www.law.cornell.edu/uscode/text/50/1802

50 U.S. Code § 1805 - Issuance of order. (2008). Retrieved June 8, 2014, from Cornell University Law School web page: http://www.law.cornell.edu/uscode/text/50/1805

50 U.S. Code § 1811 - Authorization during time of war. (2008). Retrieved June 8, 2014, from Cornell University Law School web page: http://www.law.cornell.edu/uscode/text/50/1811

BBC. (2012, October 8). *Huawei and ZTE pose security threat, warns US panel*. Retrieved June 13, 2014, from BBC web page: http://www.bbc.com/news/business-19867399

BBC. (2014, May 19). *Cisco calls for curb on NSA surveillance efforts*. Retrieved June 13, 2014, from BBC web page: http://www.bbc.com/news/technology-27468794

Blyth, K. (2013, June 17). *PRISM and SORM: Big Brother is watching*. Retrieved June 11, 2014, from The Moscow News web page: http://themoscownews.com/russia/20130617/191621273-print/PRISM-and-SORM-Big-Brother-is-watching.html

Bohm, M. (2013, August 30). *Spying Is a Sovereign Right*. Retrieved June 11, 2014, from The Moscow Times web page: http://www.themoscowtimes.com/opinion/article/spying-is-a-sovereign-right/485257.html

Connolly, K. (2009, July 22). *Germany accuses China of industrial espionage*. Retrieved June 13, 2014, from The Guardian web page: http://www.theguardian.com/world/2009/jul/22/germany-china-industrial-espionage

Cox, J. (2012, December). *Canada and the Five Eyes Intelligence Community.* Retrieved June 13, 2014, from Canadian Defence & Foreign Affairs Institute web page:

http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf

Cross-border Research Association. (n.d.). *CBRA analysis of EU Situation Centre.* Retrieved June 13, 2014, from FOCUS Project web page: http://www.focusproject.eu/documents/14976/0/CBRA+analysis+of+EU+Situation+Centre

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013, February 7). Retrieved June 10, 2014, from European Commission web page: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Emmott, R. (2014, February 24). *Brazil, Europe plan undersea cable to skirt U.S. spying.* Retrieved June 20, 2014, from Reuters web page: http://www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224

End the Lie. (2013, July 6). *Britain and Sweden block critical talks on espionage and intelligence between EU and US*. Retrieved July 13, 2014, from End the Lie: http://endthelie.com/2013/07/05/britain-and-sweden-block-critical-talks-on-espionage-and-intelligence-between-eu-and-us/

EU Commission. (2013, July 16). *Criminal law policy*. Retrieved June 10, 2014, from EU Commission web page: http://ec.europa.eu/justice/criminal/criminal-law-policy/index_en.htm

European Court of Justice. (2014, April 8). *The Court of Justice declares the Data Retention Directive to be invalid.* Retrieved June 12, 2014, from ECJ web page: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

European External Action Service. (2012, June 18). *EU Intelligence Analysis Centre (EU INTCEN) Fact Sheet.* Retrieved June 12, 2014, from Ask the EU web page: http://www.asktheeu.org:8080/de/request/637/response/2416/attach/html/5/EU%20INTCEN%20Factsheet%20PUBLIC%20120618%201.pdf.html

Farivar, C. (2013, October 21). *France angered by new revelations of NSA surveillance.* Retrieved May 29, 2014, from Ars Technica web page: http://arstechnica.com/tech-policy/2013/10/quelle-surprise-new-snowden-docs-show-nsa-targets-france-too/

Frederix, D. F. (2014, May 19). Towards an integrated EU ICT security policy. (M. Schulze, Interviewer)

galexia. (2008). *5.1. False claims regarding membership*. Retrieved June 12, 2014, from galexia web page:

http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction-5_1_.html

galexia. (2008). *5.2. False claims regarding certification*. Retrieved June 18, 2014, from galexia web page: 5.2. False claims regarding certification

galexia. (2008). *5.9. Categories of data protected*. Retrieved June 18, 2014, from galexia: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction-5_9_.html

Greenwald, G. (2013, June 6). *NSA collecting phone records of millions of Verizon customers daily.* Retrieved June 13, 2014, from The Guardian web page: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G. (2013, July 7). *The NSA's mass and indiscriminate spying on Brazilians*. Retrieved June 13, 2014, from The Guardian web page: http://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying

Hall, M. (2013, February 8). *Storm cloud emerges from EU cybersecurity strategy*. Retrieved June 3, 2014, from EurActiv web page: http://www.euractiv.com/infosociety/stormcloud-emerges-cloud-safety-news-517658

Heil, E. (2013, October 22). *What's the deal with NSA's operation names?* Retrieved June 8, 2014, from Washington Post web page: http://www.washingtonpost.com/blogs/in-the-loop/wp/2013/10/22/whats-the-deal-with-nsas-operation-names/

Herman, M. (1996). *Intelligence Power in Peace and War.* Cambridge: Royal Institute of International Affairs.

Hopkins, N., & Boger, J. (2013, August 1). *Exclusive: NSA pays £100m in secret funding for GCHQ*. Retrieved June 13, 2014, from The Guardian web page: http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

Jopson, B., Hornby, L., & Clover, C. (2014, March 23). *NSA accused of breaching networks run by China's Huawei*. Retrieved June 18, 2014, from Financial Times web page: http://www.ft.com/intl/cms/s/0/beb9f242-b26f-11e3-b891-00144feabdc0.html#axzz3596A1L00

Kirschbaum, E. (2014, January 26). *Snowden says NSA engages in industrial espionage: TV*. Retrieved June 17, 2014, from Reuters web page: http://www.reuters.com/article/2014/01/26/us-security-snowden-germany-idUSBREA0P0DE20140126

López, A. (2013, November 4). *European agencies, NSA collaborate on mass spying against European population*. Retrieved June 10, 2014, from World Socialist Web Site: https://www.wsws.org/en/articles/2013/11/04/eusp-n04.html

MacAskill, E. (2013, August 23). *NSA paid millions to cover Prism compliance costs for tech companies.* Retrieved June 13, 2014, from The Guardian web page: http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). *GCHQ taps fibre-optic cables for secret access to world's communications.* Retrieved June 13, 2014, from The Guardian web page: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Markoff, J. (2008, August 29). *Internet Traffic Begins to Bypass the U.S.* Retrieved June 13, 2014, from NY Times web page: http://www.nytimes.com/2008/08/30/business/30pipes.html?pagewanted=all&_r=1&

NISO. (2001). *Understanding Metadata.* Retrieved May 29, 2014, from NISO web page: http://www.niso.org/publications/press/UnderstandingMetadata.pdf

Nolan, S. (2013, June 8). *Revealed: Google and Facebook DID allow NSA access to data and were in talks to set up 'spying rooms' despite denials by Zuckerberg and Page over PRISM project.* Retrieved June 13, 2014, from Daily Mail web page: http://www.dailymail.co.uk/news/article-2337863/PRISM-Google-Facebook-DID-allow-NSA-access-data-talks-set-spying-rooms-despite-denials-Zuckerberg-Page-controversial-project.html

Norton-Taylor, R. (2010, June 25). *Not so secret: deal at the heart of UK-US intelligence*. Retrieved June 13, 2014, from The Guardian web page: http://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released

Office of the High Commissioner for Human Rights. (1976). *International Covenant on Civil and Political Rights.* New York.

Pelican, L. (2012). *PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT NECESSARY GAME.* Washington, D.C: Journal of Communications Law.

Perloth, N., Larson, J., & Shane, S. (2013, September 5). *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*. Retrieved June 16, 2014, from NY Times web page: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=1&

Perlroth, N. (2014, June 9). *2nd China Army Unit Implicated in Online Spying*. Retrieved June 15, 2014, from NY Times web page: http://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html

Protection of individuals with regard to the processing of personal data. (2014, March 12). Retrieved June 10, 2014, from European Parliament web page: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN

Richelson, J. (2005, March 11). *The National Security Agency Declassified*. Retrieved May 25, 2014, from The National Security Archieve: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/

Rushe, D. (2013, June 8). *Facebook and Google insist they did not know of Prism surveillance program.* Retrieved June 13, 2014, from The Guardian web page: http://www.theguardian.com/world/2013/jun/07/google-facebook-prism-surveillance-program

Sanger, D., Barboza, D., & Perloth, N. (2013, February 18). *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.* Retrieved June 15, 2014, from NY Times web page: http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

Schaack, B. V. (2014). *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change.* U.S. Naval War College, Newport. Retrieved June 10, 2014, from https://www.usnwc.edu/getattachment/a88e97e5-11ec-4dfb-a013-4cfa5f8efe5a/The-United-States--Position-on-the-Extraterritoria.aspx

Schmid, G. (2001, September 5). *Echelon spy system*. Retrieved June 11, 2014, from EU Parliament web page: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+PRESS+DN-20010905-1+0+DOC+XML+V0//EN#SECTION1

SIGINT Activity Designators (SIGADs). (2014, May 19). Retrieved May 25, 2014, from electrospaces.net: http://electrospaces.blogspot.de/p/sigint.html

Slides about NSA's Upstream collection. (2014, May 20). Retrieved May 25, 2014, from electrospaces.net: http://electrospaces.blogspot.de/2014/01/slides-about-nsas-upstream-collection.html

SPIEGEL. (2007, August 27). *Espionage Report: Merkel's China Visit Marred by Hacking Allegations*. Retrieved June 10, 2014, from SPIEGEL web page: http://www.spiegel.de/international/world/espionage-report-merkel-s-china-visit-marred-by-hacking-allegations-a-502169.html

SPIEGEL. (2013, August 26). *Codename 'Apalachee': How America Spies on Europe and the UN*. Retrieved June 10, 2013, from Der Spiegel web page: http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

SPIEGEL. (2013, November 4). *Codependent: Merkel's Pragmatic Approach to the NSA Scandal*. Retrieved June 10, 2014, from SPIEGEL web page: http://www.spiegel.de/international/world/nsa-scandal-berlin-restricted-by-close-relationship-with-us-intelligence-a-931503.html

SPIEGEL. (2013, July 22). *'Key Partners': Secret Links Between Germany and the NSA.* Retrieved June 13, 2014, from Der Spiegel web page: http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html

Strange, H. (2013, June 20). *Angela Merkel refers to internet as 'virgin territory'*. Retrieved May 25, 2014, from The Telegraph web page: http://www.telegraph.co.uk/news/worldnews/europe/germany/10133039/Angela-Merkel-refers-to-internet-as-virgin-territory.html

Stratfor. (2011, November 11). *RUSSIA/CHINA/US - US report on Chinese, Russian "cyberespionage" pondered*. Retrieved June 13, 2014, from Wikileaks: http://wikileaks.org/gifiles/docs/74/745426_russia-china-us-us-report-on-chinese-russian-cyberespionage.html

Text of the FISA Amendments Act of 2008. (2008). Retrieved June 8, 2014, from Govtrack.us: https://www.govtrack.us/congress/bills/110/hr6304/text

The Local. (2014, 16 January). *Germany seeks 'no spy' pact among EU members*. Retrieved June 7, 2014, from The Local web page: http://www.thelocal.de/20140116/germany-seeks-eu-no-spy-pact-britain-opposed-nsa-snowden

The Washington Post. (2013, July 10). *NSA slides explain the PRISM data-collection program*. Retrieved June 2, 2014, from The Washington Post web page: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

United States Government. (2012, May 3). *SID Oversight and Compliance*. Retrieved May 25, 2014, from ACLU web page: https://www.aclu.org/files/natsec/nsa/sid_oversight_and_compliance.pdf

US National Security Agency. (2011, April 15). *Mission*. Retrieved June 13, 2014, from NSA web page: http://www.nsa.gov/about/mission/index.shtml

Villadsen, O. (2008, June 27). *Prospects for a European Common Intelligence Policy.* Retrieved June 13, 2014, from CIA web page: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art07.html

Washington Post. (2013, July 10). *NSA slides explain the PRISM data-collection program*. Retrieved May 24, 2014, from Washington Post web page: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Waterfield, B. (2013, November 4). *Brussels demands 'EU intelligence service' to spy on US*. Retrieved June 13, 2014, from The Telegraph web page: http://www.telegraph.co.uk/news/worldnews/europe/eu/10425418/Brussels-demands-EU-intelligence-service-to-spy-on-US.html

Watts, J. (2013, September 9). *NSA accused of spying on Brazilian oil company Petrobras*. Retrieved May 27, 2014, from The Guardian web page: http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

Zawilska-Florczuk, M., & Frymark, K. (2014, January 14). *The NSA: the impact of the wiretapping scandal on German-American relations*. Retrieved June 3, 2014, from OSW web page: http://www.osw.waw.pl/en/publikacje/osw-commentary/2014-01-14/nsa-impact-wiretapping-scandal-german-american-relations

APPENDICES

INTERVIEW

Central question of the dissertation: "Towards an integrated EU ICT security policy: What are the political and technical obstacles of securing the European IT infrastructure against espionage and surveillance and how can they be overcome?"
Date: May 19th, 2014
Location: The interview was conducted via phone
Interviewer: Mario Schulze, European Studies student at the Hague University of Applied Sciences
Interviewee: Dr. Florent Frederix, Directorate-General for Communications Networks, Content and Technology

Q: In recent times there has been a lot of coverage in the media especially about the NSA surveillance program PRISM. Looking back in history however PRISM is not really a novelty. The EU parliament in 2001 published a report about ECHELON, which maybe can be seen as a predecessor to PRISM. Since then, which concrete steps have been taken on the union level in order to prevent a further violation of EU citizen's fundamental rights to privacy as well as damage to the member states' economies?
A: Interviewee declined to give an answer due to only having been with the Commission for ten years

Q: In November 2013 Viviane Reding tabled the idea of creating a European intelligence service in order to level the playing field with the NSA, which was met with a lot of skepticism especially on part of a number of UK politicians.
Firstly, given the strong ties between UK and US intelligence services, is it likely that progress will soon be made in this area?
A: It appears to be unlikely. Theoretically, because of the existence of major intelligence services in Asia and America it would make sense to have such a service in Europe, but it would in any case require the consent of the member states. Beyond that more countries in

the EU than just the UK have reservations about such an idea because of the implications this would have for their own services.

Secondly, will the EU Commission for this purpose seek to have the member states confer more decision-making privileges onto the union in the area of Defense and Security, which is as of now still a field dominated by national legislation?

A: This is difficult to predict since the composition of the EU Commission will change in the wake of the election this year.

Thirdly, does the Commission believe that there is a lack of interest on part of the national governments of member states to decidedly act against espionage provided that such surveillance does not target business or government?

A: I would say that the main issues simply lie elsewhere than on a lack of corporation. There is a lack of expertise in this field especially compared to China and the US. Europe needs to invest in research and innovation in the area of cyber security.

Q: So the focus at this point lies on bottom-up approaches rather than introducing new legislation and institutions?

A: It is possible to do a lot on the policy level, but a network is like an open boarder, whoever is just determined enough to gain information can do so. That is why the main focus must lie on achieving the technical ends to secure the infrastructure.

Q: **Part of securing information that is transmitted from or being stored in Europe is certainly to decentralize networks on the one hand and to retain as much data as possible domestically on the other hand. One step in this direction was the recently concluded agreement between the EU and Brazil to establish a direct transatlantic cable connection between Europe and South America. Firstly, will there be any more efforts in the coming years to further emancipate the European IT infrastructure from the US's?**

A: This is not my unit or field of expertise but to my knowledge this is the only project of its kind right now.

Secondly, are there any plans to legally compel businesses that collect data of EU citizens and enterprise to exclusively store this information on servers within Europe in order to make the operations of such ventures subject to EU data protection laws?

A: European companies will be urged to respect European data protection laws even if they store user data outside European boarders, foreign business will have to adhere European Safe Harbor agreements.

Q: An article by Guardian reporter Glenn Greenwald one week ago revealed that according to documents released by former NSA employee Edward Snowden the NSA has intercepted devices manufactured by US networking company Cisco in order to manipulate them and then proceed to compromise targeted networks. Now that this has become known, could the EU possibly impose embargos against networking products especially from the US, Russia and China at least in environments that are known to be essential for the IT infrastructure as a whole such as the ISPs?
A: It is possible that some states or companies may take action individually but regarding collective action, it is at least too early to say if such measures may be taken.

Q: Following the Snowden revelations US president Barack Obama pointed out that espionage even amongst military allies had always been common practice anywhere in the world. He also suggested that European countries would spy amongst each other and the results of the EP's Electronic Mass Spying of EU Citizens Inquiry confirms that this is true for at least 4 countries in the EU. Will there be any initiatives by the EU Commission to sanction such behavior by means of the existing legal framework or will there even be changes to the current legislation in order to at least oblige member states' governments not to spy on each other and their citizens, except where this is otherwise justified e.g. for the purpose of crime prevention?
A: The EU guarantees protection of user data and privacy for its citizens. The Data Protection Directive requires member states to obtain a court order before any surveillance of a target can take place. Surveillance therefore also must not take place indiscriminately, although some member states still have post 9/11 legislation that allows the collection of call records. Currently, to my knowledge there is no "no-spy agreement" between EU member states in progress.

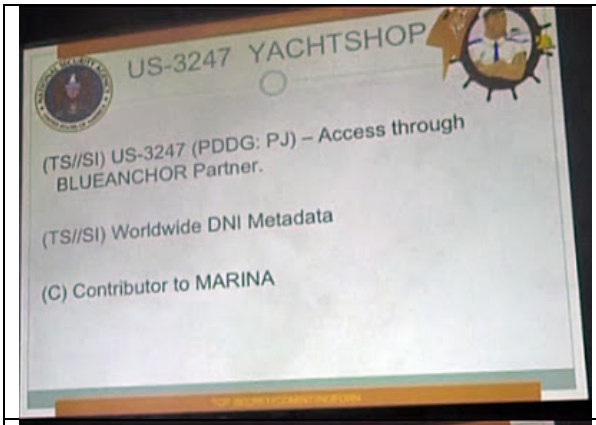

Figure 1, source: http://electrospaces.blogspot.de/2014/01/slides-about-nsas-upstream-collection.html

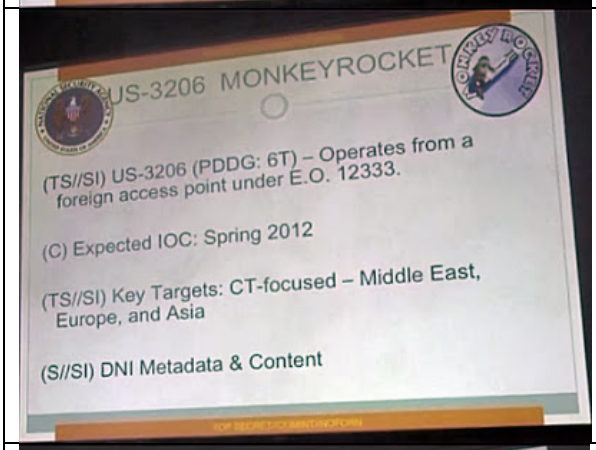

Figure 2, source: http://electrospaces.blogspot.de/2014/01/slides-about-nsas-upstream-collection.html

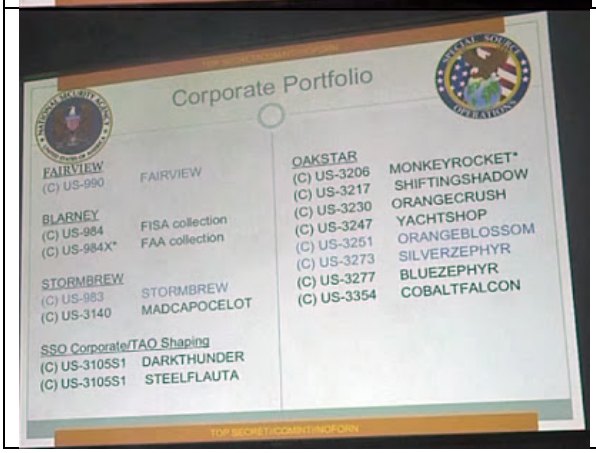

Figure 3, source: http://electrospaces.blogspot.de/2014/01/slides-about-nsas-upstream-collection.html

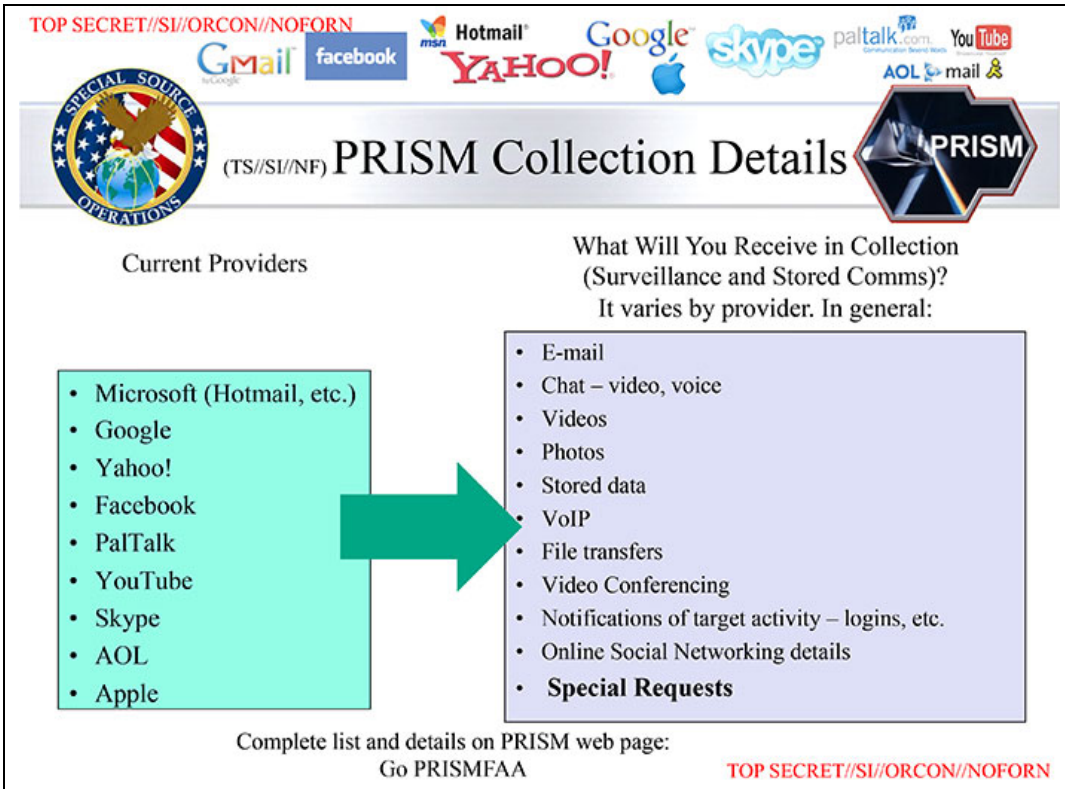

Figure 4, source: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

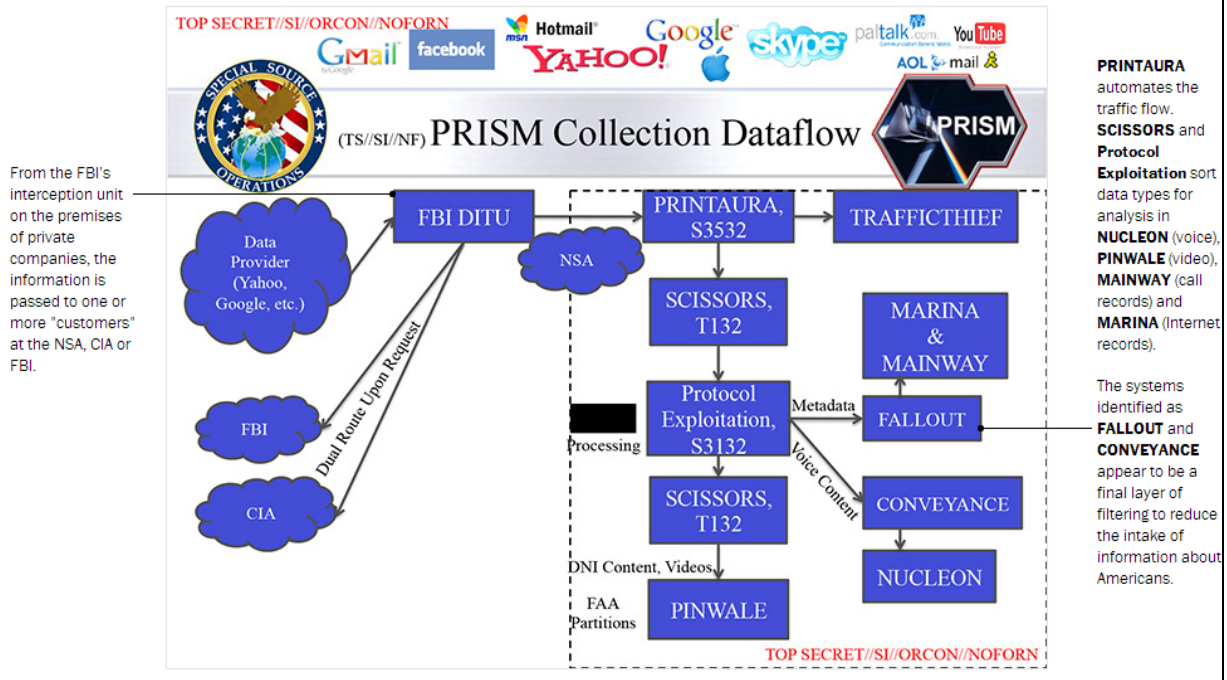

Figure 5, source: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

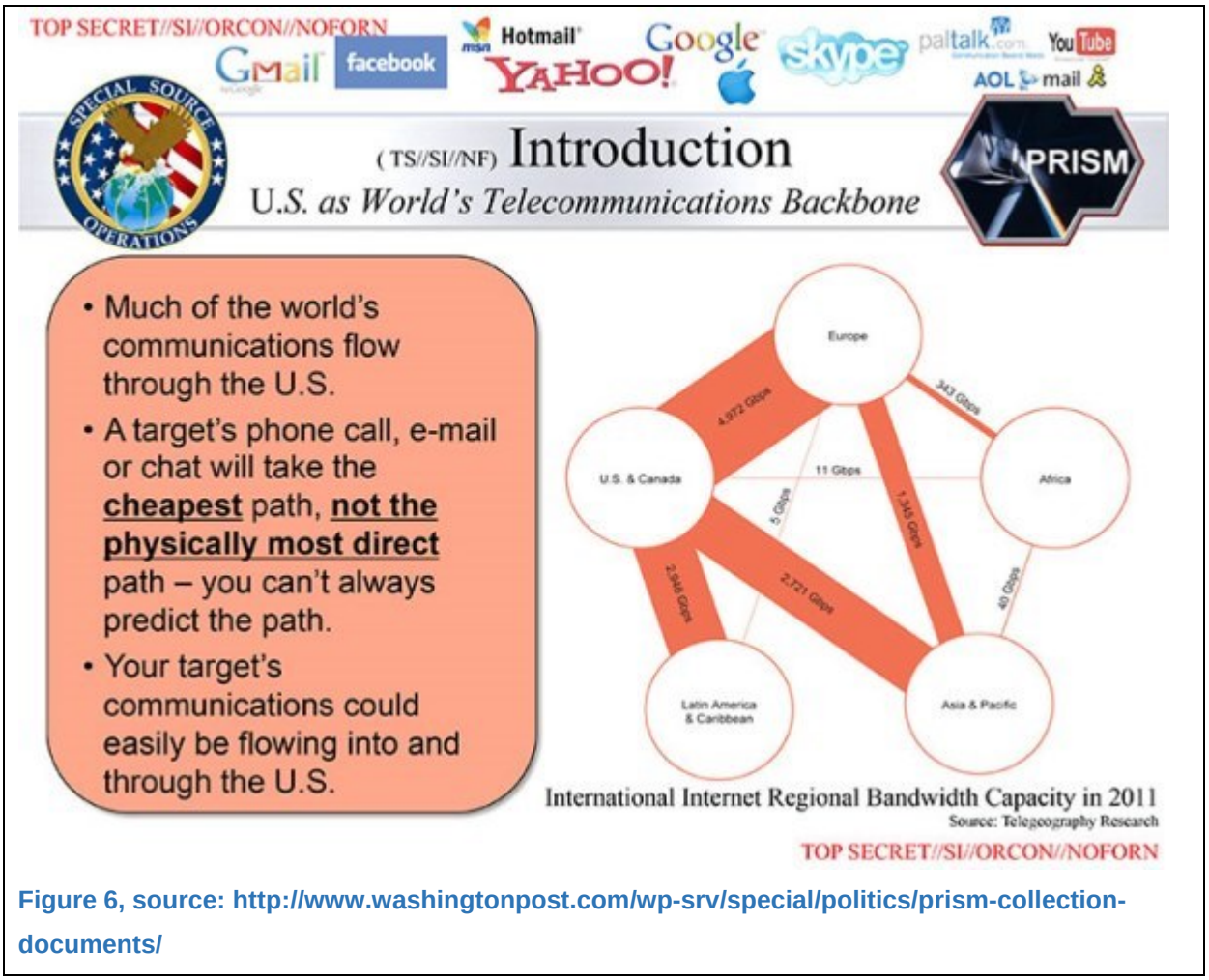

Figure 6, source: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/