FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Cyber Espionage

An analysis of threats from Intelligence Gathering with an emphasis on Industrial Espionage in today's information society

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Oleg Denisov
Matrikelnummer 0725490

am
Fachbereich Rechtswissenschaften der Technischen Universität Wien

Betreuung: Ao. Univ.-Prof. Dr. iur. Markus Haslinger

Wien, 20.04.2014

(Unterschrift Verfasser) (Unterschrift Betreuung)

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Cyber Espionage

An analysis of threats from Intelligence Gathering with an emphasis on Industrial Espionage in today's information society

MASTER'S THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Business Informatics

by

Oleg Denisov
Registration Number 0725490

to the department of law
at the Vienna University of Technology

Advisor: Ao. Univ.-Prof. Dr. iur. Markus Haslinger

Vienna, 20.04.2014

(Signature of Author) (Signature of Advisor)

Erklärung zur Verfassung der Arbeit

Oleg Denisov
Geerzkamp 7, 22119 Hamburg

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

(Ort, Datum) (Unterschrift Verfasser)

Acknowledgements

First and foremost, I would like to thank my supervisor, Professor Markus Haslinger. Your expertise, enthusiasm and support have made it a pleasure to work with you. A special 'thank you' goes to the seven interview partners, who helped me with their support and know-how on this very sensitive topic, and who can not be named in respect to the obligation of confidentiality regarding the company's identity. Finally, I want to thank my beloved family, who supported me through the whole writing process.
This work is dedicated to you.

Abstract

In recent years the technological advancements in the IT sector have created capabilities for state-affiliated authorities of an extent beyond belief. Taking into account the vast global network that is the internet, new opportunities arose to carry out cyber espionage for agencies like the US-American NSA or the British GCHQ, targeting individuals, companies, institutions and providers of critical infrastructure. This thesis analyses the present techniques of cyber espionage, and the corresponding emerging risks and threats to the know-how of companies, and to the privacy of individuals, outgoing from intelligence gathering techniques and industrial espionage: topics, that, due to their confidential character, have been subject only to limited research.

Further, it investigates the possible preventive measures in the sphere of information security, to protect corporate and personal information, data in particular. In addition, further risks associated with global surveillance and cyber espionage in today's information society are considered, including the topics of Big Data, mobile devices and Cloud Computing, as well as the presence of cyber war. Furthermore, the European Union's strategy to fight cyber attacks and intelligence gathering, as well as their plans concerning reporting requirements are highlighted. Finally, a look is taken into the scope of security measures, covering inter alia corporate security and alternatives for the individual person.

After a theoretical introduction and a situational analysis with the objective to develop anticipation and prevention, the findings of seven interviews with IT experts are presented, evaluated and integrated into the existing state of knowledge.

The results reveal that awareness needs to be raised regarding the various risks to information security, not only in the IT related sphere, but also with respect to the highest risk imposing body, the human being.

Kurzfassung

In den letzten Jahren haben die technologischen Fortschritte in der IT-Branche staatlichen Behörden Möglichkeiten geschaffen, die weit jenseits der Vorstellungskraft liegen. Unter Berücksichtigung des riesigen globalen Netzwerks, des Internet, enstanden neue Möglichkeiten für Geheimdienste, wie die US-amerikanische NSA oder die britische GCHQ, Cyber-Spionage an Einzelpersonen sowie Unternehmen, Institutionen und Anbietern von kritischen Infrastrukturen durchzuführen. Diese Masterthesis analysiert die aktuellen Techniken der Cyber-Spionage und die entsprechend auftretenden Risiken und Bedrohungen für das Know-how von Unternehmen und für die Privatsphäre des Einzelnen, ausgehend von modernen Techniken der Informationsbeschaffung (Intelligence Gathering) und der Industriespionage: Themen, welche aufgrund ihrer geheimen Charakteristik bisher Gegenstand nur begrenzter Forschung waren.

Ferner wird untersucht, welche möglichen präventiven Maßnahmen im Bereich der Informationssicherheit existieren, um die unternehmensinternen Informationen und die Privatsphäre des Individuums, insbesondere Daten, zu schützen. Zusätzlich werden weitere entstandene Risiken in der heutigen Informationsgesellschaft betrachtet, die mit der zunehmenden globalen Überwachung und Cyber-Spionage entstanden sind, unter Berücksichtigung der Themen Big Data, mobile Geräte und Cloud Computing, sowie der Präsenz eines Cyber-Krieges. Ebenfalls diskutiert wird die Strategie der Europäischen Union im Kampf gegen Cyber-Angriffe und die globale Informationsbeschaffung sowie deren Pläne bezüglich einer Meldepflicht. Schließlich wird ein Blick auf eine Auswahl von Sicherheitsmaßnahmen geworfen, die unter anderem für die Unternehmenssicherheit und die Sicherheit der Privatsphäre der einzelnen Person existieren.

Nach einer theoretischen Einführung und einer situativen Analyse mit dem Ziel, Antizipation und Prävention zu entwickeln, werden die Ergebnisse von sieben Interviews mit IT-Experten vorgestellt, bewertet und in den bestehenden Wissensstand integriert.

Die Ergebnisse zeigen, dass das Bewusstsein im Hinblick auf die verschiedenen Risiken für die Informationssicherheit gesteigert werden muss: Und zwar nicht nur in der IT-bezogenen Umgebung, sondern auch in Bezug auf den Menschen, der heute immer noch das größte Risiko für ein Unternehmen darstellt.

Contents

List of Figures **xiv**

List of Tables **xv**

Abbreviations **xix**

1 History **1**
1.1 Short introduction into the history of espionage 1

2 Theoretical Political and Practical Background **5**
2.1 Definitions of espionage 5
What is espionage? 5
What is cyber espionage? 6
Targets of (cyber) espionage 6
Methods of espionage 6
Human Intelligence 7
Signals Intelligence 8
2.2 Industrial Espionage in numbers 8
No reliance on accurate data 10
2.3 How is espionage carried out? 11
Difference between random and targeted attacks 12
2.4 Technical conditions for intercepting communication and access 13
The importance of fibre-optic cables 15
Hollow fibre-optic cables 15
Automated evaluation of intercepted communication 15
2.5 Brusa, UKUSA, Five Eyes 16
2.6 The communication interception system ECHELON 17
Neglected propositions 19
Damage caused by ECHELON 20
Technology behind ECHELON 20
ECHELON-type communications interception system and European Union law 21
Communications surveillance as a violation of the fundamental right to privacy 21
The protection of privacy under international agreements 21

Monitoring of intelligence services . . . 23
ECHELON's capabilities of conducting industrial espionage . . . 24
Conclusions taken from ECHELON . . . 24
2.7 Insurance companies advance to new markets . . . 25
2.8 NSA and its assignments . . . 26
How the events of 9/11 affected US authorities . . . 27

3 Cyber Spying **29**
3.1 USA's view on world cyber security issues . . . 29
3.2 Increasing industrial espionage over the internet . . . 29
3.3 UN's input on Internet surveillance . . . 30
3.4 International Cyber Espionage activities . . . 31
Chinese industrial espionage . . . 31
ThyssenKrupp and EADS as targets . . . 31
Other Chinese espionage activities . . . 31
Targeting US-weapon systems . . . 32
Drone technology . . . 32
US investigations on threats by Chinese telecommunication companies 33
Australian company reports cyber attack from China . . . 34
Chinese counter-espionage . . . 34
Dummy infrastructure yields excessive cyber attacks . . . 35
Verizon report indicating industrial espionage . . . 35
Phishing . . . 38
Evolving cyber espionage techniques . . . 39
Watering hole attack . . . 39
3.5 Internet surveillance in Russia . . . 39
3.6 BND and surveillance . . . 40
Germany's role in intelligence gathering . . . 41
3.7 British plans of building a new military cyber unit . . . 42
3.8 Austria develops cyber 'militia' . . . 42
3.9 Mobile malware on the rise . . . 42
3.10 Visualization tools . . . 43
Google's malware statistics . . . 44
3.11 Outlook . . . 44

4 Programs **47**
4.1 Programs and operations indicating state-affiliated cyber espionage . . . 47
FinFisher . . . 47
FinFisher in detail . . . 48
BKA acquires FinFisher . . . 50
Information provided through presentation slides . . . 51
FinUSB Suite . . . 51
FinIntrusion Kit . . . 51
FinFly USB . . . 51

FinFly Web . . . 52
FinFly ISP . . . 52
FinSpy Mobile . . . 52
China's cyber operations . . . 53
Structure of an attack on the example of APT1 . . . 55
Infrastructure . . . 58
Stuxnet . . . 59
Flame, miniFlame, Gauss and Duqu . . . 63
Flame . . . 63
Gauss . . . 64
miniFlame . . . 65
Duqu . . . 66
GhostNet . . . 66
Planet Blue Coat . . . 68
Red October . . . 69
Winnti . . . 71
NetTraveler . . . 72
4.2 Analysis . . . 72

5 Governmental surveillance **75**
5.1 A new pinnacle of global surveillance outgoing from the USA . . . 75
Edward Snowden's confidential documents . . . 76
5.2 Prism . . . 77
Microsoft's cooperation . . . 78
Backdoors in Skype, SkyDrive and Outlook . . . 79
How Prism works . . . 79
Fairview & Blarney . . . 80
5.3 Upstream . . . 81
BND in possession of Prism . . . 81
5.4 Boundless Informant . . . 82
5.5 Tempora . . . 83
5.6 XKeyscore . . . 85
Australia's and New Zealand's involvement . . . 89
5.7 Metadata - connecting the dots . . . 90
5.8 US surveillance on European 'allies' . . . 91
NSA's ranking of intelligence priorities (espionage) . . . 92
5.9 NSA and data from US citizens . . . 92
Loophole in FISA Amendmend Act 702 . . . 93
Crossing the line . . . 94
5.10 Genie . . . 95
Exploitation . . . 96
USA's ROC . . . 96
5.11 Social Media Intelligence - SOCMINT . . . 96

5.12 Resistance movements and control instances . . . 97
The German Control Panel . . . 98
5.13 Other activities . . . 98
Monitoring German communications . . . 98
French surveillance . . . 99
US hacking Hong Kong and China . . . 99
5.14 Industrial Espionage as part of NSA's mass-surveillance . . . 100
Cyber attack on Belgacom . . . 100
Spying on the G-20 summit . . . 101
... and the United Nations headquarters . . . 101
Special Collection Service . . . 102
Smartphone surveillance . . . 103
Monitoring of international transactions . . . 103
5.15 NSA's budget . . . 104
5.16 Trivialization associated with reasoning . . . 105
5.17 Analysis . . . 105

6 Risks associated with global surveillance and cyber espionage 109
6.1 Big Data . . . 109
6.2 Objects turning 'smart' - customer surveillance . . . 110
6.3 Safety of Cloud services . . . 110
6.4 The presence of Cyber War . . . 111

7 Strategies of the European Union 113
7.1 Cyber Security Strategy . . . 113
Information Security support by the ENISA . . . 115
European Cybercrime Center . . . 116
7.2 Reporting requirements in cases of espionage . . . 116
Data Breach Notifications . . . 117
Plans of the German BND . . . 118
NCAZ . . . 118
7.3 EU's penalties on cyber criminality . . . 118
7.4 Analysis . . . 119

8 Scope of security measures 121
8.1 Defensive strategies . . . 121
8.2 Encryption of data . . . 122
Method and purpose of Encryption . . . 122
Security of encryption systems or when you can speak about a system being secure 123
Overview of a selection of encryption tools . . . 123
8.3 Intrusion Detection System . . . 125
8.4 Are companies prepared for APT cyber attacks? . . . 126
8.5 The Critical Security Controls for Effective Cyber Defence . . . 129
8.6 Where companies should put their focus on . . . 129

Is proper defence possible? . . . 130

9 Conclusion **133**

10 Terms and Definitions **137**
10.1 Terms and Definitions . . . 137

11 Results and Discussion **141**
11.1 Expert interview sample . . . 141
11.2 The expert interview method . . . 142
Interview: The topics . . . 142
Risk analysis and evaluation . . . 142
Risks of business cooperation . . . 145
Frequency and scope of cyber attacks . . . 145
Communication with authorities . . . 146
Personnel . . . 146
Clean Desk Policy and Logging . . . 148
Access . . . 148
Risks from data carriers and encryption of devices / data traffic . . . 149
Systematic password change . . . 150
Firewall, Anti-Virus, Anti-Spam . . . 151
Updates and tests . . . 151
Risks of using mobile devices and cloud storage . . . 152
Open Source as an alternative . . . 153
Insurance - an option? . . . 154
Possible counter measures . . . 154
Organisation (Risk management) . . . 154
Personnel . . . 155
IT-security . . . 155
Outlook and Conclusion . . . 157

12 Expert-Interviews **159**
12.1 Interview Transcripts . . . 159
12.2 Transcript 1 . . . 159
12.3 Transcript 2 . . . 167
12.4 Transcript 3 . . . 176
12.5 Transcript 4 . . . 187
12.6 Transcript 5 . . . 194
12.7 Transcript 6 . . . 208
12.8 Transcript 7 . . . 222

13 Appendix: Overview of intelligence services **233**

Bibliography **235**

List of Figures

3.1 Overview of the three main data breach causers (reprinted from [204, p.22]). 37
3.2 How malware is initially distributed (reprinted from [204, p.29]). 37
3.3 Variety of malware components (reprinted from [204, p.30]). 38
3.4 Data packet flow across submarine cable routes 44

4.1 Geographic locations of APT1's victims (reprinted from [133]). 54
4.2 APT1's cyber espionage operations against organizations by industry (reprinted from [133, p.22]). 55
4.3 A list of common commands on the example of the BISCUIT backdoor, utilized by APT1 (reprinted from [133, p.33]). 57
4.4 HTRAN tool as 'middle-man' residing on APT1 hop points (reprinted from [133, p.41]). 58
4.5 Control flow at entry point (export function) (reprinted from [193, p.16]). 61
4.6 The interface of the Gh0st RAT Beta 3.6 tool (reprinted from [152, p.36]). 67
4.7 Overview of Rocra's C2 infrastructure (reprinted from [111]). 71

5.1 Submarine cable map centring on the United Kingdom's position (source: [194]) . 85
5.2 Personal information packed in Metadata: Comparison of mostly used internet services (reprinted from [26]). 91

7.1 Attack distribution data for 2012 (reprinted from [63, p.11]). 115

8.1 Companies' assumptions of the own protective measures against Advanced Persistent Threat (APT)s (reprinted from [182]). 127
8.2 Assumptions of the highest risks from APTs (reprinted from [182]). 128

List of Tables

13.1 List of the most relevant intelligence services, which appeared in this thesis. 234

List of Abbreviations

API Application Programming Interface

APT Advanced Persistent Threat

ASD Australian Signals Directorate

ASIO Australian Security Intelligence Organisation

AV Anti-Virus

BfV Bundesamt für Verfassungsschutz

BKA Bundeskriminalamt

BND Bundesnachrichtendienst

Brusa British-U.S.A.

BSI Bundesamt für Sicherheit in der Informationstechnik

C2 Command & Control

CC ITÜ Kompetenzzentrum für informationstechnische Überwachung

CEO Chief Executive Officer

CIA Central Intelligence Agency

CISO Chief Information Security Officer

COMINT Communications Intelligence

COMSEC Communications Security

CSDP Common Security and Defence Policy

DGSE Direction Générale de la Sécurité Extérieure

DIA Defense Intelligence Agency

DNI Digital Network Intelligence

DoD Department of Defense

ECHR European Convention of Human Rights

EDA European Defence Agency

EEA European Environment Agency

ELINT Electronics Intelligence

ENISA European Network and Information Security Agency

FAPSI Federalnoje Agentstwo Prawitelstwennoi Swjasi i Informazii

FBI Federal Bureau of Investigation

FISA Foreign Intelligence Surveillance Act

FISC Foreign Intelligence Surveillance Court

FSB Federalnaja sluschba besopasnosti Rossijskoj Federazii

FTP File Transfer Protocol

GCHQ Government Communications Headquarters

HUMINT Human Intelligence

INTELSAT International Telecommunications Satellite Organization

IOC Information Operations Center

ISAC Information Sharing and Analysis Center

ISP Internet Service Provider

LAN Local-Area-Network

MI5 Military Intelligence 5

MI6 Military Intelligence 6

NAC Network Analysis Centre

NATO North Atlantic Treaty Organization

NCAZ Nationale Cyber-Abwehrzentrum

NDA non-disclosure agreement

NDEU National Domestic Extremism Unit

NSA National Security Agency

NSCID National Security Council Intelligence Directive

OS Operating System

RAT Remote Administration Tool

RIPA Regulation of Investigatory Powers Act

ROC Remote Operations Center

ROI Return on Investment

SCS Special Collection Service

SIGINT Signals Intelligence

SOCMINT Social Media Intelligence

SORM System of Operative Search Measures

SSL Secure Sockets Layer

SSO Special Source Operations

STOA Scientific and Technological Options Assessment

TAO Tailored Access Operations

TECHINT Technical Intelligence

TLS Transport Layer Security

UAE United Arab Emirates

UKUSA U.K.-U.S.A.

UNO United Nations Organization

USC United States Code

VHF Very High Frequency

VM Virtual Machine

VoIP Voice over IP

VPN Virtual Private Network

WEP Wired Equivalent Privacy

WPA Wi-Fi Protected Access

CHAPTER 1

History

1.1 Short introduction into the history of espionage

Espionage is:

> *the act of obtaining, delivering, transmitting, communicating, or receiving information in respect to the national defence with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation.*[1]

Espionage is as old as human history itself and is often considered to be one of the oldest professions in the world. From the beginning of the manifestation of human's craftsmanship and trade the desire emerged to expand one's knowledge and find out about other innovative products, designs or recipes. With the travel to other regions and cultures either by foot or later on with the expeditions by ship those desires became gradually more apparent. For the ruling regimes the employment of agents always has been a very important resource for both, the protection of the own valuable information from internal and external threats, as well as their service on spying missions. Dangers at any point needed to be detected and proper defensive actions taken[2].

While most of the espionage activities were primarily related to trade and the new utilization of resources, in Venice, Italy the art of cipher and encryption slowly began to develop for the purposes of securing sensitive information (e.g. political contracts or reports). This behaviour should then start to manifest as a state-of-the-art paradigm in more governments and the occupation of spies along with it[3]. So throughout two millennia espionage has been a present tool, which many countries and individuals gained, but also have lost from.

[1] [85, p.49]
[2] [201, p.32]
[3] [201, p.36]

In the following years of the 19th century, after several wars and campaigns in Europe, the first three versions of secret services emerged. Namely, the German 'Central-Nachrichten-Bureau' in 1871 and a bit later the British Military Intelligence 5 (MI5) and Military Intelligence 6 (MI6) organizations in 1906 with domestic and foreign responsibilities respectively[4]. In Russia the first secret service 'Tscheka' (later replaced by KGB) was founded in 1917 by the Bolshevists shortly after the Russian revolution. In general, espionage activities during the first world war were characterized by many miscalculations and poor execution[5]. In contrast to the properly functioning and officially administered secret services during world war II, when actions by the British actively influenced the course of the war (e.g. Enigma machine) [6].

Besides the main tasks of infiltrating and spying, secret services like the Central Intelligence Agency (CIA) have also been using forms of propaganda or disinformation in order to influence the public[7], as well as withholding information from the public[8]. Of course, murders play also a role in secret service activities, even though a majority of killings cannot be traced back to the initiators [9].

In general, one can say that secret services are in funds of any imaginable authority, of using any method necessary to reach their targeted intention.

Today, what we know of industrial espionage is the purposeful gathering of (mainly) secret information from individuals or companies / institutions for own benefits, whichever those may be. Mostly, secret service activities aim at securing and protecting their governments' interests. Over the course of the 20th century new activities on behalf of states in form of intelligence services[10] evolved and with them new methods and techniques of obtaining information. "The product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of all collected information" is often known as 'intelligence'[11].

In the last 20 years the internet also developed and became part of almost everyone's life and daily routines in the civilized world. Therefore, we can find ourselves living in an information society, where the internet plays the role of the infrastructure and gives us humans the opportunities to create and share content, and where information is available for anyone, from almost any part of the world. In this regard, one should not refer to the internet simply as just the physical infrastructure, meaning the submarine cables, the cell phone towers and copper- / fibre-optic cables that provide the internet access[12]. There are also all the different protocols, applications and databases, that make the internet a gigantic source of information.

The methods of conducting espionage became increasingly cost-intensive and complex with the fast ongoing change in technology. After relying mainly on Human Intelligence (HUMINT), secret services all over the world began utilizing telecommunication mechanisms and devices, and closer to the end of the 20th century (super-)computers and the internet, all technologies used

[4] [201, p.40-41]
[5] [201, p.42]
[6] [201, p.44]
[7] [201, p.57]
[8] [201, p.60-61]
[9] [201, p.63]
[10] *also often called secret services*
[11] [85, p.79]
[12] [184]

to collect information, a process specifically known as Technical Intelligence (TECHINT).[13] Besides espionage activities by intelligence services, a new threat emerged with the internet: Hackers or 'hacktivists', who use today's technology to gain access to databases, private computers or communication devices.

[13] [126, p.136]

CHAPTER 2

Theoretical Political and Practical Background

2.1 Definitions of espionage

Intelligence services are run by governments in addition to national police forces in order to secure a country's safety. Their operations are characterized as being highly organized and secret. Their tasks mostly consist of[1]:

- gathering information to point out dangers to state security
- gathering information from foreign countries
- referring dangers to armed forces
- counter-espionage

What is espionage?

Espionage is the organized gathering of information without the target's (information holder) notice. Significant information in the various fields of interest is naturally kept secret from governments, as well as businesses and as such is not available to the public. The purpose of espionage is to find a way to access this information, which in most cases results in theft. Information is systematically collected from other states and evaluated for own benefits (mostly knowledge). This then becomes a "basis for decision making" (e.g. foreign policy, technological and industrial know-how, armed forces)[1]. Intelligence services serve therefore a purpose of assessing valuable "information available from public sources"[1]. The assumption is that "at least 80% of the work of the intelligence services" is referred to espionage.[1]

[1] [185, p.25]

What is cyber espionage?

Cyber espionage is the systematic practice of obtaining secrets in digital format, whether being sensitive, classified or proprietary information, from individuals, competitors, governments and enemies. But, also for military, political, or economic advantages, using illegal exploitation methods on internet, networks, software and computers.[2] The term 'cyber' refers to activities involving the use of computer systems, especially activities on the internet, rather than the real (physical) world.[3] Further examples of words formed with this term are cyber crime, cyber warfare and cyber security.

Targets of (cyber) espionage

Cyber espionage primarily targets to steal trade secrets from corporations, as well as classified information from government agencies.[3] More specifically, typical espionage targets also include[4]:

- military secrets
- abroad government secrets
- information about stability of / dangers to governments

These may consist of new & advanced weapon systems, information about the number and location of stationed troops or military strategies. Equally important is also information "about forthcoming decisions in the fields of foreign policy, monetary decisions or inside information about tensions within a government"[4]. Of course, there is also interest in economically significant information, including economy sectors, foreign transactions, as well as new technology, especially for countries whose interest it is to close the gap to the more advanced (and innovative) nation in any of those sectors.

Methods of espionage

Espionage involves breaching security measures and penetrating protection in order to access the sought information in both cases of political and industrial espionage. Tools and techniques which are used to gather the information in general do not differ in terms of level of protection between those two fields. However, the "level of protection is generally lower in the economic sphere" when industrial espionage is conducted, because the business representatives often tend to have a low risk awareness when it comes to interceptible communication media, compared to the government, which tries to keep its valuable information secret and protected at all costs[5]. Two main categories of *intelligence gathering* in espionage operations are Human Intelligence (HUMINT) and Signals Intelligence (SIGINT).

[2] [63, p.6]
[3] [20]
[4] [185, p.25]
[5] [185, p.25-26]

Human Intelligence

One of the most effective and most applied espionage methods is that of using humans as sources for the collection and provision of information. Very often only a few people have access to internal (sensitive) information and handling/accessing the secret information requires generally strict rules. Moreover, the information is often kept at one place, and if it has to move the protective space, various security and encryption methods are applied before doing so. The use of humans (therefore human intelligence) can very often ease or even skip the hard and risky part of getting access (e.g. involving technology) or using encryption techniques to get to the 'raw' information.[6] When human intelligence is involved in espionage, operations are generally differentiated in[6]:

- poached individuals from the target area
- infiltrated agents from the own intelligence service or business

In military operations human intelligence can also cover activities involving reconnaissance patrols, debriefs, interrogations and conduct of counter-intelligence.[7]

Some of the reasons why poached individuals are working for foreign intelligence services or businesses include[8]:

- sexual seduction
- extortion
- bribery
- convincing of ideologies
- awarding of particular importance or honour

Other cases may involve involuntary collaboration, where individuals are persuaded during conversations on conferences, trade fairs, congresses, hotel bars and other public places. This human-to-human interaction, often used with the aim to get additional information (e.g. user credentials) is also known as *Social Engineering*[9].

Human intelligence provides clear advantages of direct access, but has also its disadvantages e.g.[10]:

- counter espionage always focuses people or leading agents
- high risks on the trust level
- humans very often tend to be error-prone and as such fall into the net of espionage

[6] [185, p.26]
[7] [85, p.66]
[8] [185, p.26]
[9] [49, p.94]
[10] [185, p.26]

Thus, whenever possible the use of agents and poached individuals is replaced by anonymous and human-independent espionage.[10]

Signals Intelligence

Signals Intelligence is the primary source type of intelligence gathering that is present in today's espionage operations and is covered in this thesis. While SIGINT generally refers to signal monitoring and interception, "including communications signals, electronic emissions, and telemetry"[11], Technical Intelligence (TECHINT) describes rather the technical abilities of an enemy or the technology that is used to collect intelligence. It is also more of a aggregation of the three types of sources of intelligence, like "imagery, measurement and signatures, and signals intelligence (IMINT, MASINT, SIGINT)"[12].

Two other types, which represent subsets of SIGINT are COMINT, referring to foreign communication interception "(excluding open radio and television broadcasts)" and Electronics Intelligence (ELINT), meaning non-communication electromagnetic signals - interception (mainly radar)[13].

Specific electromagnetic signals, e.g. transmissions from radar stations, can be of great importance to military forces, showing valuable information about enemy anti-air set-ups. This type of espionage is related to Electronics Intelligence. Electromagnetic transmissions are used in radar technology for providing aircraft, ship, submarine and troop positions from a non-negligible source of information to an intelligence service. Also of great importance is the tracking of other foreign espionage satellites and the recording and decoding of their signals (e.g. for counter operation purposes). Signal recording is done by solid stations on the earth-surface as well as by low circulating satellites.[14]

The evaluation of intercepted communication in the fields of military and diplomacy is obviously done by most intelligence services around the world, some of which also make use of advanced technology to monitor foreign country's civil communications. But some even don't hesitate to monitor their own national civil communications (cf. Chapter5). Generally speaking, the "monitoring of the communications of the country's own citizens is subject to certain triggering conditions and controls"[14]. Evidence that such assumption is only of theoretical value is shown by activities of authorities like the National Security Agency (NSA), which is illustrated in this thesis.

2.2 Industrial Espionage in numbers

At this point it should be noted, that one refers to *industrial espionage*, when someone externally, in this particular case a state intelligence service tries to obtain "information kept secret by a firm."[15] If, however, the invader is a rival firm, the proper term for it is *competitive intelligence*.[15]

[11] [126, p.79]
[12] [126, p.136]
[13] [126, p.79]
[14] [185, p.27]
[15] [185, p.97]

According to a study by Corporate Trust from 2012, generally almost *two thirds* of espionage damage is caused by employees. A criminal statistic from 2010 says that while the number of crimes went down by 2%, the "monitoring and intercepting of data" increased by full 32.2%[16]. The number of cases, when the *internet* was used as means even went up by 190%. The German economy alone suffers estimated €4.2bn total damage per year, caused by industrial espionage. That's an increase of 50% compared to 2007 (€2.8bn). From all the companies who reported of becoming victim to industrial espionage, 82.2% of companies suffered financial damage from it. Middle-sized companies are affected the most by espionage (23.5%), followed by Large companies (18.8%) and then small-sized companies (15.6%).[16]

In terms of affected industry sectors, the backbone of the German economy, the automotive, aerospace and machine engineering industries, have been mostly targeted (29.8%), followed by banks, insurance companies, and financial services providers (21.5%). Then comes the logistics & transport sector with 7.9%, and the computer & software sector with 7.0%.[17] Unexpectedly, the chemical & pharmaceutical industry amounts for 6.2%, which appears to be a bit low, considering the high innovative power of concerns like Bayer and BASF. But, of course, the numbers depend on the number of participants from the respective sectors, and as such, these numbers can differ from reality. In general, every sector that is somehow linked to the research of technologies is a favoured target for espionage. In terms of targeted departments, R&D is leading with 27% in front of Sales with 24%, C-Level (highest-level executives) with 17%, Shared Mailbox with 13%, Senior 12% and others.[18]

Additional numbers show[19]:

- Only around 20% of cases have been reported to the responsible authority, the German Federal intelligence and security service Bundesamt für Verfassungsschutz (BfV) or the police, while 57.6% of companies asked external security personnel or forensic investigators.
- 31.2% stated that the topic Information Security is handled by the general manager. At least 20.4% stated they have established a Chief Information Security Officer (CISO).
- 46.4% have a security policy with strict rules for information security.
- 18.8% of all companies, which use control systems, have reported an attack, however, 63.6% of these companies also described risks of future financial impact, 36.4% said that an attack could cause malfunction of their systems, and 13% even issued realistic concerns about a malfunction causing to endanger the population.

Moreover, it should be noted that hacker attacks on IT-systems and devices such as smartphones, laptops and tablets, nowadays amount for whole 42.4% (compared to 14.9% in 2007).[20] Modern devices like tablets become more popular in corporations, but inherit due to their structure one major security flaw. In contrary to (personal) computers, tablets and smartphones run

[16] [41, p.5]
[17] [41, p.15]
[18] [119, p.14]
[19] [41, p.8]
[20] [41, p.23]

applications or programs, which are certified/validated by central commercial authorities.[21] The user as such has little control over data entered into the device. Another cyber-related aspect is illustrated by the amount of monitoring of electrical communications such as e-mails, which was reported in 12.2% (10.7% in 2007) of all cases.[22]

When it comes to the impact of industrial espionage for each of the affected companies, those incidents resulted mostly in high costs in legal disputes (65.4%), followed by damage of reputation / image (59.9%), the infringement of patent rights (44.2%) and the loss of revenue due to loss of competitive advantage (36%). The direct damage to reputation and later on the financial loss, together still remain an apparent issue.[23]

As to security measures that were taken in order to protect oneself from industrial espionage, 90.6% stated that they have enabled password protection on all their devices. At least 86.1% reported having secured their internal firm network (e.g. with a Firewall). On average every second company makes use of encryption of network connection to partner companies (e.g. VPN), and encryption of data on notebooks. Continuous monitoring of log data (e.g. with Intrusion Detection Systems) is done by 20.9% and at least 18.9% have stated that they use cryptology in e-mail exchange. 18.6% prohibited USB-sticks and portable Hard Drives. And 13.9% have the security certificate of ISO 27001.[24]

Overall, a notable increase of espionage activities and a rise of APTs in recent years can be seen, which requires holistic approaches. One such approach would be applying the international standard for information security ISO 27001[25], which has around 20.000 certifications worldwide.[26] A certificate can serve as a quality characteristic to both customers and to business partners and thus lead to a competitive advantage. Institutions that seek such a certificate can be IT service providers, which want to show proof of their proper realisation of measures for IT baseline protection, or cooperating companies, which would like to be informed on the IT-security level their business partners can assure. In short, it serves as proof for sufficient IT-security implementations, and thus lower risk.[27]

No reliance on accurate data

In general, it is very difficult to determine accurate numbers in terms of extent of damage caused by industrial espionage or competitive intelligence. Especially, considering the fact that industrial companies, security firms and counter-intelligence services have high interest in "putting the losses at the high end of the realistically possible scale."[28]

While numbers can help in developing security strategies, the real scale of losses is rather irrelevant, because the government has always the responsibility to fight industrial espionage and competitive intelligence to prevent losses of valuable know-how, which in the worst case can

[21] [123]
[22] [41, p.22]
[23] [41, p.24]
[24] [41, p.34]
[25] [22]
[26] [116]
[27] [43]
[28] [185, p.98]

cause incalculable damage to the nation's economy. Furthermore, it serves no good for firms to make decisions on the protection of their information, based "on total damage figures."[29]. Firms must individually analyse the damage potential and make risk calculations and then assess their resources for a proper security system (including not only the infrastructure, but also guidelines and overall 'philosophy'). In the end, the true problem is not the lack of overall accurate loss figures, but rather that cost & benefit calculations are rarely made (except in large firms), and as a consequence security is neglected.

One must emphasize on the lack of true accurate numbers, coming from these sectors affected by industrial espionage. There are many surveys on security, annual security reports etc., but most of this data on information security trends and concerns is rather used to "justify increased expenditures on security tools and technologies", meaning that it's plain marketing[30]. The numbers in most cases are hardly collected properly, but are nevertheless used by students, government officials and companies, who rely on those numbers to make the right decisions in regard to their security. The numbers are "anecdotal, are not generalizable to the business level, and are reported in cumulative form", said several researchers from The George Washington University, after making a meta study on this very topic[30]. Therefore, all numbers that are used to explain security vulnerabilities and the ever growing threat from cyber attacks (including espionage), should always be regarded with care. In the end, there is unreliable data that is masked as reliable data, and people, decision-makers in particular do not "question the reliability of the data", which results in resources being "allocated inappropriately or ineffectively".[31] When it comes to sensitive information, companies keep as much details undercover as possible, so that accurate numbers cannot exist, as long as there are no regulations that force them to publish incidents involving attacks and security breaches. The numbers that are mentioned in this thesis or other sources are illustrated as indicators of the damage scale industrial espionage over the internet can cause, and therefore should not be taken for granted!

2.3 How is espionage carried out?

> *According to information provided by the counter-intelligence authorities and by the heads of security of large firms, all tried and tested intelligence service methods and instruments are used for the purposes of industrial espionage. Firms have a more open structure than military and intelligence service facilities or government entities.*[32]

Firms are therefore exposed to additional particular risks, coming from industrial espionage carried out by intelligence services[33]:

- Simpler recruitment of employees. Because, facilities of counter-intelligence authorities and those of industrial security services are incomparable.

[29] [185, p.99]
[30] [181, p.1]
[31] [181, p.8]
[32] [185, p.100]
[33] [185, p.100]

- Workplace mobility, referring to carrying devices with you (e.g. laptop) and thus posing high risk of data theft outside the firm's facility and security zone[34].

- Small and medium-sized firms are more vulnerable to security breaches and therefore information loss, than security-sensitive institutions (e.g. state bodies).

- The same reasons apply also to local tapping of communications.

Difference between random and targeted attacks

E-mail phishing attacks represent an often used method when it comes to infiltrating computer systems. Random attacks involve sending millions of e-mails with attached malware or with links leading to websites where malware is installed. The primary aim of the perpetrators is to get as many credentials as possible in order to gain the most access and money with it as possible. So, during such a literally 'spam-run' thousands and millions of computers become infected, whether it is the home user or the corporate user all over the world. Concurrently, it is fairly easy for security companies and groups (such as f-secure or citizen lab) to get a copy through a sample of the malware program, which is often provided by external sources or internal honey pots. In the labs it can be analysed and then an update of AV software is released to the public. On the other hand, in targeted attacks the number of e-mails sent out is far smaller. 1-5 e-mails are sent to targeted organizations and can infect the computer systems, often unnoticed for months and even years. So there are the criminals who use random spam runs to steal money and there two other groups who belong to the type of targeted attacks. Those two are state-affiliated attacks and those by hacktivists, who mostly do it out of beliefs, protest or just to make a statement.[35] In 2012 there has been an increase of 42% of targeted attacks, according to Symantec[36]. The process or 'anatomy' of a targeted attack usually consists of 5 steps[37]:

- Reconnaissance, describing the search for a particular victim (e.h. through means like Social Networks)

- Incursion, describing the successful breach into the victim's system

- Discovery, referring to the actual detection of the attack by the victim or by others

- Capture, representing the acquisition of the attack (e.g. malware)

- and Exfiltration, referring to the successful removal of (preferably) all traces of the intrusion from the system / network.

[34] Copying hard disks is a standard method in industrial espionage.
[35] [212]
[36] [119, p.10]
[37] [119, p.11]

2.4 Technical conditions for intercepting communication and access

The two most important types of communication in today's information society are of course wired and wireless communication. Internet runs over a large network of fibre-optic cables that serve as the main medium to transmit signals across the world.

All sorts of communication are transmitted through wire (speech, fax, e-mail, data). Wired communication can only be monitored if you have access to the wire. An access to it is possible, as long as the access point's location is on the territory of the monitoring state. So, from a technical stand point any domestic wire can be monitored. Foreign intelligence services mostly do not have legal access to cables from other countries, so that illegal action must be done accepting the high risk such action implies.[38] Collaborations of multiple states (e.g. cooperative projects involving submarine cables) in an intelligence alliance provide access to any gateway point of wired communication and as such a diverse selection of intercontinental connections. Today, for instance, optical fibre-cables (which are required for internet use) are laid down without any significant detours from the US straight to e.g. Australia or New Zealand. This way the interconnectivity of the worldwide network can be provided.

Fibre-optic cables of the new generation use an erbium laser as repeater, which in contrary to old fibre-optic cables does not allow being monitored at the electromagnetic coupling of the repeater any more. Such fibre-optic cables can today only be used for intercepting purposes, if you directly access the endpoint (*terminals*) of the connection.[39] In practice, this means that members of the U.K.-U.S.A. (UKUSA) can - provided corresponding expenses - only use the endpoints of submarine cables, which pass their territory for interceptions. This regards solely wired communication entering or leaving national territory.

In conclusion, the access to such wired communication in Europe is limited to the territory of the solely European member of the UKUSA, the United Kingdom. All this is true at least for phone and fax. Communication over the internet is subject to some different conditions[40]:

- communication over internet runs "using data packets". When different data packets are sent (or addressed) to the same recipient, they "may take different routes" to reach their destination.

- at the beginning of the internet age mainly "spare capacity in the public network was used for the transmission of e-mail communications". As such, data packets following the routes were "unpredictable and arbitrary".

- an e-mail, which is sent from a customer of one provider to a customer of another provider "is generally routed through the firm's network", regardless whether it's the quickest route. Routing is done by devices called *routers*, which are situated at "network junctions and which determine the route by which data packets will be transmitted". The "transition to other networks" then follows "at points known as *switches*"

[38] [185, p.31]
[39] [185, p.32]
[40] [185, p.32-33]

- in the beginnings of the internet 'era' the switches for the routing of global internet communications were placed in the USA. For that very reason, "intelligence services could intercept a substantial proportion of European Internet communications. Today, only a small proportion of intra-European Internet communications are routed via the USA."

- today intra-European communications are only to a small proportion "routed via a switch in London to which, since foreign communications are involved, the British monitoring station Government Communications Headquarters (GCHQ) has access." Nowadays, for the most part the communications do not leave the continent: For instance, "more than 95% of intra-German Internet communications are routed via a switch [the DE-CIX internet exchange point] in Frankfurt."

In practice, only a limited volume of internet communication that is transmitted by cable is therefore accessible by authorities of the UKUSA alliance, as long as there are no further collaborations that extend their reach.

There are also other sorts of communication interception techniques like radio communications, satellite communications and interceptions from aircraft, ship or spying satellites, but those shall not be further explained on the topic of this thesis.

Here is a list (in descending order) of some countries highly involved in intelligence gathering, showing the number of countries that are connected by fibre-optic cables[41]:

- United States is connected to 63 countries (Five Eyes alliance)
- France: 60
- United Kingdom: 57 (Five Eyes alliance)
- India: 55 (for reference)
- Germany: 40
- Australia: 38 (Five Eyes alliance)
- China: 36
- Iran: 12 (for reference)
- Russia: 7
- Canada: 6 (Five Eyes alliance)
- New Zealand: 4 (Five Eyes alliance)

The geographic locations of France and especially the United Kingdom provide both countries large data collecting capabilities.

[41] [42]

The importance of fibre-optic cables

Fibre-optic cables became most important targets for government surveillance, after they have been replacing copper telephone wires and satellite and microwave transmissions, which have been used for surveillance purposes in an earlier 'era'. A large number of global fibre-optic cables, which together are able to carry thousands of gigabits per second (10 Gbps for one), lie on the ocean floor and provide "higher-quality transmission and greater capacity", than the earlier and older technology[42]. Today, the world's hundreds of undersea cables cover 99% of all transferring intercontinental data, including most phone calls.[43]

One of the key US surveillance tactics in the 20th century has been the process of tapping undersea transmission cables, which at that time were simple "copper lines carrying sensitive telephone communications"[44]. Back then, divers who were able to place listening devices on the outside of a cable's housing, could eavesdrop on the transmitting data. For that very purpose, the US had four submarines, who were equipped accordingly for such missions.[44] In contrast to the copper cables, fibre-optic cables are less expensive, have less signal degradation, need therefore low power, and due to being thinner, are more lightweight and flexible.[45] Them being thin resulted in a difficulty to tap them successfully, compared to copper cables. Interception operations always "ran the risk of alerting cable operators that their network had been breached"[46]. Therefore, it is much easier to collect the information either directly from the various cable landing stations all over the world, or from the network operations centres, that operate the entire system.[46]

Hollow fibre-optic cables

In March 2013, researchers at the University of Southampton in the UK were able to develop a new 'hollow' fibre-optic cable filled with air, that is able to achieve 99.7% of the speed of light. As such, speeds close to 10 terabytes per second, which is 1,000 times faster than current fibre-optic cables, would be achievable.[47]

Automated evaluation of intercepted communication

Intercepting foreign communications is done by collecting all of the transmitted communications via satellite or cable, rather than monitoring a single telephone connection. Computers are then filtering relevant keywords, instead of analysing each single communication separately - which from a resource stand point is quite impossible any way. In this regard it should also be mentioned that "specific faxes and e-mails can also be singled out through the use of keywords"[48].

[42] [196]
[43] [76]
[44] [196]
[45] [72]
[46] [196]
[47] [109]
[48] [185, p.32-33]

Voice recognition (speaker recognition) is also possible, but only after the computer system has been trained to recognise it in advance. Whereas, *speech recognition*, which describes the translation of spoken words into text, despite having trouble with ambient noises and vocalization (accent, pitch, volume), in recent years has been massively developed to a degree where it is broadly used, specifically in the fields of military (aircraft, helicopters) and telephony and computer gaming/simulation. However, performance indicators like word error rate (short: WER) and real time factor (speed) still vary immensely and cannot be solely relied upon.[49]

There are also other limiting factors such as computer capacity and the "limited number of analysts who can read and assess filtered messages"[50]. In respect to keywords, emphasis must be laid on the problem of the sheer range of topics involved in such a working interception system. Keywords can relate to military security, forms of crime, "trade in dual-use goods", "compliance with embargoes" or economic activities[50]. Taking action in order to narrow down the range of keywords to specific interesting areas "would simply run counter to the demands made on intelligence services"[50].

2.5 Brusa, UKUSA, Five Eyes

The British-U.S.A. (Brusa) Agreement was first secretly signed by the United Kingdom and the United States in 1943, containing an informal plan for the exchange of Signals Intelligence between the two nations. For the first time, it formalized a collaboration of intelligence agencies between the UK and the US to share intelligence information. Shortly after the end of World War II, on March 5th, 1946 the two signed the UKUSA Agreement.[51] This agreement was a representation of a continuous cooperation between the two main forces USA and United Kingdom which can be backdated to the First and Second World War. The Americans incited the establishment of a SIGINT alliance first in August 1940. Some months later in February 1941 a cipher machine (codename: PURPLE) was delivered to the United Kingdom. Afterwards, a code-breaking cooperation started in spring 1941 and continued with success, when the British were able to break the German fleet code (codename: ENIGMA) gaining huge advantage over the enemy's strategic warfare, and decisively affect the course of war[52]. The inclusion of the other three members of the UKUSA Agreement happened with the transfer of SIGINT personnel from Europe to the Pacific in 1945 in participation in the war against Japan. In this regard, an "agreement was reached to provide the Australian intelligence services with British resources and personnel"[52]. As such, intelligence agents returned to the USA through Canada and New Zealand. Finally, a conference produced a top-secret classified agreement, consolidating further detailed arrangements for a SIGINT agreement between the United States and the British Commonwealth. In the following two years further discussions took place until the definitive text of the UKUSA Agreement - nowadays also known as '**Five Eyes**' - was signed, which established a framework for the exchange of Signals Intelligence, now between the five nations United States,

[49] [114]
[50] [185, p.35]
[51] [125, p.370]
[52] [185, p.60]

United Kingdom, Canada, Australia and New Zealand in June 1948[53].

2.6 The communication interception system ECHELON

ECHELON was a communication interception system, which was established in the early 1970s as a global network with the capabilities of monitoring "listening posts and satellites intercepting cables, telephone communications, radio and microwave signals, wireless communications, e-mail, faxes, and other forms of communication traffic"[54]. Law prevented each of the UKUSA members to intercept communications of own citizens, however the exchange of information between each of the intelligence services remained largely unaffected. While the NSA was not allowed to monitor communications within their borders, the British GCHQ could provide them with information very easily. Several ground stations, distributed all over the world on the UKUSA participant's territory have been built to cover a major part of worldwide communication. Countries, which signed 'third-party' agreements participated to an extent in the UKUSA network. Those include Germany, Norway, Denmark and Turkey.[54]

A temporary committee on the ECHELON system was established by the European Parliament on July 5th, 2000 at a trial of the Committee on Citizens' Freedoms of Rights, Justice and Home Affairs on the subject "the European Union and data protection"[55]. Two Scientific and Technological Options Assessment (STOA) (is a department of the Directorate-General for Research of the European Parliament which performs research at the request of committees) studies have been conducted concerning the ECHELON system, one in 1997 and the other in 1999. In both reports the author Duncan Campbell claimed that the NSA intercepted "all e-mail, telephone and fax communications in Europe"[55]. After bringing the topic to public attention for the first time in 1997, the report from 1999 explained further details in a "five-part study of development of surveillance technology and risk of abuse of economic information"[55]. Especially the existing intelligence capacities and the mode of operation of ECHELON have been analysed. ECHELON was described as being used "for purposes of industrial espionage", differing from its former original "purpose of defence against the Eastern Bloc"[56]. The companies Airbus and Thomson CFS were named as two victims, who had been damaged by ECHELON from industrial espionage. The claims on reports were primarily based on American press.

The ECHELON system was characterized as being different from other intelligence systems, having two features making it unique and extraordinary.[57]

1. The first feature enables the user (intelligence service) to carry out total surveillance in a manner that satellite receiver stations and spy satellites are used to "intercept any telephone, fax, Internet or e-mail message sent by any individual" and as such control its contents.

[53] [185, p.61]
[54] [125, p.371]
[55] [185, p.21]
[56] [185, p.22]
[57] [185, p.23]

2. The second feature is the systems capability to be operated worldwide in cooperation among several states (UK, USA, Canada, Australia and New Zealand), which gives it "added value in comparison to national systems".

This way participants in the ECHELON program could share technology, cost and extracted information. Moreover, such international cooperation allowed the "worldwide interception of satellite communications", as only through such global cooperation could be ensured that "both sides of dialogue can be intercepted"[58]. Keeping that in mind, it is emanated from that fact that an even greater number of states participating in ECHELON were aspired. Also, the way ECHELON operated using satellite receiver stations, agreements among the participants of the system are essential, especially because establishing infrastructure on the territory of a state is not possible without its allowance.[58]

Threats to privacy and business outgoing from a system as ECHELON arise not only by its monitoring capabilities, but also by its operability in a "largely legislation-free area"[58]. Residents of the home country are rarely targets of an interception of international communication system. As such, the person affected by the interception (i.e. his/her messages) "would have no domestic legal protection, not being resident in the country concerned"[58].

Based in Fort Mead in Maryland, the NSA was the organization involved the most in the ECHELON "covert surveillance system"[59].

The report[60] on the existence of a global system for the interception of private and commercial communications from July 11th 2001 deals with the subject 'ECHELON interception system' in detail, and gives various indicators on self-protection for companies and individuals, and legal measures on the global and EU levels.

The report states in regard to industrial espionage, that part of intelligence services' tasks is to collect "economic data, such as details of developments in individuals sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc.", all reasons why affected companies are often "subject to surveillance"[61]. Further it says, that US intelligence services are not purely involved in the investigation of general economic facts alone, "but also (do) intercept detailed communications between firms, particularly where contracts are being awarded"[61]. This represents a risk for firms, that their information may be used for competitive intelligence gathering, instead of using it in the fight against corruption, even if officials from the USA and the UK are naturally stating otherwise. However, at the same time, the report states that "no such case [spying on foreign firms for the purposes of gathering competitive intelligence] has been substantiated"[62]. At the time when the report was written, the temporary committee already pointed out, that the risk and security awareness in (especially) small- and medium-sized companies would be "often inadequate", and the threats outgoing from "economic espionage and the interception of communications" would be not noticed. In this regard, it was stated, that due to lack of security awareness in many European institutions, action taking would be necessary.[62]

[58] [185, p.24]
[59] [106, p.453]
[60] [185]
[61] [185, p.13]
[62] [185, p.14]

At that time possible self-protection measures were suggested too, including the introduction of secure encryption systems in order to secure the entire working environment and protect all communication channels.

Neglected propositions

Very interesting to see is that during the 12 years between the report and the beginning of the 'NSA-affair' (cf. Chapter 5) almost none of the actual propositions and 'calls' have been applied. Already in 2001, the analysis from the ECHELON system allowed to derive measures to encourage the self-protection of firms and citizens. Following list shows the propositions, that illustrate the parallels between then and today, and can be easily applied to today's problems in terms of data security[63]:

- The call on the Commission and the member states "to inform their citizens and firms about the possibility that their international communications may, under certain circumstances, be intercepted; . . . ";
- . . . "to develop and implement an effective and active policy for security in the information society;. . . ", to increase awareness and guidelines for viable solutions;
- the urgent need "to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software";
- . . . "to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes";
- . . . "to lay down a standard for the level of security of e-mail software packages";
- the call on the European institutions and the public administrations of the member states "systematically to encrypt e-mails, so that ultimately encryption becomes the norm";
- and to provide training for staff.

All these propositions for better protection are evidently present in today's information society, and if applied properly can greatly reduce the risk of becoming victim of cyber espionage, or the interception of communication in particular.

Overall, the report appeals on the collaboration between member states of the EU, and an open exchange of information on the matter of interception systems between the Five Eyes alliance (especially the USA) and the European nations. The measures proposed are fully understandable and applicable in all firms, who rely on network structures and strive for the unlimited availability of data.

Especially the process of recording and evaluation of communication including phone, fax and email by British and US-American intelligence services triggered waves of criticism after the *ECHELON* program had been openly discussed in public in 2001. Especially considering

[63] [185, p.18-19]

that fax communication was regarded as being safe from surveillance, and ECHELON was in fact capable of infiltrating full communication.[64]

Damage caused by ECHELON

Damage caused by operations involving the ECHELON system is stated to be varying from $13bn to $145bn.[65]

Earlier STOA reports blamed the US for using ECHELON for economic espionage benefiting US companies over other competitors in major contracts on the global market. A thesis, which is backed by former CIA director James Woolsey, who said in an article in the *Wall Street Journal* in 2000 "that the policy of the US government was to use the US intelligence system to spy on European companies in order to level the playing field by gathering evidence of bribery and unfair trade practices"[65].

Alongside the practice of economical espionage there were also indicators, that the ECHELON surveillance and interception techniques have been used for political purposes as well. It is quite likely to assume "that the vast intelligence network of the UKUSA alliance and the sophisticated surveillance techniques offered by ECHELON can be and are often used not only for the purposes of monitoring and detection of national threats but also for the purposes of political control"[66].

Technology behind ECHELON

ECHELON was built and developed on "its own wide-area network (WAN)", similar to today's internet, except the inaccessibility to public traffic[67] . It included several components such as:

- news network 'Newsdealer'
- TV conference system 'Giggle' and others

Similarly to today's web sites and interfaces, a secure system known as 'Intelink', was used by analysts to browse through pages and "select specific geographic areas from which to obtain products ranging from video clips and satellite photos to intelligence and status reports, as well as databases"[67].

Over the years, the technology evolved, especially the computer processing power, until at some point computers were able to filter traffic for the extraction of relevant data purposes. From that time on, systems called 'dictionaries' were used to scan data for particular keywords. As such, global traffic was being scanned by all UKUSA members, individually. Keyword searches were then replaced "by the more efficient method of topic analysis", which utilizes specific principles, very similar to those of 'fuzzy logic', with the aim "to better replicate the selection process that the human itself undergoes," even though at a much slower rate[67].

[64] [125, p.370]
[65] [106, p.457]
[66] [106, p.458-459]
[67] [125, p.371]

ECHELON-type communications interception system and European Union law

When it comes to the compatibility of an ECHELON-type communications interception system with the European Union law, the conclusion in the report was made that an intelligence gathering system like ECHELON was "not in breach of Union law because it does not concern the aspects of Union law that would be required" for it to be incompatible[68]. Nonetheless, this would apply only in the case when the system is "used exclusively for the purposes of state security in the broad sense"[68]. Simultaneously, the report explicitly states that EU law would be violated, if the system was to be used for industrial espionage "directed against foreign firms" or other purposes[68]. If there would be evidence, showing that a member state is involved in a particular action, "it would be in breach of Community law."[68]

Communications surveillance as a violation of the fundamental right to privacy

> *In contrast, in the EU Member States, which are mature democracies, the need for state bodies, and thus also intelligence services, to respect individuals' privacy is unchallenged and is generally enshrined in national constitutions. Privacy thus enjoys special protection: potential violations are authorised only following analysis of the legal considerations and in accordance with the principle of proportionality.*[69]

"Any act involving the interception of communications" by intelligence services, including the recording of data for similar purposes[70], "represents a serious violation of an individual's privacy"[71] . The "unrestricted interception of communications permitted by government authorities" would only be tolerable in a 'police state'[71].

The report further states that the UKUSA members surely are aware of this, but nonetheless their laws' protection would restrict them only from infringing privacy of their own nation's inhabitants. As such, European citizens would "not benefit from them in any way"[71].

The protection of privacy under international agreements

Many international law agreements define privacy as a fundamental right. On the highest level there is the International Covenant on Civil and Political Rights, adopted by the UN General Assembly on 16 December 1966. *Article 17* of the Covenant assures the protection of privacy:

1. *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.*

2. *Everyone has the right to the protection of the law against such interference or attacks.*[72]

[68] [185, p.70]
[69] [185, p.83]
[70] German Federal Constitutional Court (FCC), 1 BVR 226/94 of 14 July 1999, Rz 187: 'The recording of data already represents a violation of that right in so far as it makes the content of the communications available to the Federal Intelligence Service and forms the basis of the ensuing analysis using search terms'.
[71] [185, p.83]
[72] [155]

On EU level, "efforts have been made to establish specifically European arrangements for the protection of fundamental rights through the drafting of a Charter of Fundamental Rights of the EU"[73]. *Article 7* of the Charter states:

> *Everyone has the right to respect for his or her private family life, home and communications.*[74]

This article is explicitly mentioning the important aspect of communications in regard to privacy. Furthermore, *Article 8(1)* of the Charter describes the right to the protection of personal data:

> *Everyone has the right to the protection of personal data concerning him or her.*[74]

The protection is here referring to both computerised and non-computerised processing of personal data, as affected in almost all forms of intercepted communication.

The only effective international instrument for the comprehensive protection of privacy remains the European Convention of Human Rights (ECHR).[75]

In this regard, *Article 8(1)*of the ECHR states:

> *Everyone has the right to respect for his private and family life, his home and his correspondence.*[76]

However, while the "protection of telephony or telecommunications" is not explicitly referenced, "under the terms of the case law of the European Convention of Human Rights, they are protected by the provisions of Article 8", because they are included in the conception of *private life* and *correspondence*[77]. Further it is explained that the "scope of the protection of this fundamental right covers not only the substance of the communication", but the recording of external data as well. As such, in the case when the intelligence service does create records of data, like the duration and time of calls (i.e. metadata), it does represent an actual "violation of privacy"[77]. An interference in the exercise of the fundamental rights to privacy may only be admissible, "if there is a legal basis under national law'[77] In general, the law must be "accessible and its consequences must be foreseeable"[77].

In this regard, the Temporary Committee emphasizes on the unlawful interference "in the exercise of this fundamental right" by the Member States of the EU[78]. Such interference is allowed "only for the purposes listed in" Article 8(2) of the ECHR, notably in the commitment of public safety, national security or the country's economic contented state[78]:

> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic*

[73] [185, p.84]
[74] [66, p.10]
[75] [185, p.85]
[76] [64, p.11]
[77] [185, p.85]
[78] [185, p.86]

society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[79]

Industrial espionage is explicitly excluded in terms of justification of interference.[80] All this proves, that in terms of regulations and the rights of privacy, the interception of communications, like it has been conducted by the Five Eyes alliance with the ECHELON system was contrary to law.

Monitoring of intelligence services

The effective monitoring of intelligence services is a crucial and important aspect of democracies for two main reasons[81]:

1. Intelligence services operate in secret very often on a continuous basis. The entity under surveillance either does gets knowledge of it, long after the events occurred, or doesn't.

2. Intelligence services mostly collect a very extensive range of information from various sources, which can include large amounts of personal data.

In the end, the ones responsible for the monitoring have the problem of identifying "whether all the requisite information has in fact been provided, or whether some details are being held back", due to the very nature of intelligence services' secretly work.[81]

In the ECHELON report there is stated that most of the EU member states have established a "separate parliamentary monitoring committee to scrutinise the activities of the intelligence services"[81]. This includes countries like Germany, Italy, Denmark, Belgium, Portugal and the Netherlands. While the monitoring committee in each of those countries is responsible for both the civilian and military intelligence service, the monitoring committee in the United Kingdom "scrutinises only the admittedly much more significant activities of the civilian intelligence services; the military intelligence service is monitored by the normal defence committee", which shows to be irrelevant in perspective to recent activities of the GCHQ (cf. Chapter 5)[82]. In regard to Austria, the report states that "the two arms of the intelligence service are dealt with by two separate monitoring committees, which are, however, organised in the same way and endowed with the same rights"[82]. In other countries like Finland and Sweden "parliamentary scrutiny is carried out by Ombudsmen, who are independent and elected by parliament"[82]. In countries like France, Greece, Ireland, Luxembourg and Spain there are no explicit mentions of any existing parliamentary committees. As such, it can be concluded that either monitoring bodies do exist in several Member States, but which do not act in an - to the sensitive subject of intelligence service's surveillance activities - appropriate manner. Or there still are no bodies whatsoever, which should be responsible for the supervision of the agencies' activities, which must stay within democratic borders and standards.

[79] [64, p.11]
[80] [185, p.86]
[81] [185, p.92]
[82] [185, p.95]

ECHELON's capabilities of conducting industrial espionage

Whether the ECHELON system was suitable for industrial espionage, the report shows that when it comes to strategic monitoring of global telecommunications, there is a chance that information is collected, which can be of use for industrial espionage purposes. In general, truly sensitive information is mostly kept inside the firm's sphere and the specific use of industrial espionage requires the purposeful breach of the firm's internal computer networks. In the case, however, when information is sent outside via media through means such as cables or radio, a communication surveillance system like ECHELON can definitely be used for industrial espionage. There are three cases named, when this could occur[83]:

- in connection with firms which operate in three times zones, so that interim results are sent from Europe to America and then on to Asia;
- in the case of video-conferences in multinational companies conducted by VSAT or cable;
- when important contracts have to be negotiated locally (construction of facilities, telecommunications infrastructure, rebuilding of transport systems, etc.), and the firm's representatives have to consult their head office.

Naturally, if a firm neglects to take protective measures for any of those cases, sensitive internal information can be intercepted and benefit competitors. In small and medium-sized enterprises in particular the awareness of information security and its linked risks is neglected to a degree that interceptions of communication from outside are not even noticed.

Conclusions taken from ECHELON

The global intercepting communications system code-named ECHELON was undoubtedly in use by a cooperation of the five nations under the UKUSA Agreement. Highlighted is the fact that its main purpose was to intercept commercial and private communications, and not military communications.[84]

In summary, the limits of the interception system include[84]:

- only a small number of communications in dense communication areas are transmitted over satellites
- as such, the majority of communications can only be intercepted by cable and radio signal tapping
- the nations under the UKUSA Agreement have access to a rather limited piece of the whole cable and signal communications
- especially counting in the immense personal and time costs to evaluate the communications thoroughly with given budget and capacities

[83] [185, p.102]
[84] [185, p.133]

As regards to possible existence of other interception systems, evidence also showed that other nations such as Russia and especially France (due to its geographical position and technical capabilities) could use a similar system as long as they dispose of the right funds and locations.

In terms of compatibility with EU law, one has to differentiate between two cases[85] :

1. The system is used for intelligence purposes only - no violation of EU law, because "operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union (CFSP)"

2. The system is misused for gathering competitive intelligence - violation of EU law, because such action "is at odds with the Member States' duty of loyalty and with the concept of a common market based on free competition."

The report also suggested European citizens to begin encrypting their e-mails as a means from protecting their own and maybe their employer's sensitive information. Overall, all results derived from the indicators on the existence and functionality of ECHELON serve evidence that an extensive and wide reaching surveillance system was in use or at least represented plans on future intelligence gathering by intelligence services, in particular those belonging to the members of the UKUSA alliance. Also, various concerns regarding whether ECHELON operated in it's legislative boundaries have been stated and a number of safety measures have been expressed in regard to the protection of sensitive data (privacy, know-how etc.). Taking recent events involving the NSA-surveillance scandal of 2013 into consideration (cf Chapter 5), one can conclude than only very little has been learned and applied from the knowledge gained from the ECHELON disclosure in terms of regulations on an (inter-)national level. In the end, ECHELON was a harbinger of what would be possible in the sphere of SIGINT and of a global surveillance system, that is capable of industrial espionage and efficient intelligence gathering beyond belief.

2.7 Insurance companies advance to new markets

'Cyber-insurance' is a term, which got a lot of attention in recent years. Companies fear the loss of their know-how and sales and as such seek pre-emptive measures, besides eventually improving the IT-infrastructure's security. While the German market still is quite small, the demand for 'Insurance policies' in the US is increasing, reaching a premium volume of cyber insurances of 800 Million Dollar in 2011, and counting. At the moment there are only 5 foreign providers of special products including HISCOX, CHUBB, XL, CNA and AIG[86]. The tendency that only the US is affected by cyber attacks is clearly changing. A cyber-insurance consists of several components. In Germany insurance companies offer such clauses as options, integrated in the policies. Cyber-insurance focuses on the insurance protection in case of the loss of personal data or confidential data that a company manages, stores, processes or transfers. In addition the insurance comprises potential crisis management costs or eventual payments undertaken to blackmailers. The new insurance is modular, so that the insurance protection can be compiled individually. It can also secure third-party claims due to data privacy infringements, as well as

[85] [185, p.133-134]
[86] [97]

forensic activity costs and even data recovery costs. It is presumed that the market for this kind of new insurances will expand in the following years further.[87]

2.8 NSA and its assignments

The NSA plays a huge role, when it comes to analysing global intelligence gathering activities in today's internet age. Therefore, it makes sense to include a bit of background information on its establishment and development over the years.

The NSA was secretly established in 1952 by Harry S. Truman - US president at that time - with the main assigned area of carrying out US SIGINT and Communications Security (COMSEC) activities. Since 1957 the NSA's headquarters have been at Fort George G. Meade, Maryland. In regard to the definition of Communications Intelligence (COMINT), the controlling National Security Council Intelligence Directive (NSCID) states: "[COMINT] shall not include . . . any intercept and processing of unencrypted written communications. Press and propaganda broadcasts, or censorship."[88]

Naturally, NSA field stations collect various communications signals such as e-mail, fax or telephone intercepts around the globe, which are then sent to Fort Meade for analysis. Results of this analysis are then also forwarded and presented to other agencies (e.g. Defense Intelligence Agency (DIA), CIA). Personnel-wise, the NSA employs a mix of military personnel and civilians.[88]

Since 1952 many operations including *MINARET* and *SHAMROCK* have been practised in the fields of political espionage intercepting electronic communications, which at this point shall not be addressed in more detail. Several recommendations to hold the Agency accountable for their actions had no substantial effects. One recommendation "contributed to the establishment of the Foreign Intelligence Surveillance Act (FISA) of 1978 which created the Foreign Intelligence Surveillance Court (FISC) to which requests were to be made to authorise electronic surveillance and physical search[88]. The FISC issued about 500 FISA warrants per year from 1979 to 1995, and then slowly increased them until 2004 when some 1758 were issued."[88]

The NSA's commitment on utilizing the powers of the internet resulted basically from its main task to intercept radio signals and telephone communications. At first, the internet was just another electronic medium. Later on, after the internet's fast growing and expansion the interest in the internet's capabilities increased respectively. The NSA with its academics and electro engineers as such developed to the worldwide leading organisation of virtual operations.[89]

An article from the *Observer* newspaper published on March 2nd, 2003 contained a leaked NSA memorandum, dated January 31st, 2003. It described a US-developed "aggressive surveillance operation, which involves interception of the home and office telephones and the e-mails of UN delegates"[90]. The memo's main purpose was to win votes in favour of war against Iraq.[91]. Despite the importance of the *Observer* report, it got almost no attention in media.

[87] [39, p.25]
[88] [106, 459]
[89] [48, p.66]
[90] [106, 460]
[91] [106, 461]

Under the premise 'war against terror' the US allowed the NSA to both develop and expand their programs with a great emphasis on the fields of spying and surveillance. The government allowed the intelligence agencies to "use events such as the bombing in Oklahoma City, attacks on the World Trade Center in New York, and the bombings of the American embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya, to justify the continued monitoring of people and organisations around the world"[91]. Systems like ECHELON have been operated successfully, monitoring thousands domestic and international communications.

US officials argue that:

> *The United States has never aspired to be a country where the state continually spies on its citizens and is not accountable to them for its actions, in fact the Constitution goes to some lengths to limit the powers of government and protect the rights of individuals in this respect. However, there are always difficulties when a country is in a state of war or siege. The state and/or military are then often tempted to justify a temporary loss of civil liberties in exchange for a general feeling of increased national and/or personal security.*[91]

This passage is referring to the events of 9/11 that interrupted the United States' balance and led it to a more aggressive course.

How the events of 9/11 affected US authorities

The events of 9/11 made the world power United States of America vulnerable, which enforced the government to take drastic actions. Just a few days after the September 11 attacks, the Justice Department lawyer, John Yoo, called attention:

> *. . . that the government might use electronic surveillance techniques and equipment that are more powerful and sophisticated than those available to law enforcement agencies in order to intercept telephonic communications and observe the movement of persons but without obtaining warrants for such uses. [. . .] while such actions could raise constitutional issues, in the face of devastating terrorist attacks the government may be justified in taking measures which in less troubled conditions could be seen as infringements of individual liberties"*[92]

which should become first a first act to take drastic measures, even if it results in the intrusion of privacy. With the vast technological development the internet became a platform which appeared perfectly suitable for applying spying and monitoring techniques. Especially considering the fact that in terms of regulations the relevant area (IT) of legislation is to this day partially controversial (e.g. data retention, copyright, connection data).

An example for the arbitrariness of action-taking by US government officials is illustrated, when in late 2001 President George W. Bush issued a secret executive order "authorizing the NSA to conduct phone-taps on anyone suspected of links with terrorism without the need to issue warrants from a special court, as required by the Foreign Intelligence Surveillance Act"[92].

[92] [106, 462]

Unfortunately, this programme of surveillance became only public in December 2005, published by the *New York Times*. This article also stressed that: "The previously undisclosed decision to permit some eavesdropping inside the country without court approval was a major shift in American intelligence-gathering practices, particularly for the NSA, whose mission is to spy on communications abroad", which shows again the extensive reactions the events of 9/11 have caused, even though partially understandable, because of the impact the incidents have caused on that day in 2001[92].

It is evident that both, practices and capabilities of the NSA have created scepticism and deep irritation from foreign nations, but also US citizens. Despite various indications on NSA's violation of domestic and international law, US officials keep justifying the authority's activities as "being necessary to acquire information about threats to national security, international terrorism, and the narcotics trade."[93] The strong level increase of knowledge and applications in various fields of technology, especially in computer science and electronic communications have "heavily influenced the way that procedures and techniques have developed in the 'second oldest profession" to a degree where IT-infrastructure is being exploited regularly in very effective ways[93]. This resulted in a core problem, where there is a huge gap between the advances in technology and legal structures, which protect the rights of individuals and institutions. As such it comes down to the question whether today's societies are capable of responding and dealing with the new challenges that they are confronted with increasingly in recent years, especially since the publications of Edward Snowden in June 2013 (cf. Chapter 5). And, whether people can change the course from Orwell's 1984 prophecies, back to a state where privacy is respected according to a democratic governance.

After 9/11 the Bush administration in secret allowed the NSA domestically to collect large amounts of e-mail records. The legal basis for that 'bulk collection' comes under section 215[94] of the 2001 Patriot Act, interpreting it as an allowance to "collect phone metadata in the US", which would mark the first step of legitimate intelligence gathering[95].

[93] [106, 463]

[94] ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

[95] [26]

CHAPTER 3

Cyber Spying

3.1 USA's view on world cyber security issues

The events of 9/11 trigged decision makers in the US to become more prepared in the fight against terrorism with the cost of giving up civil liberties in order to increase the nation's security. This meant a more drastic approach of utilizing global network resources that the internet provided. Governments, the one of the US in particular, are seeking to control the internet and monitor communications, which ultimately can result in espionage activities. The government saw itself forced to take action in order to protect not only physical infrastructure, but also the digital cyberspace, which experienced increasing threats from hostile opponents. Today, national security and economy both depend upon information technology and the information infrastructure, the internet in particular, which also connects millions of different computer networks. Vulnerabilities in the infrastructure which clearly exist create threats of organized cyber attacks. Due to the fundamental problem of achieving protection of critical infrastructure systems from attacks by removing vulnerabilities, and at the same time mitigating the effects of the attacks forced the government to let institutions responsible for national (cyber) security take drastic proactive measures.[1]

A recent US governmental announcement to prioritise the fight against cyber-criminality and industrial espionage over internet suits the new harsh approach. Hacker attacks in special cases are supposed to be retaliated with trade sanctions, provided one can identify the perpetrator.[2]

3.2 Increasing industrial espionage over the internet

Already in early 2009 the German Office for the Protection of the Constitution (BfV) expressed concerns about the increasing threat potential of industrial espionage to companies and governmental authorities. In particular, intelligence services form China and Russia, as well as

[1] [106, p.449]
[2] [54]

countries from Near, Middle and Far East, and North Africa are presumed to be actors behind espionage attacks. One concluded from the methods applied and from the target types that it is very likely that the work was done by or on behalf of intelligence services. The location and the large number of leading-edge technology would make Germany a "very attractive" target[3]. They also referred to recent events of espionage activities over the internet, specifically the events of summer 2007 are mentioned when computers of the Federal Chancellery, Ministry of economy and research, and the foreign office were infected by trojans. Hackers from the Chinese Peoples Liberation Army were suspected to be behind those attacks[3].

Having said that the German Office for the Protection of the Constitution repeatedly requested especially medium-sized companies to take action in developing / installing better protection technologies against cyber espionage. Emphasized is especially the need of a closer cooperation between security authorities and companies. According to Heinz Fromm, former president of the German Federal Office for the Protection of the Constitution the only way to improve the defensive work is through getting sufficient and accurate information about hacker attacks and indicators of espionage from the economy [4].

3.3 UN's input on Internet surveillance

In a report[5] titled 'The use of the Internet for terrorist purposes' and published in October 2012 the United Nations addresses the importance of more surveillance of internet users, explaining it would be necessary for better investigations and thus potential prosecutions of terrorists. The report refers to social sharing sites like Facebook, YouTube, Twitter and Dropbox, which are being extensively used for spreading propaganda. The internet would be used by potential terrorists who act in anonymity and at low cost. In conclusion it says that "one of the major problems confronting all law enforcement agencies is the lack of an internationally agreed framework for retention of data held by Internet Service Provider (ISP)s", referring to Europe's enactment of "mandatory data-retention law"[6].

In reaction to the potential arising threats in recent time, the report suggests to keep records of communication in instant messaging services such as Skype. Other discussed topics addressed in the report include[6]:

- Cell phone tracking
- Open Wi-Fi networks
- Video games brutality
- Financing companies for surveillance

Instead of dealing with the extent, nature and potential of the threat of cyber attacks by terrorists, the report discusses the way how the internet makes terrorist activities possible and

[3] [211]
[4] [51]
[5] [151]
[6] [138]

more specifically how it can be misused for such purposes. The report is rather a justification of reasons that governments try to proclaim as necessary, including the adjustment of laws. Accordingly the close cooperation between governments and law enforcement authorities is suggested: "Recommended measures to be taken by law enforcement authorities pursuant to the guidelines", including cooperation with ISPs, their assistance and "prioritizing requests for large volumes of data while avoiding unnecessary cost and disruption of business operations"[7].

3.4 International Cyber Espionage activities

Chinese industrial espionage

Already in 2009 the BfV pointed out that espionage activities over the internet from Chinese intelligence services have dramatically increased in the past years, posing a great threat for German infrastructure such as the national electricity grid. According to Walter Opfermann from the department of counter-intelligence the financial risk potential in Germany amounts for around €50bn each year. Furthermore, he says that primarily small and middle-sized companies would represent preferred targets due to their high level of innovativeness and poor security equipment. He also appeals companies to raise following questions[8]:

- Where do I employ personnel with specific backgrounds?
- When do I close IT-accesses of employers during the stage of termination?

Preventive action is necessary, but it is difficult to act against online espionage attacks, especially if there is no cooperation with Chinese authorities.[8]

ThyssenKrupp and EADS as targets

In mid 2012 "massive" attacks of "special quality" were directed at the German industry concern ThyssenKrupp[9]. The only published information was about the whereabouts of the attack (USA), and that the IP-addresses have been identified as of Chinese origin. Victims of similar attacks are also named, including the major enterprises Bayer and IBM. Again, information on affected systems or data was not mentioned.

In early 2013 information leaked out about cyber attacks on computer systems of the aerospace group EADS. Officially, the attack was described as 'standard', while damage numbers were kept secret. Still, the attack had such an impact forcing the company to notify the government. Mentioned are especially e-mails as the source of malware.[9]

Other Chinese espionage activities

Chinese cyber espionage campaigns seem to hit primarily targets which are linked to military technology. In 2011, Chinese hackers have attacked the network security company RSA secu-

[7] [151, p.132]
[8] [143]
[9] [1]

rity. The “technology stolen” provided the hackers to “penetrate military-industrial targets”[10] And this vulnerability was exploited shortly after on Lockheed Martin’s security systems. Even Google had announced in 2010 about having become victim of ’intrusions’ coming from China. For all companies one main problem of cyber espionage is represented by it’s invisibility, which makes companies unable to act.[10] Besides companies, computer systems of government agencies and research institutions are targeted by cyber espionage, according to the Office of the National Counter Intelligence Executive[11], the institution responsible for the topic of national espionage threats in the US, causing damage of “tens of billions of dollars of trade secrets, technology and intellectual property”[12].

Targeting US-weapon systems

Another case of involving US weapon systems became public in late May 2013, when Chinese hackers were involved in a cyber espionage operation, which eavesdropped on about two thirds of large US-weapon systems. According to a confidential report from the Defense Science Board prepared for the Pentagon, the hackers seeked technical details on fighter jets, helicopters and missile systems (complete list: [13]). According to published information, the attacks were specifically targeting this sort of information on US technology. Details on the date or which companies or computer networks have been specifically affected, were not mentioned, though it is presumed, that the acquired information can be used to improve the development of Chinese weapon systems.[14]

Drone technology

One of China’s espionage targets is the advanced drone technology of the US. A particular operation, is called ’Beebus’, which can bee seen as yet another APT and was traced back to a C2 node at “bee.businessconsults.net”, an address associated with the the ’Comment Crew’. For years a Beijing based Chinese hacker group systematically searched for findings on information of US drones, targeting top aerospace and defence organizations in particular. Small and large US companies were similarly targeted.[15]

The targets are rather unusual, namely US drone technology. According to a *New York Times* article, the hackers had focused on a wide range of companies, first specializing on large companies that are particularly active in the fields of aviation and space technology, then moved on to more specialized smaller companies, which deal with the development of technologies for unmanned aerial vehicles. Confirmed have been attacks on at least six major enterprises, and at least 20 companies in total, over the course of almost two years, what also could be the largest campaign that focused drone technology to date. The group executing the attacks is

[10] [147]

[11] http://www.ncix.gov/

[12] [144]

[13] http://www.washingtonpost.com/world/national-security/a-list-of-the-us-weapons-designs-and-technologies-compromised-by-hackers/2013/05/27/a95b2b12-c483-11e2-9fe2-6ee52d0eb7c1_story.html

[14] [146]

[15] [67, p.14]

called 'Comment Crew', which is correlated to be connected to the Chinese hacker unit 61398 (see 4.1).[16]

It comes to no surprise that the Chinese government could have strong interest in drone technology. For quite some time, the country has been developing own drone models, including a flying machine called Yi Long[17], which is strongly reminiscent of the predator drone from the US military.

China's focus on drone technology by means of cyber espionage is understandable. Drones are the next future technology that can be used both for surveillance as well as for military operations involving the killings of criminals, but can also be used in conflicts with areas of Xinjiang and Tibet. According to a statement of Ian M. Easton, a military analyst: "cyberespionage was one tool in an extensive effort over years to purchase or develop drones domestically using all available technology, foreign and domestic"[18]. The attack itself took place by infiltration techniques such as phishing and using attachments with malware with variations of PDF (Adobe) and Microsoft Word exploits.[18]

US investigations on threats by Chinese telecommunication companies

On November 17th, 2011 the House Intelligence Committee launched an investigation on "national security threats posed by Chinese Telecom companies working in the U.S."[19]. Named are the two large Chinese Telecom companies Huawei and ZTE, who are known for making smartphones. In the document concerns are expressed for the use of critical infrastructure against the U.S. emphasizing the threat of foreign industrial espionage by the Chinese government. The review of the investigation was supposed to give knowledge on whether mitigation measures to ensure the security of the U.S. telecommunications network needed to be further developed. Former Ranking Member as a prosecutor, Mr. Ruppersberger said:

> *We already know the Chinese are aggressively hacking into our nation's networks, threatening our critical infrastructure and stealing secrets worth millions of dollars in intellectual property from American companies. This jeopardizes our national security and hurts U.S. competitiveness in the world market, costing our country countless jobs. The same way hacking can be a threat, vulnerabilities can derive from compromised hardware on which our telecommunications industry rely. The purpose of this investigation is to determine to what extent Chinese communications companies are exploiting the global supply chain and how we can mitigate this threat to our national and economic security.*[20]

Prior to this event in October 2011, a report from the Office of the National Counter-Intelligence Executive was published and contained accusations about "foreign spies stealing US economic secrets in cyberspace" with an emphasis on espionage by Russian and Chinese

[16] [213]
[17] [129]
[18] [213]
[19] [154, p.1]
[20] [154, p.2]

authorities [21]. Information from the Federal Bureau of Investigation (FBI), CIA and the NSA indicated that both countries would be the most aggressive collectors of US economic informations and technologies. According to the report hackers are instructed by governments to obtain data from industries for the purposes of enhancing economic growth in their own country. The report also calls attention on threats of data loss through the ways of either the large number of Russian migrants in US technology companies or the increasing number of US factories in China, which in fact are natural consequences of globalisation. The report further mentions publications of secret reports which leaked by the actions of WikiLeaks or LulzSec. The authorities fear more leaks of important plans such as US weapon systems in the near future.[22].

The scepticism against Chinese companies led in recent years to breakdowns of planned takeovers from US companies due to security concerns of responsible committees (e.g. Huawei & 3Leaf Systems)[23].

Australian company reports cyber attack from China

In May 2013 it was discovered that the Australian Security Intelligence Organisation (ASIO) headquarters in Canberra have been victim to a cyber attack, presumably by Chinese Hackers, who acquired secret blueprints containing valuable intelligence on security and IT system layouts. One very interesting thing, which explains the lack of disclosing hacker attacks and keeping as much information away from the public as possible, is stated by Federal Attorney - General Mark Dreyfus: "The more that is disclosed about what's known about espionage activity in Australia or operational aspects in counter-intelligence, the more that our opponents, people who are engaging in espionage, will know about our capability and know about the methods that we have for detecting espionage or cyber threats."[24] That's basically the very reason this topic needs to be handled in the public and why security firms who analyse and derive valuable information from the results are so necessary in today's information age. Undoubtedly it is a risk for companies disclose information on cyber attacks. To ensure that the incidents are regarded confidential within the cooperation with authorities, first the appropriate legal requirements must be created. Reporting incidents such as cyber attacks must be handled as sensitive information, so that 'opponents' as mentioned above will not able to get the information in the first place. In addition, the risk of reporting requirements could force companies to invest in preventive security measures from the beginning, which would be desirable.

Chinese counter-espionage

Who does the US-government eavesdrop on? To find answers to that question, Chinese hackers occasionally steal data sets containing valuable intelligence from Google. In 2010 the hackers seeked to find out, if the US-government monitors Chinese spies, who work in the US in cover. Allegedly, the data contained information, which had been collected for several years. At the same time, Microsoft had also been victim of a similar attack. Companies like Google and

[21] [156]
[22] [142]
[23] [203]
[24] [16]

Microsoft, which are based in the US, are favoured targets, due to their popular and free e-mail services such as GMail and Outlook, and other web-based services (e.g. Cloud, Social), because those companies have high market shares and possess large volumes of personal data, that could be exploited by hackers.[25]

Dummy infrastructure yields excessive cyber attacks

During an experiment of the Japanese IT-security company Trend Micro, when a water-pressure control system of a pumping station was being used for simulation purposes, 39 cyber attacks over a one-month period have been observed targeting the ICS/SCADA systems of the station coming from 14 different countries. These numbers prove also, that espionage is an international problem, because the attacks originated not only from China (35%), but also from the US (19%).[26] The honeypot architecture was built realistically to represent a real station as accurately as possible, including weakly secured systems with the usual vulnerabilities. The attacks utilized a "number of malware exploitation attempts on the servers", primarily attempting to get remote access to the ICS/SCADA systems[27]. Other attacks were efforts to gain as much information as possible (statistics, logs etc.). During the observation period, the same attackers also came back to retry the intrusion by using other methods and techniques.[28] This particular example illustrates how infrastructure became a valid target of persistent perpetrators of cyber espionage and shows how this sector needs a great deal of attention when it comes to security.

Verizon report indicating industrial espionage

Verizon, an US mobile communications provider, published a report named 'Data Breach Investigations Report'[29] in April 2013. It contains statistics and results of investigations done during 2012 regarding security threats to data. In total, 47.000 reported security problems were factorised into the study and 44m records were compromised. The report explicitly states that off the large amount of reported security incidents, almost all statistics and charts relate "to the 621 'breaching' leading to confirmed data disclosure"[30]. As such, the report shows that off those 621 analysed breaches, 20% go back to state-affiliated actors using methods of cyber espionage targeting intellectual property. Of those, a Verizon analyst explained whole 96% of cases the cyber espionage attacks were coming directly from China. In respect to the high number he also said that it may be some sort of coincidence that the data chosen as a sample contained that much of Chinese origin. But surely it can also mean that China is in fact deeply involved in industrial espionage worldwide.[31] While many attacks were targeting organizations involved in the fields of finance, the analyst showed surprise when the investigation revealed that there was a "fifty-fifty split between the number of large organizations and small organizations that experienced breaches related to cyber espionage"[31]. Initially, the researchers suspected big companies

[25] [145]
[26] [210, p.10]
[27] [210, p.11]
[28] [210, p.12]
[29] http://www.verizonenterprise.com/DBIR/2013/
[30] [204, p.11]
[31] [50]

containing large amounts of intellectual property to be spied on the most. This proves once again the importance of higher security standards for small and mid sized companies, because the lack of protection is the weakness the attacker knows about and tends to exploit. The analyst believes "that they pick the small organizations because of their affiliation or work with larger organizations", which of course may also be the case[31]. Companies in the fields of manufacturing, transportation, information technology, and professional services appear to be the ones which are the most common victims, even considering the rather small sample size of 120 incidents (cf.[32]).

In comparison to cyber espionage, financially motivated cyber crime of all data breach incidents appeared to be responsible for whole 75 percent, followed by hacktivists with 5 percent. This shows proof once again, how cyber espionage has evolved in recent years; however, the high number of financially motivated attacks might indicate, that this particular example of cyber espionage is not state-affiliated, but rather the work of hackers. In regard to the small percentage of hacktivists (e.g. Anonymous) it should be noted that they mainly act out of ideological motives, which are difficult to separate. In the end, the report indicates that "much of the activity claimed by these actors in 2012 shifted to other forms such as denial of service (DoS) attacks", strengthening the assumptions taken from recent events in 2012/2013[33].

Additionally, in 52% of the cases some sort of hacking was used. 40% involved malware, 35% direct physical attacks, followed by "social tactics like phishing" (29%)[34]. Another important indication the report gives, is the targeting of valid credentials for accessing networks by basically all threat actors. This is of course to this day a problem, which can only be reduced by two-factor authentication, which is slowly spreading. Single-factor password-based authentication had always its weaknesses, and the more people are using the internet, the more risks arise that this method, especially when passwords are poorly chosen, needs a (security) update. According to the report about 80% of hacking attacks targeting passwords, would be forced "to adapt or die"[35].

Figure 3.1 illustrates a good overview of origin, target and the used types of tools, confirming the overall assumptions about each of the data breach threat actors. It comes to little surprise that phishing attacks are described as having increased fourfold in just one year (2011-2012).

While the big majority of total breaches are credited to external actors, 14% are a result from internal actors, taking information to a new employer (HUMINT).[36]

Malware being undoubtedly one of the most effective and used tools in espionage operations as per report is accountable for 40% of all total breaches (not only espionage) and as Figure 3.2 illustrates is mainly distributed two ways, through direct instalment or coming as an e-mail attachment (mostly in an archived format). The report also states one should "keep in mind that these vectors are not mutually exclusive"[37]. As such, "in many cases, an actor may gain initial entry using a malicious e-mail attachment, and then install additional malware on that and other systems throughout the environment", which is also very true, as is shown in chapter 4[37].

[32] [204, p.15]
[33] [204, p.21]
[34] [204, p.6]
[35] [204, p.34]
[36] [204, p.23]
[37] [204, p.34]

	ORGANIZED CRIME	STATE-AFFILIATED	ACTIVISTS
VICTIM INDUSTRY	Finance Retail Food	Manufacturing Professional Transportation	Information Public Other Services
REGION OF OPERATION	Eastern Europe North America	East Asia (China)	Western Europe North America
COMMON ACTIONS	Tampering (Physical) Brute force (Hacking) Spyware (Malware) Capture stored data (Malware) Adminware (Malware) RAM Scraper (Malware)	Backdoor (Malware) Phishing (Social) Command/Control (C2) (Malware, Hacking) Export data (Malware) Password dumper (Malware) Downloader (Malware) Stolen creds (Hacking)	SQLi (Hacking) Stolen creds (Hacking) Brute force (Hacking) RFI (Hacking) Backdoor (Malware)
TARGETED ASSETS	ATM POS controller POS terminal Database Desktop	Laptop/desktop File server Mail server Directory server	Web application Database Mail server
DESIRED DATA	Payment cards Credentials Bank account info	Credentials Internal organization data Trade secrets System info	Personal info Credentials Internal organization data

Figure 3.1: Overview of the three main data breach causers (reprinted from [204, p.22]).

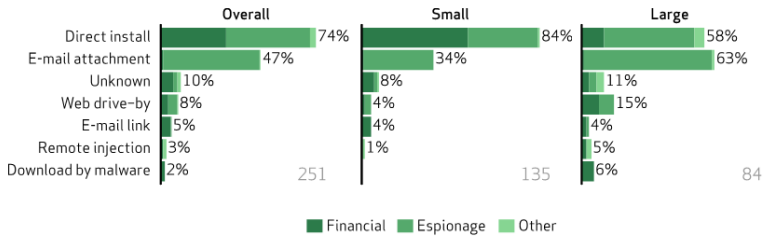


Figure 3.2: How malware is initially distributed (reprinted from [204, p.29]).

In terms of which malware component or combination is used in the end, the report suggests that there is no real specific one, but rather a variety of them, indicating that "state-affiliated actors often use the same formula and pieces of multifunctional malware during their campaigns."[38] In numbers regarding the variety of malware cf. figure 3.3.

[38] [204, p.30]

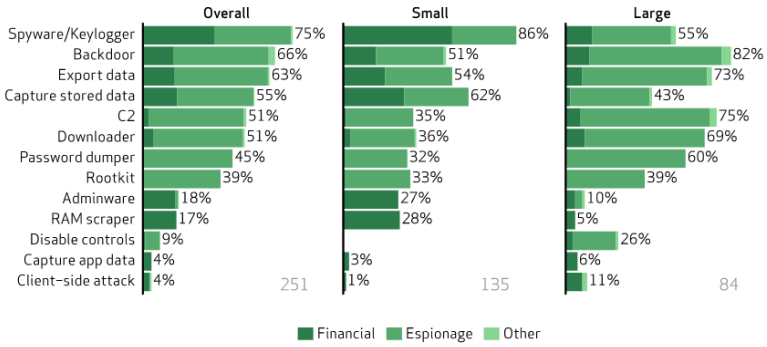


Figure 3.3: Variety of malware components (reprinted from [204, p.30]).

Phishing

Phishing is illustrated as a very effective tool in espionage operations, due to the fact that it simply works. While naturally phishing e-mails often vary in quality they serve the same purpose, namely to get the user's attention and action. According to the report "running a campaign with just three e-mails gives the attacker a better than 50% chance of getting at least one click"[39]. Running it twice increases the probability "to 80% and sending 10 phishing e-mails approaches the point where most attackers would be able to slap a "guaranteed" sticker on getting a click"[39] (on average one of 20 e-mails is guaranteed to yield a successful 'catch'). Moreover, it takes 12 hours on average for the user to take action, opening the attachment or link. But, there is also the factor of 'dependence' on the whole process yielding the result the threat actor seeks. The dependence between the steps leading to a successful compromise, meaning the system has to be vulnerable in the first place, the software must be installed unnoticed and the communication back to the attacker via C2[40] has also to work. While, of course most state-affiliated phishing methods include highly sophisticated and adaptable malware, and as such this will not very likely appear to be a problem, it is still interesting to see how probable and thus effective this method in espionage operations has become.

While threat actions besides malware, hacking and social (phishing) are also analysed in the report, espionage-wise they have very insignificant influence (including categories such as Misuse, Physical, Error, and Environmental). Not surprisingly in terms of the number of breaches in specific areas, the report shows credentials, system (information), internal (organizational data), and (trade) secrets as the four main targeted objects, preferred by spies.

The report also shows the problem of late discovery. Most 'breaches' (66%) are discovered months (mostly espionage related) or even years (4% of total, espionage alone accountable) after they have compromised the systems. Another point in relation to this is that 69% of incidents are discovered externally, instead of inside the company. After 92% of breaches discovered externally in 2011, the number went down to 69% in 2012, which still is excessively high,

[39] [204, p.38]
[40] *C2 refers to command and control (C&C).*

indicating the clear lack of internal detection capabilities. External institutions include "ISPs, Information Sharing and Analysis Center (ISAC)s, and intelligence organizations"[41]. Basically, all of the espionage cases were discovered by external - to the company unrelated parties - in contrast, for instance to financial cases, where fraud detection, customers and law enforcement represented the majority.

In conclusion, evidently neither phishing nor brute force attacks on passwords are new tools. It's the company's neglect, that to this day attacks utilizing such techniques remain being effective. And the sheer high numbers regarding the discovery time and how they are made show two of the most important challenges to both, the security industry and management. While prevention is undoubtedly necessary, the timely detection and response are at least on the same level of importance regarding defence. All in all, the data provided by the report shows very interesting and clear indications on how espionage has developed in terms of which technology was used, and which assets have been targeted. However, the information should still be viewed with a portion of scepticism, considering recently disclosed documents, among others involving companies like Verizon, by Edward Snowden (see Chapter 5).

Evolving cyber espionage techniques

While most of the cyber espionage operations targeting specific employees in corporations have been utilizing the method of spear-phishing e-mails with an attachment carrying malware, in 2012/2013 a change has been observed to other means of exploitations, namely in browser plug-ins and web browsers.[42] One technique is called the '*watering hole*' attack, when a targeted individual clicks on a link to a specific infected website.

Watering hole attack

During a watering hole attack, the hacker first observes his target's online behaviour. Then, he selects a website with a particular vulnerability and compromises it by injecting HTML or JavaScript (which loads a compromised e.g. flash file), so that the targeted victim is redirected to another site the next time he tries to visit the original; "like a lion waiting at a watering hole"[43]. The separate site can host all kinds of different exploit code, depending on the "chosen vulnerability" and as such infect the target with a 0-day exploit[43]. Further procedure would include the attacker gaining access to the compromised computer. Here education of employees is required, so that they can be aware of such a new form of cyber attack.

3.5 Internet surveillance in Russia

Security services in Russia can use surveillance on telephones and internet without any court order approval. A national interception system called System of Operative Search Measures (SORM) is primarily in use by the country's main security service, the Federalnaja sluschba

[41] [204, p.53]
[42] [158]
[43] [159]

besopasnosti Rossijskoj Federazii (FSB) since 1996. First, it was established to monitor telephone communications, including mobile traffic, until two years later it was complemented by SORM 2, allowing to monitor the internet, including Voice over IP (VoIP) as well. There is also the recently developed SORM 3, which collects data from all communication media and stores it for a duration of three years. With SORM, authorities can also use mobile control points, enabling them to use instant interception and recording of the operator's traffic, directly after plugging-in a device (e.g. laptop) containing the program into communication hubs. Russia's Supreme Court stated that over the course of five years the number of telephone intercepts had doubled, reaching 466.152 intercepts in 2011 including e-mails.[44] While, by law in the US and Western Europe, a warrant is required in order to enforce network operators and ISPs to get to requested data, in Russia, "an FSB operative is also required to get an eavesdropping warrant, but he is not obliged to show it to anyone"[44]. As such, there is no obligation to the FSB to give evidence on a valid warrant to Telecom providers.

> *In short, the Russian approach is far more flexible and intrusive than the Western one: if the FSB needs to add new phone numbers or e-mail addresses to the intercept list, it does not need to repeat the whole procedure, as in the West. The FSB just updates the requirements list in the SORM control device, known as a Punkt Upravlenia, or PU.*[44]

Countries such as Ukraine, Kazakhstan, Belarus and Uzbekistan all have very similar systems. In Ukraine for instance, SORM even allows "to interrupt the conversation", which is of course an even greater intrusion and violation of democratic principles[44].

While its focus is to spy on the country's political protesters and opposition leaders (which is shown continually in recent years) and to support the president's influence and stability, SORM is definitely used for regular surveillance purposes, including all fields of modern communication. It is presumed that Russia's approach of sharing technology with former client states is strategy, which is supposed to help in a joint development to keep for instance social media under surveillance.

3.6 BND and surveillance

In 2011 the Bundesnachrichtendienst (BND) had strategically intercepted almost 3 million telecommunications, invoking Article 10 (cf. [45] - Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) and the anti-terrorism act (cf. [46] - Terrorismusbekämpfungsgesetz). The number of intercepted telecommunications can be divided into three justifying fields, 'international terrorism' (329.628 E-Mails & telephone conversations, from which only 290 '0.01%' were identified as being relevant), 'proliferation and conventional armament' and 'illegal locking'. That's about one interception every 5 seconds. Filtering out of the specific targets was done with the help of the usual method using over 10.000 keywords.[47]

[44] [190]
[45] [6]
[46] [157]
[47] [140]

After Edward Snowden's discoveries, it also became known that the BND to some degree has been cooperating with the NSA. For instance, the NSA provided the BND with several analytical tools for eavesdropping on foreign data streams that ran through German territory. The focus of the BND amongst others was the Middle East route, which serves as a route for data flow through crisis regions. [48]

Another factor in providing intelligence to the US is the fact that the US by law is allowed to monitor data in Germany. American intelligence services can invoke eavesdrop operations in Germany on legal bases, which date from the former German Federal Republic. According to administrative arrangements of 1968, the Western Allied intelligence services are allowed to request 'reconnaissance measures' from both BND and BfV, who have to pass raw data. This results in a direct right of Americans to access German intelligence (data). Until 2012, the agreements were classified as secret. According to the German federal government they are still in force, but haven't been taken up since 1990. Presumably, the collaboration between US intelligence services and BND are regulated by several letters of intent, which to this day are classified as top secret. In addition, former Federal governments have assured the Americans the rights to take 'adequate safeguards' in cases of imminent threats of their armed forces. This includes the right to collect communication.[49]

According to research done by *Der Spiegel* in August 2013, the BND presumably transfers great amounts of metadata from their monitoring system - a BND location in Bad Aibling - to the NSA.[50]

Germany's role in intelligence gathering

Hans-Georg Maaßen, president of the BfV, in connection with the NSA affair in an article for the *Handelsblatt* had rejected recently voiced economic espionage allegations against the US and Great Britain. According to him, the danger would come from the East (referring to Russia and China in particular), and that the BfV has "no knowledge that could support the theory of economic espionage in the West" and that "in fact, to this day throughout Europe, not a single case of American or British economic espionage has been demonstrated"[51,52]. Thus, there would be no reason to question the close collaboration with the US and Great Britain.[52]

The suspicion of industrial espionage by North Atlantic Treaty Organization (NATO) allies already has grown in connection with the ECHELON system (cf. Chapter 2). Then, shortly after the recommendation of the parliamentary committee the Bad Aibling station was closed. Also, in 2000 former CIA chief James Woolsey had openly admitted in the Wall Street Journal that after the collapse of the Warsaw Pact, the ECHELON activities had shifted to industrial espionage (see [53]). This serves as a clear indicator on Germany's long-time cooperation with

[48] [23]
[49] [96]
[50] [13]
[51] [58]
[52] Original: „Uns liegen keinerlei Erkenntnisse vor, die die These einer Wirtschaftsspionage aus dem Westen stützen könnten. Tatsächlich wurde bis zum heutigen Tage in ganz Europa kein einziger Fall amerikanischer oder britischer Wirtschaftsspionage nachgewiesen." (2013-08-27)
[53] http://cryptome.org/echelon-cia2.htm

other intelligence services, in the fields of intelligence gathering, SIGINT in particular.

3.7 British plans of building a new military cyber unit

According to reports from the *Daily Mail* the British government wants to invest about €600m into establishing a new unit for cyber warfare. British defence minister Philip Hammond describes it "as the biggest military revolution since tanks replaced cavalry brigades in the First World War a century ago"[54]. The 'cyber army' would be necessary to be able to react for foreign critical cyber attacks on British infrastructure. Also, he said: "Future wars would be fought by 'IT geeks in rooms like this rather than soldiers marching down the streets, or tanks or fighter aircraft"'[54]. Britain would already have "a defensive cyber military force to fend off cyber attacks by terrorists and others[54]. It will now develop an attack force in conjunction with GCHQ spy chiefs."[54] British intelligence agency GCHQ will also work in close collaboration with the military unit. The authority already operates a Cyber Security Operations Centre - and evidently works in close contact with the NSA. This illustrates how internet capabilities are energetically being used, to prepare for war scenarios and how the different spheres of defensive and aggressive cyber operations begin to merge.

3.8 Austria develops cyber 'militia'

According to minister of defence Gerald Klug, it is about the protection of sovereignty for the republic (Austria)[55]. Austria is in the process of establishing a cyber militia, which is supposed to deal with aspects of cyber security. The Bundesheer will besides the tasks of 'Katastrophenschutz' and 'Auslandseinsätzen' make this field as the central point of their new security strategy. From 2014 on, 'Grundwehrdiener' will be able to pick a training module for the protection of the internet, which includes the prevention of espionage, industrial espionage, terrorism and the threats to infrastructures from hackers. Klug wants the Bundesheer to cooperate with other authorities as well. How the increase of control and security on the internet is compatible with the increased data protection, was not mentioned.[56]

3.9 Mobile malware on the rise

According to statistics from Kaspersky Lab, the Android Operating System (OS) is in the leading position, when it comes to being a cyber-criminal's target of choice. All mobile malicious code samples that were discovered, were targeting Android (in Q2 2013), having breached 100.000 mobile modifications ("consisting of 629 malware families"), an over 50% increase compared to 2012[57]. The distribution of the particular malware species is as follows[57]:

- Backdoors (32.3%)

[54] [207]
[55] Es geht um den Souveränitätsschutz für die Republik.
[56] [3, p.4]
[57] [74]

- Trojans (23.2%)
- SMS-Trojans (27.7%)
- Spy-Trojans (4.9%)
- Others (12.0%)

It comes to little surprise that Android is the most, if not exclusively, targeted Mobile-OS. Android amounted 81% of global market share in Q3, 2013, followed by iOS (12.9%).[58] Besides the increasing popularity of Android, another reason for it - being primarily targeted - lies in the degree of control that providers have about their products, as well as the development and distribution of applications. For instance, Apple's Walled Garden App Store, where apps are fully checked on their security before being published, has prevented a majority of malware infections on iOS. Also, iOS shows considerably less security gaps, than its main rival, due to the fact that Apple doesn't provide iOS developers access to Application Programming Interface (API)s.[59]

3.10 Visualization tools

In order to visualize the amount of cyber attacks on networks, the German telecommunications company Telekom launched a website called http://www.sicherheitstacho.eu. According to them, up to 450.000 attacks a day would be registered on their systems. Statistics show the attack types, which countries are affected and where most attacks come from. Interestingly enough, the United States (815.000) leads with double the amount in front of the United Kingdom in terms of 'source countries', followed by Germany and China (statistics taken for the month of September 2013). It should be noted, that source countries can use the technique of bouncing through 'hop point' systems before accessing the victim systems (see 4.1) and thus hide the real attacker's country of origin. For the same month, most attacks were on the SSH protocol, which can be used for establishing an encrypted network-connection between two systems.[60]

When hacked data become publicly available, such as customer data including e-mails, logins etc., one can always presume that activists or other hacker groups have been behind the attacks, but almost never intelligence services of countries, due to their specifically targeted area of interest.

Another tool for visualization is offered by the website http://apps.opendatacity.de/prism/en, which shows how "Internet packets wander around the Internet cables". Therefore, some of the most popular services like Amazon, Google, and Skype are used to illustrate which countries are visited by the data packets (and therefore a possibility of intercepting that communication is given). Figure 3.4 shows a request from Germany (you can also select Switzerland or France) to access Facebook.

[58] [11]
[59] [35]
[60] [38]

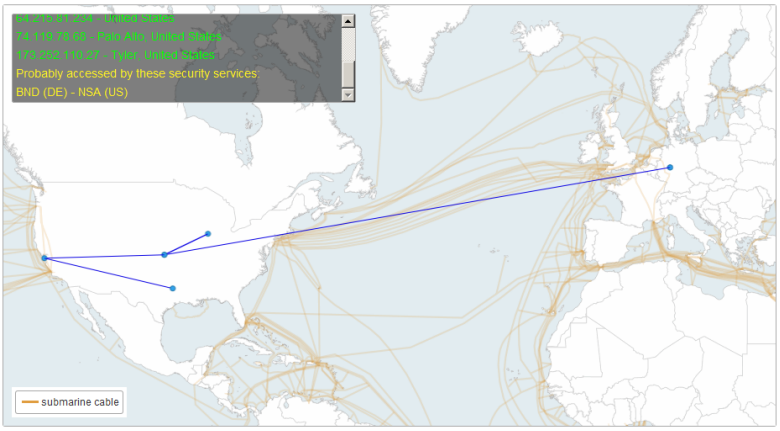


Figure 3.4: Data packet flow across submarine cable routes

Google's malware statistics

As a result from recent events involving hacker attacks and governmental surveillance, Google launched a website, which shows statistics about malware (see [61]). Named 'transparency report', the website provides information on "criminal requests and national security requests from government's worldwide", as well as numbers from malware and phishing attacks that were registered on the internet. On average the system is flagging about 10,000 sites a day. In particular, it documents "how many people see its security warnings each week, where malicious sites were hosted around the world (and by which Internet Service Providers), how long it took for Web masters to clean up their sites, and – somewhat depressingly– how quickly Web sites got re-infected after they were scrubbed of malware"[62]. As of October 21st, 2013 the percentage of scanned websites, which host malware in Germany alone was 5%. Research and analysis is done with the help of so called autonomous systems, which consist of either one or more networks, which again are operated by legal persons (companies, universities, ISPs); such autonomous systems are a part of the network layer in the Internet infrastructure. According to Google, this data should help to improve security on the Web, also by encouraging other institutions to cooperate in the fight against malware.[63]

3.11 Outlook

According to a report from October 2011, the US National Counterintelligence Executive predicts, that there will be accelerations in the changing rate in "information technology and communications technology"[64] in the near future (up to 5 years), driven mainly by 4 factors, affecting

[61] http://www.google.com/transparencyreport/safebrowsing/
[62] [161]
[63] [21]
[64] [156, p.6]

and potentially disrupting various security procedures in the US and which create openings for collecting economic and technology information. Those 4 factors are described as[65]:

1. Technological shift, referring to the fast growing technology market (with powerful devices like laptops and smartphones with internet connectivity/remote access) and its increase of software & hardware diversity and complexity, which will threaten the safety of sensitive information.

2. Economic shift, describing the security problem of data becoming available (cloud computing) at any time and from any place throughout all the different organisation forms, which will increase "opportunities for theft or manipulation".

3. Cultural shift, indicating the shift in the mindset of working individuals regarding expectations of privacy and work, and how the increase in flexibility (being online) results in an increased possibility of theft.

4. Geopolitical shift, referring to the ever growing globalization and how with it boundaries become blurred, because business can be done from anywhere in the world.

All these factors add to the difficulty to defend privacy and sensitive resources in the 'jungle' that is the internet. In this regard Rig Ferguson, director of security research and communication from Trend Micro emphasized:

> *The reason why criminals are focusing their attacks on stealing personal data is simple. It's the sheer volume of people working from multiple devices that leaves them vulnerable to attacks.*[66]

It is presumed that China, Russia and other cyber espionage actors will continue with their thrive for closing the gap of economic and technological power - in particular to the US.[67] It is also to be expected that the role of non-state and non-corporate actors will grow, due to the "migration of most business and technology development activities to cyberspace", which allows for economic espionage without the need of enormous resources[68]. These actors can then operate as direct "surrogates or contractors for intelligence services" or companies[68]. Naturally, hackers hired by intelligence services or criminal organisations, and hacktivists are also included in the group of (possible) threatening actors conducting cyber espionage activities. Hacktivists like Anonymous have shown recently, that they possess powerful resources, which ultimately could be used "to disclose sensitive information as a means of expressing dissent against" a private company or a government[69].

[65] [156, p.6-7]
[66] [158]
[67] [156, p.8]
[68] [156, p.10]
[69] [158]

CHAPTER 4

Programs

4.1 Programs and operations indicating state-affiliated cyber espionage

Over the course of the last two to five years several new sophisticated malicious software computer programs have been discovered by various security companies. In the following chapter some of the most famous and hazardous ones are discussed and their capabilities of conducting espionage illustrated.

FinFisher

FinFisher is a surveillance software program which belongs to the malware group of trojans. The software is developed and marketed by the company Gamma International GmbH, which is a member of the British Gamma Group of Companies [1]. The spy tool was initially developed for intelligence services and police authorities. Besides FinFisher, the company, specializing on security, offers a wide range of tools for the purposes of eavesdropping and surveillance. The commercial intrusion kit FinFisher, or rather its part FinSpy, became known as an often used tool used by several countries, including amongst others Australia, the Czech Republic, Egypt, Estonia, Ethiopia, Indonesia, Latvia, Mongolia, Qatar, the UAE, and the United States[2].

First exposition and detailed technical analysis of FinFisher was done in summer 2012 by Citizen Lab - an interdisciplinary laboratory based at the Munk Centre for International Studies at the University of Toronto, Canada - upon obtaining versions of the surveillance software by Vernon Silver of *Bloomberg News* [3]. Several months prior the exposition, the malware was used by infecting devices of Bahraini democracy activists in order to transmit their communications to authorities of Bahrain. Also, democracy activists in Washington and London belonged to the

[1] [100]
[2] [10]
[3] [135]

list of targets. Evidence on it being actually a FinSpy product is given through several strings such as 'finspyv4.01' and 'finspyv2' contained in infected processes. The analysed trojan was sent to selected activists through e-mail. After opening the attached image files a trojan has been installed on the hard disk bypassing virus scanners and crashing debuggers. Once infected, the software would record data including screenshots, passwords, Skype recordings and sent files. This data would then be encrypted and transmitted to a server with the IP Address *77.69.140.194*, which as shown in the analysis belongs to the biggest telecommunication company in Bahrain. At the time of the software's exposure nobody of Gamma was willing to comment on it.

Although companies like Gamma or DigiTask[4] always tend to defend their work as being developed for intelligence services to help hunting down criminals, the actual example shows, how political activists also are targeted on purpose, without being Bahraini citizens, by just being in Bahrain at that time or without any knowledge of being part of investigations by authorities. Human rights organizations like the British Privacy International demand export prohibitions for such surveillance technologies for several years, including commencing legal action against the British government, but dialogues are very slowly going and do not bring the desired effects.[5]

FinFisher in detail

Citizen Lab used several different approaches during the investigation of the malware. A Virtual Machine (VM) was first infected with the malware and then the file-system, network, and running operation system was monitored and analysed. The initial (infecting) email contains a typical notification about topics (e.g. reports of torture) pointing to the attachment file for further information. The '.rar' (WinRar[6]) attachment file contained "executables as picture files or documents"[7]. The image files itself, according to the Citizen Lab analysis, were labelled with 'righttoleftoverride' (RLO) characters, "containing characters flowing from right to left, such as Arabic or Hebrew"[7]. The malware infected file would appear as for instance '*exe.Rajab.jpg*', which would in reality be a file having a UTF-8 based file name '*gpj.bajaR.exe*', which as such can only be displayed through ANSI-code[8]. By clicking the file, the file executes as an '.exe' file instead of the appearing '.jpg' file and the trojan is installed. After that the attacker gets remote access to the victim's machine, which can be used to harvest and withdraw data. In the background several folders are created, copies of files created, renamed, and system processes infected. Citizen Lab states:

> *Examining the memory image of a machine infected with the malware shows that a technique for infecting processes known as 'process hollowing' is used. For example, the memory segment below from the 'winlogon.exe' process is marked as executable and writeable.*[9]

[4] Developer of the German 'Staatstrojaner'
[5] [59]
[6] http://www.rarlab.com/
[7] [135]
[8] American National Standards Institute
[9] [135]

Important system processes like 'svchost.exe' and 'winlogon.exe' are infected and persistence is enabled, so that in case of reboot the malware remains intact.

In terms of resisting analysis and evading identification, the malware uses several techniques such as a virtualized packer and anti-debugging. Moreover, the malware actively goes through the list of running processes and modules for traces of an installed Anti-Virus (AV) software. The process then appears to be hidden from each different AV solution.

In regard to the actually data harvesting process and the encryption method used by the malware the following can be mentioned[10]:

- data is stored locally
- while being hidden and encrypted
- having a naming scheme similar to:

  `C:\Windows\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}`

- wide range of data collected includes "screenshots, keylogger data, audio from Skype calls, passwords and more"
- data is collected in a file with a similar naming scheme similar to 't111o00000000.dat' in the same folder
- the writing process was held by the infected process 'winlogon.exe'[11]

The examination of this file revealed the contents as being screenshots of the system's desktop. In case of a file transfer through Skype, a '.tmp' file is created and after it is written to the disk, a new '.dat' file is created and encrypted accordingly. Regarding audio Skype conversations, very similarly a standard windows module 'dsound.dll' is accessed and the sound feed directly copied to the same '.dat' file.

In order to disguise the harvested data in the '.dat' files encryption, more precisely AES-256-CBC (with no padding) is used. According to the analysis by Citizen Lab, a highly predictable AES key structure is used:

The "predictability of the AES encryption keys" allowed the team to decrypt and view the records in full plain-text[12].

The malware communicates by connecting to the server IP address '77.69.140.194', talking to the remote host on five different TCP ports (22,53,80,443,4111). As already mentioned, this IP address belongs to "Batelco, the principal telecommunications company of Bahrain"[12].

In conclusion functionality comprises[12]:

- Bypassing 40 frequently tested AV systems
- "Covert communication with headquarters" & remote access

[10] [135]

[11] Standard Microsoft Windows process handling user profile loading / signing-off

[12] [135]

- Complete Skype Monitoring
- Live monitoring / recording of Audio (Microphone) & Video (Webcam) sources
- Common communication (e-mail, chat, VoIP) recording
- Tracing the target's whereabouts
- Filters to record only essential information
- Covert extracting of files from hard disk drive
- Key-logger (process-based)
- Supporting common operating systems (Windows, Linux, Mac OS)

In regard to the 'Bahraini' FinSpy program, Martin Johannes Muench, CEO of GAMMA International in Munich defended his software as necessary to find criminals and to "save lives"[13]. Besides, the acquired FinSpy version would have been just a sample for demonstration purposes, but nevertheless the company's workers did have a modified version of the spyware with changed characteristics, which was sent to all customers in form of an update.[13]

Of course, FinFisher can and definitely has been applied outside Bahrain, but the basic functionality and infection process remains the same, and shall illustrate how surveillance and intelligence gathering tools generally work from start (sending an e-mail to specific target) to finish (control the system via C&C).

BKA acquires FinFisher

According to a secret document in January 2013 it became known that the Bundeskriminalamt (BKA) has acquired FinFisher/FinSpy trojan programs.[14] After using a trojan by a company called DigiTask[15] the German government is eager to develop his own trojan. This task is managed by the recently established Kompetenzzentrum für informationstechnische Überwachung (CC ITÜ). The costs of this project amount to 3 million Euro offering 30 new positions. The BKA seeks to complete this project called *self development of a software with source-telecommunications surveillance* ('die Eigenentwicklung einer Software zur Quellen-Telekommunikationsüberwachung') until the end of 2014. Until then, according to the BKA, the commercial trojan program by the company Elaman/Gamma should be used[16].

[13] [188]

[14] [141]

[15] The DigiTask trojan program fell into dispute when the Chaos Computer Club (http://www.ccc.de/de/updates/2011/staatstrojaner) - an association of hackers - revealed that the program was capable of doing more than actually permitted by law.

[16] [141] German original quote: Das BKA hat, für den Fall eines erforderlichen Einsatzes ein kommerzielles Produkt der Firma Elaman/Gamma beschafft.

Information provided through presentation slides

On August 30th, 2013, the security company F-Secure Corporation[17] had published secret information (provided through brochures and presentations) containing new information on the FinFisher and other "attack tools"[18]. The slides contain information on the history and background of FinFisher and other tools. Gamma International states there, that 'Backtrack' was officially the most used "intrusion tool worldwide" with over 4 Million downloads, which started the main research process on other products[18].

FinUSB Suite

The FinUSB tool uses a conventional USB stick as the source of infecting computers. By plugging in the USB stick containing the software, data can be extracted covertly from target systems. As the typical operations public systems (with quick forensic analysis only running for 20-30 seconds) and target systems (using sources that have physical access to automatically extract intelligence; data is fully encrypted) are named.[18]

FinIntrusion Kit

The FinIntrusion Kit provides the user with a range of features. Wireless Local-Area-Network (LAN)s (802.11), as well as Bluetooth devices can be discovered and Wired Equivalent Privacy (WEP) (64 and 128bit) pass-phrases can be recovered within only 2-5 minutes. Further, it can break both, Wi-Fi Protected Access (WPA)1 and WPA2 pass-phrases using so called dictionary attacks. Also, it can emulate the Rogue Wireless Access-Point (802.11) and monitor the wired and wireless LAN and even extract usernames and passwords, even if the used sessions are already SSL/TLS-encrypted. As examples the typical applications are named such as GMail, Facebook and Hotmail. Another ability of the FinIntrusion Kit is breaking into e-mail accounts "using Network-, System- and Password-based Intrusion techniques" fully remotely. As the typical operations, wireless networks (traffic, username, and password recording and encryption breaking) and access remote systems (gain access to e-mail accounts, web servers and remote infrastructures) are named. As such, a user's online banking credentials can be stolen rather easily.[18]

FinFly USB

FinFly USB features a hidden backdoor, deployed from USB, which can "infect switched off target systems", even if "the hard-disk is fully encrypted with TrueCrypt". The installation is supposed to be automatic through a bootable system. The execution of the backdoor is either automatic (Windows 2000/XP) or one-click (Windows Vista/7) depending on the operating system.[18]

[17] www.f-secure.com
[18] [104]

FinFly Web

The FinFly Web tool features “drive-by-infections” (malware installation upon visiting a particular website) of browser modules, supporting all common browsers (IE, Firefox, Safari, Chrome, Opera). It “supports generation of stand-alone websites to infect targets where only e-mail address or username inside a discussion board is known”. Modules can be integrated by local ISPs into popular sites like YouTube and GMail. Even if the user visits a (to him) trusted site, the infection takes place.[18]

FinFly ISP

This mechanism involves injecting the malware ’remote monitoring solution’ hidden as downloads and software updates respectively directly through the ISP. It can also be remotely installed “through websites visited by the target”.[18]

FinSpy Mobile

This is a tool to infect operating system running mobile phones with malware. This would include basically any major OS, such as Windows Phone, Android, iOS and BlackBerry. According to f-secure this malware would be the first one known for the Windows Phone OS. Other features include full encryption of all communication and all temporary files, the option of surveillance of the BlackBerry Messenger, the abilities of “recording of incoming and ongoing e-mails”, “live surveillance through silent calls”, “basic communication interception like calls, SMS/MMS and call logs”, as well as (GPS/Cell ID) location tracking.[18]

Considering the presentation slides being produced for marketing purposes it is still unlikely that all features do work without a hitch. Taking into account that ISPs are central connection nodes between millions of computers and the internet, it is only logical from a intelligence service point of view to inject spy malware through them, directly providing a wide range of possible ’victims’.

All these tools reveal how it would be easily possible to access the contents of a - by the user - locked computer during, for instance a house search without the user’s notice. Today, USB sticks can be almost inconspicuously small. Even if the user actively refuses to give out a TrueCrypt key, the features the tools provide indicate it may still possible to get to the data. The next time the user would start the computer, all relevant data during a login process including passwords and other sensitive information would be recorded.

In August 2012 Citizen Lab reported about several samples which appeared to be versions of FinSpy mobile with a detailed analysis on its functionality (running on all common OS). The FinFisher product involves some form of interaction from the user to execute and install the program. Its capability is to forward phone speeches, SMS, and e-mails, access the microphone, download files and track the position of the user, everything in secret. Control servers were identified as being located in following countries: “Bahrain, Brunei, the Czech Republic,

Ethiopia, Indonesia, Mongolia, Singapore, the Netherlands, Turkmenistan, and the United Arab Emirates (UAE)".[19]

China's cyber operations

The US security company Mandiant released a report in 2013, containing detailed information on cyber espionage activities (in the report referred to as the APT [20]) mainly originating from China. Over the course of 6 years Mandiant had investigated hacker attacks on 141 companies and organisations worldwide. The majority of the attacks came from a specific district of Shanghai, China. While China's ministry for foreign affairs neglected any accusations concerning China's governments involvement in that matter, the report shows otherwise, in any case, the inability to handle criminal actions of such large extent in the strongly monitored IT-sector of the country. The report describes 4 main indicators of Chinese origin[21]:

- Documented attacks show Chinese IP Addresses from which the attacks came from. More specifically most IP Addresses belonged to China Unicom, one of the biggest ISPs of the country, whereas another part belonged to China Telecom. Both are state-owned. They also could trace back the traffic to Shanghai's district Pudong New Area in 98,2% of the cases.

- In most cases the operator's keyboard layout setting was 'Chinese (Simplified) - US Keyboard'[22,23].

- The observed hackers had enormous technical resources of their disposal including thousands of servers and a sizeable IT staff dedicated to handle maintaining the computer infrastructure and create individually customized e-mails, which included instructions to visit a manipulated website. What becomes interesting in regard to the hacker's objectives is the fact that the methods applied did not include particular tools to make money or finance their operation (e.g. no spam, bribes, fraud was used). Most of the data acquired included hundreds of terabytes of documents, court records, and e-mails from IT-companies, law offices, and companies involved in the sectors of energy and construction. Data, which is mostly valuable if you have the resources, meaning experts that can properly analyse and filter it. This would perfectly suit the interest of governments.

- Obvious is the fact that Unit 61398[24], which is responsible for technical reconnaissance and the interception of telephone and internet communications is located in the same district of Shanghai, the Pudong New Area.

[19] [136]

[20] [133, p.2]

[21] [127]

[22] Microsoft's Remote Desktop client configures this setting automatically based on the selected language on the client system. Therefore, the APT1 attackers likely have their Microsoft operating system configured to display Simplified Chinese fonts.

[23] [133, p.4]

[24] In 2011, according to Chinese experts of the US-Thinktank project 2049, the Unit 61398 was responsible for technical reconnaissance in the US and Canada.

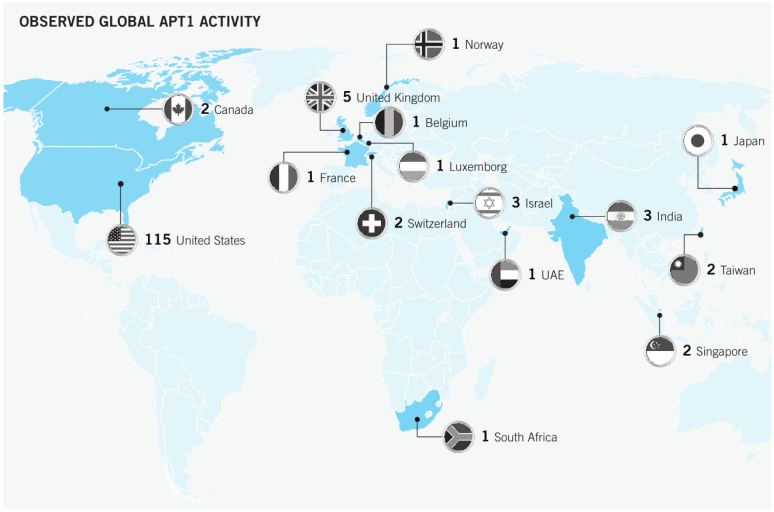


Figure 4.1: Geographic locations of APT1's victims (reprinted from [133]).

It is quite natural that a state seeks control over its ISPs, which can provide the government access to large resources of information. In particular, the amount of resources available to the hackers gives to believe that a close connection between the hacker group and the government exists, especially considering the duration of the operation(s) lasting for several years.

The key findings described in the protocol include[25]:

- APT1's use of utilities for stealing e-mail (GETMAIL and MAPIGET).
- APT1's maintained access to the networks for avg. 356 days (longest being 1.764 days).
- Stealing 6.5 terabytes of compressed data from a single organization over a ten-month period.

During two years (Jan. 2011-Jan. 2013), "1,905 instances of APT1 actors logging into their attack infrastructure from 832 different IP addresses with Remote Desktop" have been confirmed.[26]

According to Mandiant, 87% of APT1 victims were located in primarily English-speaking countries.[27]

As shown in figure 4.2 the cyber espionage operations do not concentrate on specific industry sectors, but rather cover a broad range of industries to gather information from, over a longer period. "The dots within each bar represent the earliest known date on which APT1 compromised a new organization within the industry."[28]

[25] [133, p.3]
[26] [133, p.4]
[27] [133, p.21]
[28] [133, p.23]

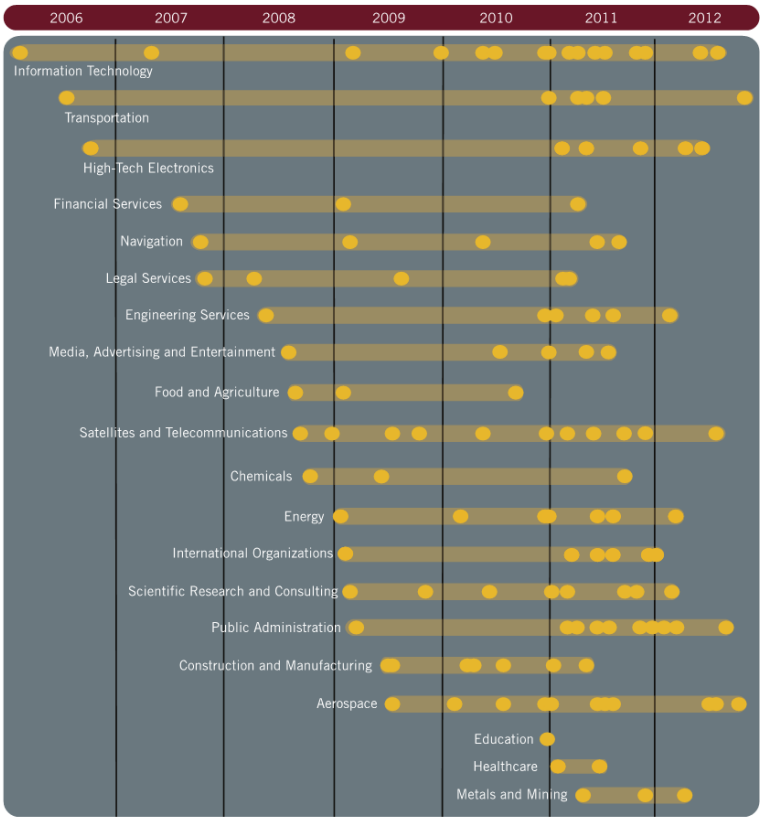


Figure 4.2: APT1's cyber espionage operations against organizations by industry (reprinted from [133, p.22]).

Stolen information includes a wide range of different types of information, from system designs, product manuals, parts lists, manufacturing procedures, standards, business plans, product pricing, and many more. But e-mails, user credentials, and network architecture information were also affected. In general, is is difficult to name accurate numbers regarding stolen data, because APT1 had the ability to delete compressed archives, and the "pre-existing network security monitoring rarely recorded or identified the data theft" and in the end the time between data theft and Mandiant's investigation was rather long.[29]

Structure of an attack on the example of APT1

Initially, the popular method of a 'spear phishing e-mail' was used, sending it from a free web mail service containing a fake text (in most cases in well written English) and a malicious ZIP file (e.g. Oil-Field-Services-Analysis-And-Outlook.zip), which after being opened contains an executable backdoor that in the report is referred to a categorized WEBC2 family (e.g. 'WEBC2-

[29] [133, p.25]

TABLE', or 'WEBC2-RAVE')[30]. The file names include a wide variety of industries including military, diplomatic and economic themes. In rare cases suspicious e-mail recipients answered to the sender for verification purposes, if the contents of the '.zip' file are legal and clean. Someone of ATP1 responded within several minutes with a confirmation, which indicates a rather high amount of human resources available to handle such e-mails individually. Very similar to the FinFisher malware, the infected executable inside the ZIP file is masked as a PDF file with a PDF icon. In reality the file name includes over 100 spaces after '.pdf' followed by '.exe'. Upon executing the file the backdoor is installed for remote access. Furthermore, "in almost every case, APT backdoors initiate outbound connections to the intruder's Command & Control (C2) server"[31]. This tactic is mainly used in order to bypass network firewalls, which generally "adept at keeping malware outside the network from initiating communication with systems inside the network", whereas they are less reliable when it's the other way around[31].

The report describes two category-types of utilized backdoors: 'Beachhead Backdoors' and 'Standard Backdoors'.

Beachhead Backdoors are categorized by the following features:

- Usually minimally featured (simple tasks such as retrieving files, triggering execution or gathering basic system information).
- Designed to retrieve a web page from a C2 server.
- Contents between HTML tags or HTML comments are then interpreted as commands.

New variants of WEBC2 have been continually released for several years, which gave Mandiant the assumption to believe that APT1 had direct access to developers. ATP1 attackers have a set of commands at their disposal once the backdoor was successfully installed, including the download and execution of a file, sleep (inactivity for a specified time) and the opening an command shell (such as cmd.exe on Windows systems). This backdoor type is often used within spear phishing e-mails.

Whereas **Standard Backdoors** are categorized as follows:

- More extensive standard non-WEBC2 APT1 backdoor.
- HTTP protocol or a custom protocol is used, uniting with regular web traffic.
- Victim's system is controlled by a variety of methods.

Figure 4.3 illustrates a standard subset of remote commands characteristic of most backdoors, not only used by APT1.

In order to cover communications between the backdoor and their C2 servers from network defenders such as firewalls, a couple of backdoors use the technique of mimicking protocols to blend with internet traffic. Two examples involve mimicking the MSN Messenger (backdoor

[30] [133, p.31]
[31] [133, p.30]

Command	Description
bdkzt	Launch a command shell
ckzjqk	Get system information
download <file>	Transfer a file from the C2 server
exe <file> <user>	Launch a program as a specific user
exit	Close the connection and sleep
lists <type>	List servers on a Windows network.
ljc	Enumerate running processes and identify their owners.
sjc <PID>|<NAME>	Terminate a process, either by process ID or by process name.
upload <file>	Send a file to the C2 server
zxdosml <input>	Send input to the command shell process (launched with "bdkzt").

Figure 4.3: A list of common commands on the example of the BISCUIT backdoor, utilized by APT1 (reprinted from [133, p.33]).

name: MACROMAIL) and the GMail Calendar (backdoor name: CALENDAR). In addition to that, many of APT1's backdoors have even the ability to "use SSL encryption so that communications are hidden in an encrypted SSL tunnel"[32]. APT1 also used a number of publicly available 'privilege escalation tools' such as *fgdump*[33], *gsecdump*[34] and many other in order to dump user credentials (e.g. login & password) for accessing restricted resources within the network.[35] In regard to internal reconnaissance, the commands such as those shown previously are remotely executed through a command shell or batch scripts (for automation). Data results (lists containing information on network configuration, processes, accounts, network connections etc.) are then written to a typical text file.

As soon as the intruder has access to the victim's system, he can "move around the network undetected"[36]. Shared resources can be connected to, as well as commands on other systems can be executed to infect further systems and networks using new backdoors on multiple systems. Provided the hacker gets his hands on legitimate Virtual Private Network (VPN) credentials access to the whole network can be granted, because VPNs are in most cases only single-factor authentication protected. With the victim's credentials web portals such as web-based e-mail systems (e.g. Outlook Web Access) can be entered without the victim's notice and for an extended amount of time.[36] Files of interest (like screenshots or text files) are packed into password protected archives (e.g. RAR files, which also can be split into several parts) and then sent via File Transfer Protocol (FTP) or via existing backdoors.

According to the report, unlike other APT groups "APT1 uses two email-stealing utilities" making them specifically unique[37]. "The first, GETMAIL, was designed specifically to extract email messages, attachments, and folders from within Microsoft Outlook archive ('PST') files" (with the ability to steal emails with a specific range of dates), whereas the other MAPIGET

[32] [133, p.33]
[33] http://www.foofus.net/fizzgig/fgdump/
[34] http://www.truesec.se
[35] [133, p.34]
[36] [133, p.36]
[37] [133, p.38]

"was designed specifically to steal email that has not yet been archived and still resides on a Microsoft Exchange Server"[37].

Infrastructure

At first it may be a good idea to block any IP address from China trying to establish a connection to your network. Unfortunately, APTs attackers such as APT1 have the ability to easily "bounce through intermediary systems such that they almost never connect to a victim network directly from their systems in Shanghai"[38]. With the sheer size of resources available through their infrastructure, they are able to make attacks appear coming from almost any point of the world. The report describes this technique of network redirection as 'hop points' or 'hops'. These 'hops' often "belong to third-party victims who are compromised for access to infrastructure", instead of victims "who are compromised for their data and intellectual property."[38]. The attackers use a C2 user interface to issue commands to the victim's infected system. The communications between the backdoor and the C2 server are "forwarded from the hop to the intruder's Shanghai system"[38]. According to the report a large number of instances "in which APT1 intruders used the publicly available 'HUC Packet Transmit Tool' or HTRAN on a hop" could be identified. HTRAN is a utility that functions as a mediator, "facilitating connections between the victim and the attacker who is using the hop point"[39].

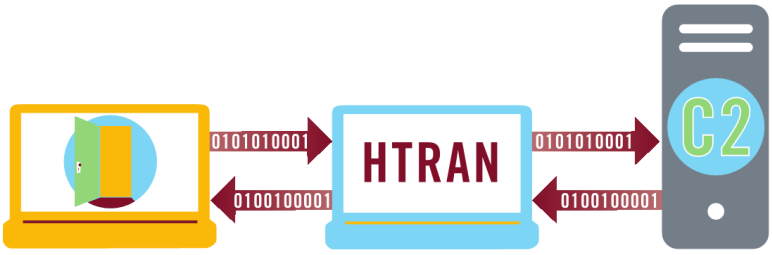


Figure 4.4: HTRAN tool as 'middle-man' residing on APT1 hop points (reprinted from [133, p.41]).

The attacker uses HTRAN by specifying the IP address of his own location and port, which listens for incoming connections. An example of a typical command is:

```
htran -tran 443 58.247.242.254 443
```

Port 443 would listen for connections on the 'hop' and "automatically proxy them to the Shanghai IP address" on the same port.[40]

In the years 2011 and 2012 alone, Mandiant was able to confirm 937 actively listening and communicating APT1 C2 severs running on no less than 849 distinct IP addresses registered

[38] [133, p.39]
[39] [133, p.40]
[40] [133, p.42]

to 709 organizations in China, followed by 109 in the US. They consider hundreds or even thousands of other servers, aside those which were confirmed.

As shown from both FinSpy and ATP1, clear similarities in the technical approach can be seen.

Stuxnet

Stuxnet - a threatening (one of a kind) sabotaging malware - became popular when a malware infection of an Iranian nuclear plant had been discovered in July 2010. The sophisticated malware was special, because for the first time its purpose was to infiltrate industrial computer systems. So called SCADA (monitor and control of industrial processes) systems running 'SIMATIC WinCC' or 'SIMATIC Siemens STEP 7' software were affected in facilities like power plants, gas pipelines or those responsible for water treatment. For this, the malware uses a number of different vulnerabilities in systems operated by Windows OS, infecting through USB-drives and open network shares. The malware has a root kit component which keeps hidden from malware detection systems as soon as the system has been infected. Similarly to other malware programs, this one was also controllable remotely by the hacker, giving him full control over the respective system and facility.

The security company Symantec created a white paper with a full analysis of Stuxnet. The technical term is W32.Stuxnet, indicating the targeted category of the malware being Windows application programming interface for developing 32-bit[41] applications. Stuxnet is described as a "large and complex threat" and its goal being to "reprogram industrial control systems [...] by modifying code on programmable logic controllers (PLCs)" to make it work hidden by the attackers' intentions[42]. The goal is achieved with the help of several components, including a Windows root-kit, zero-day exploits, the first ever PLC root-kit, techniques for evading AV detection, peer-to-peer updates, network infection routines, a C2 interface, and complex process injection and hooking code. Stuxnet evidently existed at least one year before it was discovered.

What's interesting about Stuxnet is also the fact that the PLCs are "often programmed from Windows computers not connected to the Internet or even the internal network"[43]. Also, it is unlikely that the targeted industrial control systems were "connected to the Internet"[43]. Prior the actual attack the attackers need first the ICS's schematics to understand the special configuration, which then again need to be stolen or provided somehow (e.g. HUMINT, or through previous Stuxnet / other malware versions). Afterwards a unique Stuxnet version would be developed and tested in a mirrored environment, which would work specifically to reach a goal by sabotaging the ICS. In the report it is presumed that the whole development process would require "six months and five to ten core developers" and a number of other individuals taking care of management etc.[43]. Moreover, digital signatures signing the malware and thus avoiding suspicion are required, which can only be obtained by someone who may have physically entered the facilities. Afterwards, the targeted environment needs to be infected inside the premise, presumably by the use of a removable drive (e.g. USB). After the initial infection, Stuxnet begins

[41] Almost all Windows versions from WinXP to Windows7 use the 32-bit architecture and are affected by Stuxnet.
[42] [193, p.1]
[43] [193, p.3]

to spread and search for Field PGs (computers running Windows and used to program PLCs).[43]

> *Since most of these computers are non-networked, Stuxnet would first try to spread to other computers on the LAN through a zero-day vulnerability, a two year old vulnerability, infecting Step 7 projects, and through removable drives. Propagation through a LAN likely served as the first step and propagation through removable drives as a means to cover the last and final hop to a Field PG that is never connected to an untrusted network.*[43]

Due to the fact that remote control with the use of C2 requires an outbound internet connection, and the target computers were unlikely to have one, "all the functionality required to sabotage a system was embedded directly in the Stuxnet executable"[43]. The executable would get updates "throughout the facility through a peer-to-peer method established by Stuxnet"[43]. After finding the right computer target, that ran Step 7, Stuxnet "would then modify the code on the PLC"[43]. Those modifications are mainly responsible for sabotaging the system. Due to its hidden nature, Stuxnet would not reveal any of those modifications to victims. Also, due to the use of self-replication methods, "noticeable collateral damage by infecting machines outside the target organization" was caused[43].

According to the report, an analysis of monitored traffic to the Stuxnet C2 servers revealed encrypted data containing computer name, OS version, IP, and whether the computer was running the Siemens SIMATIC Step 7 industrial control software. Approximately 100.000 infected hosts have been identified. Systems located in 155 different countries were affected, with a majority in Iran (58.31%), followed by Indonesia and India (17.83% and 9.96%)[44]. Iran's leading position indicates as it being the initial target. Further analysis concluded that five different organizations, based on the recorded computer domain name and having presence in Iran, were targeted between June 2009 and May 2010 with a range of 12 hours to 28 days of time required after compilation to the first infection.[45]

The main features of Stuxnet are controllable through a '.dll' file that contains various resources and different exports. In addition to the '.dll' file, "stuxnet also contains two encrypted configuration blocks."[46].

The report states:

> *The dropper component of Stuxnet is a wrapper program that contains all of the above components stored inside itself in a section name 'stub'. This stub section is integral to the working of Stuxnet. When the threat is executed, the wrapper extracts the .dll file from the stub section, maps it into memory as a module, and calls one of the exports.*[46]

The export-functions are e.g. starting RPC server, verification of correct instalment of the malware, verification of version information, update from infected Step 7 projects, de-installing of

[44] [193, p.6]
[45] [193, p.7-8]
[46] [193, p.12]

Stuxnet, checking internet connection, command and control routines and so on. All the code for controlling the work is contained in the essential '.dll' file.[47]

Also:

> *Whenever an export is called, Stuxnet typically injects the entire DLL into another process and then just calls the particular export. Stuxnet can inject into an existing or newly created arbitrary process or a preselected trusted process.*[48]

Trusted processes can be standard Microsoft Windows processes or a number of security products such as Kaspersky KAV (avp.exe), AntiVir (avguard.exe) or Symantec (rtvscan.exe). Stuxnet was so subtle, that it was able to detect one of the above security products, and the target process of injection would either be determined or it would fail, if the security product would be considered as "non-by-passable"[48].

Figure 4.5 shows, how detailed and sophisticated the control flow at entry point is, having various checks in order to inject the right process.

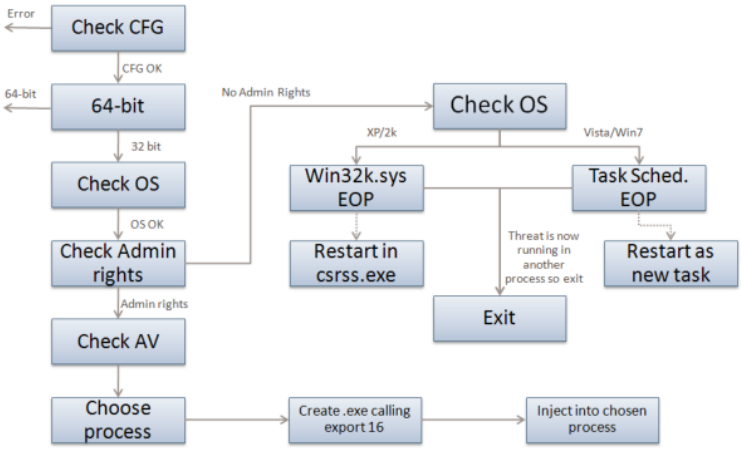


Figure 4.5: Control flow at entry point (export function) (reprinted from [193, p.16]).

At first, it is checked, whether the configuration data is up-to-date. If true, the next check involves the OS-architecture, because only systems running Windows 32-bit OS (including Windows Server 2008) can be exploited. Afterwards, the programs checks admin rights, which represent the highest privileges for gaining full control over the systems. If not, it will, however, try to attain those, by using zero-day escalation. Finally, depending on the flow, processes are chosen for injection purposes (Note: EOP = elevation-of-privilege).[49]

The Stuxnet control flow of the installation routine has also various checks during the actual installation of Stuxnet, infecting registry keys, checking data, communication between differ-

[47] [193, p.13]
[48] [193, p.14]
[49] [193, p.16-17]

ent components via global mutexes, executing OS specific commands, creating encrypted files, infecting processes, and dropping two root-kit files.

The root-kit files are both digitally signed and appear to be valid files belonging to other products.[50]

After the installation the system contacts the C2 server on port 80 "and sends some basic information about the compromised computer to the attacker via HTTP"[51]. Two C2 servers have been identified as:

- www[.]mypremierfutbol[.]com
- www[.]todaysfutbol[.]com

Two URL's, pointing to servers, located in Denmark and Malaysia.[51]

The end goal of Stuxnet has been to infect particular types of PLC devices. Through the PLC, access is provided to options such as execution, control and monitoring of an industrial process.

Stuxnet versions infecting computer systems between 2009 and 2010 have been identified varying in size, content (resources), but similar or identical behaviour and functionality, with minor differences in code.

In conclusion, according to the report Stuxnet "represents the first of many milestones in malicious code history - it is the first to exploit four 0-day vulnerabilities, compromise two digital certificates, and inject code into industrial control systems and hide the code from the operator"[52].

Stuxnet gives evidence on direct-attack attempts on critical infrastructure, utilizing immense resources to develop and execute it in a very sophisticated and unique way. Symantec, who decided to analyse the structure and functionality of the malware by using reverse engineering states: "Stuxnet is the type of threat we hope to never see again"[52], which only shows the magnitude of its complexity and potential to cause damage to industrialized countries.

While officially Stuxnet's origin could not be discovered, according to an article from the *New York Times*, several authority employees whose names were not made public stated, that US president Obama officially signed the operation, after it was already allowed by George W. Bush in 2006.[53] Israeli Officials also told *Der Spiegel*, that Stuxnet was a operation run by their country [54].

Stuxnet was responsible for destroying Iranian uranium enrichment centrifuges by gaining access to the Supervisory Control and Data Acquisition (SCADA) software that were in control of the centrifuges.

Today, Stuxnet is often cited as "the most dramatic use of a cyberweapon" and that "no other known cyberattacks carried out by the United States match the physical damage inflicted in that case."[55]

[50] [193, p.17]
[51] [193, p.21]
[52] [193, p.55]
[53] [183]
[54] [168]
[55] [82]

Flame, miniFlame, Gauss and Duqu

Over the course of 2012 a variety of different malware, which have similar characteristics and targets, was discovered by security firms.

Flame

> *Flame can easily be described as one of the most complex threats ever discovered. It's big and incredibly sophisticated. It pretty much redefines the notion of cyber war and cyber espionage.* [56]

The Flame virus was used similarly to Stuxnet in Iran and the Middle East, presumably with the intention to slow down the nuclear bomb-making abilities of Iran and developed by someone related to an intelligence service. Flame has also the features of key logging, screenshot taking, voice/VoIP recording and others. Through Bluetooth the malware is able to look for near devices and can spread in networks. The commands to those actions are coming from a C2 system, that naturally has to be connected to the internet. The contents are then compressed, encrypted and sent to the controller. During the infection phase, Flame checks if AV software is installed, and hides its presence, by not doing any operations. In contrast to Stuxnet, Flame's purpose was primarily to collect data from e-mails and files without huge restrictions and it appeared on fewer systems in the Middle East and North Africa. This makes the malware an all-round-tool, which can be either used for overall data theft, or on specifically chosen targets with its respective modules. According to Kaspersky, 189 infected computers have been discovered in Iran, followed by Israel and Palestine (98), Sudan (32), Syria (30), Lebanon (18), Saudi Arabia (10) and Egypt (5). As such it's safe to assume that Flame was specifically built to target particular systems. The development efforts must have required great resources, indicating that most likely intelligence services have been behind the malware. As possible ways of initial infection the usual methods of spear phishing and website [forwarding] are named. The sources of infection include USB drives and infected PCs, connected to a network, exploiting the same vulnerability (Zero-Day-Exploit) as Stuxnet.[56]

> *When Flame is executed by a user who has administrative rights to the domain controller, it is also able to attack other machines in the network: it creates backdoor user accounts with a pre-defined password that is then used to copy itself to these machines.*[56]

Another interesting fact to point out is that Flame was also able to infect fully-patched Windows 7 systems, indicating a day-zero vulnerability. The full unpacked version of Flame has a size of roughly 20 MB and includes a number of different modules and plug-ins, allowing the attacker individual functionality for specific purposes.[56]

> *Much of these are libraries designed to handle SSL traffic, SSH connections, sniffing, attack, interception of communications and so on. Consider this: it took us*

[56] [88]

several months to analyse the 500K code of Stuxnet. It will probably take year to fully understand the 20MB of code of Flame.[56]

Kaspersky works following the principle of extrapolation, meaning they derive assumptions regarding real numbers of infected computers from the number of truely infected computers of their customers. As such the numbers can be inaccurate. The targeted victims range from individuals about certain government organizations to educational institutions, and don't indicate a clear pattern.

A report by Symantec states that several indicators of infected systems have been found in Hungary, Austria, Russia, Hong Kong, however, which partially could also be infected laptops, which carried the infections over from the already mentioned countries.[57]

A true time of origin could hardly be identified, but it is assumed that the infections have been present in February-March 2010 at the latest, probably even earlier. Regarding the origin and relations to other malware Kaspersky states that "Flame and Stuxnet/Duqu were probably developed by two separate groups" and that Flame could be positioned "as a project running parallel to Stuxnet and Duqu."[58] It is very likely that the malware has been developed by the same team that was behind Stuxnet/Duqu, but as a parallel project, considering the case that the other one would be discovered first.

According to the *Washington Post*, Flame was part of an operation led and developed in cooperation by USA and Israel. Insiders told that the NSA, CIA and Israel's military were involved in the development and that the program's target was to slow down Iranian nuclear efforts.[59]

Gauss

During the analysis of Flame, Kaspersky had discovered a special version of it, codenamed 'Gauss', which primarily is used for eavesdropping on online-banking transactions. The cyber espionage tool had infected thousands of systems in the Middle East, mostly running Windows XP (44%) and Windows 7 (47%). Since July 2012 the C2 servers seem to be offline. In contrast to usual malware, which is used in the fields of bank transactions to steal money, Gauss is rather used to monitor bank transactions. The malware uses a modular structure, a simple code base and C2 communication - all very similar to that of Flame.[60]

Gauss monitors the target's internet surfing behaviour, logs passwords, cookies, browsing history, collects information on various system characteristics and network connections, the hardware, folders and processes. Roughly 2500 infections have been registered, of which the most belong to systems located in Lebanon (1660), followed by Israel (483) and Palestine (261). According to Kaspersky, Gauss has presumably been active since September 2011, until it was first discovered by an AV software in May 2012.[60]

[57] [62]
[58] [88]
[59] [148]
[60] [172]

Gauss is a much more widespread threat than Flame, however, a self-replication functionality in the modules that has been seen e.g. in Flame, could not be found. The malware has also an encrypted package, which could not be decrypted by Kaspersky.

According to a statement from Vitaly Kamluk, Kaspersky's chief malware expert: "It can also be temporarily passed via a removable USB drive"[61]. Moreover, as soon a USB device is "put into a computer infected with Gauss, it will stay hidden on the USB"[61]. The infected USB device can then infect all other computers that it gets plugged-in to. The new computers are, however, not infected by Gauss, but rather used to mine and store data. Immediately upon plugging the USB back "into the original computer that infected it, Gauss will send all of the data gathered (and can hold information on up to 30 computers) back to its command and control servers, which are currently down"[61].

miniFlame

This is a smaller, more specialized and precise malware version of Flame, based on the same architectural platform. It's a self-contained cyber espionage trojan and was presumably built by the same architects as Flame and Gauss, developed sometime between 2007 and 2011 in six identified variants (4.x and 5.x). According to the analysis from Kaspersky it can be used as a self-contained espionage tool, but also as a plugin for Flame and Gauss, meaning those two can load miniFlame in order to get access to the infected system.[62] The attacking approach of the hackers can be divided in three main phases.

1. Flame and Gauss are first used to infect as many targets as possible.

2. Data is collected from the infected systems and more specific targets are evaluated according to the purpose of the attack.

3. miniFlame is deployed on the already infected machines (or standalone) in order to steal particular data.

Kaspersky states, they have discovered Flame and Gauss being on roughly 10.000 systems in the middle East, while miniFlame has been registered on some machines in the double-digit range in West-Asia. The infections worldwide are estimated at 50-60.

'MiniFlame' similar to most other cyber espionage tools accepts C2, including all the usual commands like 'write file, send file, load dll, write value in registry, sleep, screenshot, recording audio/video'. [62]

Similarly to the two 'siblings' Flame and Gauss, and the Stuxnet virus, it is believed that miniFlame was also developed by the United States and/or Israel "with the target to gather intelligence on Iranian interests in the Middle East"[63].

[61] [149]
[62] [173]
[63] [165]

Duqu

The security firm Symantec had discovered a variant of Stuxnet (based on same source code) in October 2011, which is smaller and built in a way to prepare a real attack by similar programs like Stuxnet.[64] It's main functionality is to search for insider information to control systems of industry plants and send the stolen information to a C2 server. The infected computer systems have mostly been associated with the production of industrial plant controls, and the systems have all been found to be located in Europe. The analysis showed that 'W32.Duqu' was actually in use in December 2010. As such, Duqu did not possess any features of reproduction and removed itself after 36 days. Rather, it was a tool for reconnaissance. Collected data is encrypted and sent to a C2 server, where the tool can also load several plug-ins, including key-loggers. The tool also hides its presence from AV software by disguising itself through a stolen digital certificate (belonging to Symantec) and installing a driver so that modules can be loaded and the data can be sent in form of image files (.jpeg). Duqu infects exclusively Windows systems and behaves similarly to a Botnet.[64]

Symantec does not give out any information on how the malware had infected the machines in the first place and which information Duqu was stealing. The platform on which both Stuxnet and Duqu are based on has been named 'Tilded'.[64]

GhostNet

On March 29th, 2009 the University of Toronto published a research paper on a newly discovered state-affiliated program named GhostNet. The findings of a 10-month investigation show that the attack follows the usual steps of sending e-mails attaching malware disguised as PDF, DOC, PPT or XLS files to specific targets, rather than 'phishing' for random victims. Again, the attacker takes great efforts and care to make the contents of the e-mail as specific and personal as possible with the adequate language so the chance that the receiver will raise suspicion is minimized. Similar to other programs, the attachment file opens a backdoor and causes the infected computer to establish a connection to a C2 server and wait for further instructions. The exploit drops a hidden remote access trojan, which is either a variant of **Gh0st RAT** or **Poison Ivy**.

Researchers managed to discover locations of some of the servers, which were used during the spying attacks. Worldwide 1.295 compromised computers in 103 countries could be found. The attacks were mainly targeting "diplomatic and economic government offices in South and South-East Asian countries" [65].

With the release of the research paper, a *New York Times* article and another independent paper related to the topic[66], created by the University of Cambridge have been published. Interestingly, amongst hundreds of other government and private offices, the Canadian researchers could identify the Dalai Lama organization as one of the victims. The mail server computers of this organization have been under the control of the attackers. Considering the ongoing conflict between Tibet and China this target comes to little surprise. According to the researchers a real

[64] [61]
[65] [134]
[66] called: The snooping dragon: social-malware surveillance of the Tibetan movement.

world scenario could be replayed, which indicated correlations between the exact time, when the systems were under the hacker's control, and real world events that happened at that time. Although no conclusive involvement of the Chinese government is reported, most computers, which were in control of the hackers almost exclusively were based in China. The researchers discovered the usual C2 functionality, when infected computers were receiving signals from outside systems and sent encrypted data to them. They stated: "The spying could be a non state, for-profit operation, for example, or one run by private citizens in China known as 'patriotic hackers'."[67]

The researchers explained also, that besides the e-mail (with an attachment version), there was also the type of an e-mail having a web link leading to a 'poisoned' site used. At the time one of the investigators said: "attribution is difficult because there is no agreed upon international legal framework for being able to pursue investigations down to their logical conclusion, which is highly local"[67], indicating on missing legislations and guidelines on this politically sensitive topic.

Roughly 30% of the infected computers were considered as targets of "high-value and include the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters."[68]

The researchers also found out, that only 11 of 34 AV products were able to detect the malware.

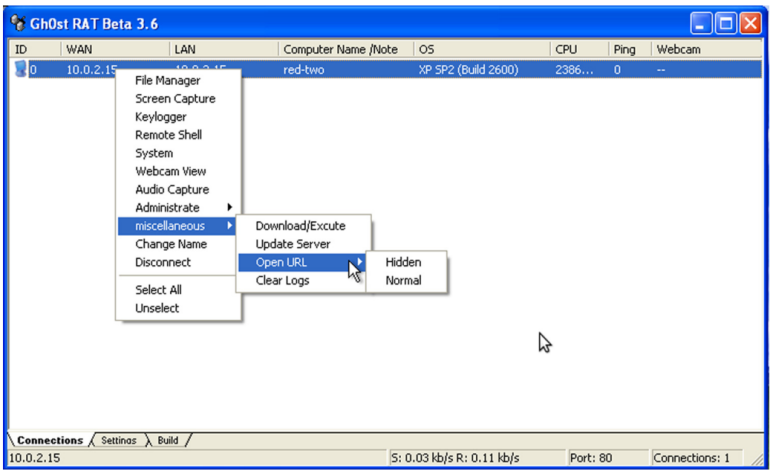


Figure 4.6: The interface of the Gh0st RAT Beta 3.6 tool (reprinted from [152, p.36]).

Figure 4.6 shows different commands that can be executed on the infected computer (ID 0)

[67] [134]
[68] [152, p.5]

remotely, basically giving all opportunities to monitor and control the affected system. 'Gh0st RAT' can also be configured using a proxy.[69] That way the true location of the attacker(s) can be kept hidden. Overall functionality and capabilities of the software is very similar to other remote-accessible malware programs discussed in this chapter.

After Gh0st RAT has been installed on the target, "the infected computer will periodically check a specific location and retrieve the IP address to which it is supposed to connect"[70]. In the case of the attacker being unavailable, the IP is changed to localhost (IP-address: 127.0.0.1) in order to limit the potentially suspicious external traffic. In the other case, a valid external IP-address is put in.

Infected systems were found in a large number of different governmental institutions, including Banks, Departments of Foreign Affairs, Embassies, High Commissions, Ministries of Foreign Affairs, University Networks and others (see [71]).

The report stresses that infected computer systems were communicating with control servers as early as May 22nd, 2007 all the way until March 12th, 2009. The average amount of time of infection was 145 days. Numbers include computers being infected for one day, as well as some with 400 days. The longest time period mentioned was 660 days.[72] The numbers again fit very well into the time-line of other active malware programs, indicating the similar functionality and fact that a major portion remained unnoticed for a very long time.

In conclusion, the GhostNet is rather small compared to other large-scale spy nets, which have been discovered in recent months and years. But nevertheless, it targeted important political, economical and technological facilities all over the world and shows the trend of an increase of a variety of tools, concentrating on high-value systems. It also shows, that it is not necessarily state intelligence agency related, but a tool that can be developed by smaller groups, who could execute such computer network operations.

The researchers stressed that definitive conclusions about the identity of the attackers and their targets could not be made.

Planet Blue Coat

In January 2013, Citizen Lab again reported about new findings of signatures from surveillance technologies developed by the company Blue Coat. With the help of the search engine Shodan [73] "61 Blue Coat ProxySG devices and 316 Blue Coat PacketShaper appliances, devices with specific functionality permitting filtering, censorship, and surveillance" have been discovered[74]. According to the report 61 of the Blue Coat appliances have been on "public or government networks in countries with a history of concerns over human rights, surveillance, and censorship"[74].

[69] [152, p.37]
[70] [152, p.39]
[71] [152, p.42-44]
[72] [152, p.44]
[73] Computer search engine searching the internet for computer and devices based on city, country, host name, OS and IP http://www.shodanhq.com/help/tour.
[74] [46]

Officially, the product 'Blue Coat ProxySG' is advertised as flexible policy-based surveillance and a tool for controlling data, users, applications and protocols, whereas the 'PacketShaper' represents an all-in-one solution, which offers whole network surveillance and control. In 2011 Citizen Lab found out that Blue Coat products were used in Burma for the purposes of filtering the internet. The report reveals that the dissemination of surveillance and filtering technologies are poorly controlled. In any forms of government the use of such technologies represents a violation of human rights and free speech. This example shows also once again the need for export control, clear and strict policies, and corporate social responsibility.[74]

Red October

In January 2013 the IT security firm Kaspersky Lab reported about finding a new cyber espionage tool called 'Rocra', presumably developed in Russia and designed to collect access codes to classified networks at critical infrastructure (energy and nuclear related) as well as governmental and scientific research organisations.

The malware is in use since 2007 and targets countries, including former USSR states, several European countries, the United States, Central Asia and other countries. According to Kaspersky Lab, Rocra was designed to gather "geopolitical intelligence, credentials to access classified computer systems"[75]. The whole espionage operation is called Red October and includes also the collection of data from routers and smartphones, and is capable of even deleting data from removable disk drives. Evidence found in the malware showed indications of Russian-speaking attackers. According to Kaspersky Lab the malware is sent via e-mail (spear phishing) targeting specific organisations. The attachment file contains malware, which exploits a security flaw in Microsoft Office software (Excel and Word documents). The attackers collect a wide range of credentials and save it to a list, and then use this information to gain entry into additional systems.

It even has the ability, after having infected the system, to steal files from Cryptofiler, a cryptography software used by the European Parliament, European Commission, European Union and the NATO. Originally, it was developed to protect sensitive information.[75]

Rocra is specifically built, so that after it is discovered and removed from the infected system it uses a secret 'resurrection module', which was hidden in the system's installed version of Adobe Reader or Office. According to the researchers, the module provides "a foolproof way to regain access to a target system if the main malware body is discovered and removed, or if the system is patched"[76]. Afterwards, "once the [command and control servers] are operational again the attackers send a specialized document file (a PDF or Office document) to victims machines via email which will activate the malware again."[76].

Again, similar to other cyber espionage operations, the Rocra malware exploits a backdoor and sends data to multiple C2 servers, "through a configuration which rivals in complexity the infrastructure of the Flame malware"[77].

Some points to be taken from the investigation are[77]:

[75] [176]
[76] [166]
[77] [176]

- Active for at least 5 years & worldwide focus on governmental and diplomatic authorities.
- Network of infected machines is controlled via a number of server hosting locations including mainly Germany and Russia, and 60 domain names.
- C2 infrastructure is built like a chain of servers, each working as proxies and as such hiding the true location.
- Attachment file is a dropper. Contents are copied to a local folder and a batch script is executed, connecting to a C2 server domain, infecting processes and registry.
- Different modules are loaded on to the machine with specific capabilities. The keyboard-module for instance records keystrokes, grabs texts from input fields and makes screen-captures.
- System is resistant to C2 server takeover and has ability to 'resurrect'.
- The System is accessing and stealing data from workstations and smartphones, "dumping enterprise network equipment configuration (Cisco)", accessing files (also deleted ones) from removable disk drives, and gathering data files from FTP servers as well as e-mail databases from Outlook or remote POP/IMAP servers.
- A module is dropped in the victim's network to scan the LAN for further hosts. Remotely the attackers are then using admin credentials accessing them and collecting information and as such spreading the 'infection' by deploying modules on additional hosts.
- Indicators (e.g. cyrillic characters in the malware module code) relate the malware to Russian-speaking origin, while the exploit code has been created by hackers from China.
- Information hijacked from infected machines include following document-extensions: txt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau, cif, key, crt, cer, hse, pgp, gpg, xia, xiu, xis, xio, xig, acidcsa, acidsca, aciddsk, acidpvr, acidppr, acidssa.
- Generally, the Rocra framework utilizes two tasks, persistent (waiting for input, connection of a device etc.) and one-time (manually collect information, extract data, perform scan etc.).
- The infection phase uses similar characteristics to other malware programs (Trojan infects relevant OS-processes such as svchost.exe, edits the registry (autorun etc.) and makes sure a connection to the C2 server is established.

Figure 4.7 illustrates the C2 infrastructure and how the victim's systems have been controlled through the use of proxies.

Interestingly enough, the country identified as having the most infections is Russia (35), followed by Kazakhstan (21), Azerbaijan (15), Belgium (15), and India (14) and other countries. During the three months of investigation (Nov. 2012 - Jan. 2013) 250 Rocra infections could be identified.[78]

[78] [175]

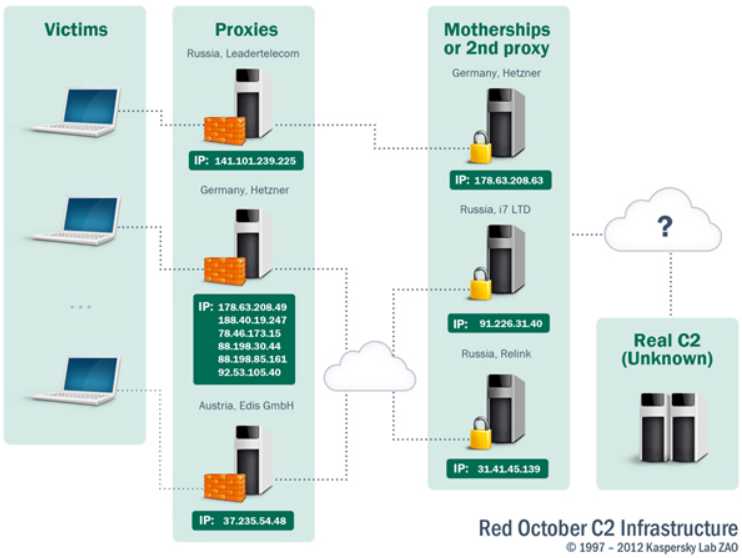


Figure 4.7: Overview of Rocra's C2 infrastructure (reprinted from [111]).

Besides the Office documents used as attached files, the attackers also "infiltrated victim network(s) via Java exploitation"[78]. A '.jar' file served as a mal-code container, which was run, after the e-mail receiver opened a link to a website containing the Java file and the victims systems were running an outdated version of Java at the same time. This exploit is known under name 'Rhino'.[78]

The campaign is presumed to be still active - though severely disrupted in its functionality - after rapidly dismantling the infrastructure shortly after the operation was uncovered and no conclusive evidence on a nation-sate sponsored attack is given.

Winnti

In April, 2013 Kaspersky Lab announced a discovery of a continuous cyber-espionage campaign run by a cyber-crime group called 'Winnti'[79], which focuses on "stealing digital certificates signed by legitimate", mainly Asia-based - "software vendors"[80]. According to Kaspersky 'Winnti' has been attacking online gaming companies since 2009 and focused also on the theft of intellectual property. The malware is a trojan horse, comprised of a DLL library, specifically compiled for 64-bit Windows environments, which made it also special, because it was the first of its kind that had a valid digital signature on 64-bit OS. The attackers were able to use a Remote Administration Tool (RAT), which allowed for C2-control of the victim's computers without their knowledge. Software development companies producing online games have been identified as victims in South East Asia, Germany, the United States, Japan, China, Russia,

[79] [112]
[80] [74]

Brazil, Peru, and Belarus.[81] Kaspersky Lab describes following three presumed "monetization schemes" used by the Winnti group:

1. *The unfair accumulation of in-game currency/'gold' in online games and the conversion of virtual funds into real money.*

2. *Theft of source code from the online games server to search for vulnerabilities in games – often linked to point 1.*

3. *Theft of source code from the server part of popular online games to further deploy pirate servers.*[81]

Due to the schemes representing more of a financial leitmotif, it can be assumed that no intelligence service was involved in the cyber espionage campaign.

NetTraveler

In June 2013, Kaspersky Lab reported of a family of malicious programs named NetTraveler[82]. The 'NetTraveler group' consists of APT actors, presumed to be of size of 50 individuals, mostly natively speaking Chinese. The group was able to compromise "more than 350 high-profile victims in 40 countries"[83]. Targeted sectors include embassies, the oil and gas industry, government institutions, military contractors, research centres and activists. The surveillance threat was presumably active since 2004 and the analysis showed that data was stolen primarily related to fields of "space exploration, nano-technology, energy production, nuclear power, lasers, medicine and communications"[84]. The attack was executed using spear-fishing e-mails with malicious attachments, which exploited two Microsoft Office vulnerabilities. Intelligence was collected on keylogs, system configuration files, popular Office-related documents and PDFs. The malware also had the feature of installing additional info-stealing modules as a backdoor, which gave the opportunity to steal further sensitive information. According to Kaspersky Lab, following countries have been identified as victims of NetTraveler: "Mongolia followed by Russia, India, Kazakhstan, Kyrgyzstan, China, Tajikistan, South Korea, Spain, Germany and others."[84] Kaspersky Lab was even able to identify six victims "that had been infected by both NetTraveler and Red October."[85].

4.2 Analysis

The threat to critical infrastructure is apparent and government and companies, whether small, mid or big-sized, must take threats to their intelligence property and system functionality seriously and invest time and resources to develop proper defences. Considering how internet-dependent today's information society has become, it is time to adapt politics, economy and

[81] [177]
[82] [110]
[83] [174]
[84] [74]
[85] [110]

technology to new standards, but without violating privacy rights of the public. This is true, particularly for countries who call themselves democracies. It should also be considered, even if recent indicators show otherwise, that attacks coming from China were sabotaged by others. If someone is planning such an attack, they want to stay undetected and thus will most likely lay false tracks. Indicators like the use of local keyboard layouts can for instance be edited in the source code of the espionage program in order to direct suspicion to another country.

Nevertheless, the analysis of the variety of malware tools has shown that all world powers, whether it is the US, Russia or China, operate cyber espionage campaigns to an extent, which is alarming. Furthermore, all the different malware packages seem to follow one base structure and infection-/instalment-process, which makes it rather fortunate to prepare counter-measures against or at least create a mindset (keyword: awareness) to be prepared to suspect, which ways hackers would take to try and get intelligence or control. The programs have all in common to thrive for information, which is accessed on the highest level including geopolitical data, which can be used by nations. The information has such a value for basically anyone, that in several cases it can also be traded in the underground and sold via auction (highest bidder). It is also apparent that the Middle East is increasingly becoming a central arena for cyber warfare.

It is almost impossible to trace back the malware to the ones who operate them and have initiated the attacks in the first place. Due to misspellings, typos, characters used in a specific language or keyboard layouts in a non-English language and foremost through the use of proxy servers, it is very hard to tell where the attack really came from, and even if you have a location, it still can be put in for on purpose for distractions from the real source.

Also, Stuxnet has shown that a critical facility does not necessarily need to be connected to the internet, to be vulnerable. It probably would still be undiscovered, if a facility worker wouldn't have taken his infected work laptop home and connected it to internet, so that the malware could spread onto thousands of other systems.

In that perspective, John Villasenor, Contributor to *Forbes*, states the following, which sums up the basic problems of today's information system's inter-connectivity:

> *Trusted digital certificates are a vital part of online financial transactions, software distribution, and other applications. Fake certificates undermine trust, creating collateral damage and unintended downstream consequences not only for the companies whose certificates are faked, but for all participants in the online ecosystem. The uncomfortable reality is that from the power grid to the financial system to personal computers and smartphones, our systems and devices have been designed with insufficient security protections. Continuing to apply expensive, partially effective band-aids won't solve the underlying problem. What's needed is a rethink of how we should be designing and building sophisticated, highly interconnected systems.*[86]

[86] [205]

CHAPTER 5

Governmental surveillance

5.1 A new pinnacle of global surveillance outgoing from the USA

> *In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy. In the absence of the respect for sovereignty, there is no basis for the relationship among Nations.*[1]

After being established in 1952, the NSA acted in operations, intercepting radio and other electronic transmissions and today shifted a large part of the focus to digital data and the surveillance of the internet. The NSA now invests so many resources on intelligence gathering, that it makes it rather awkward or misplaced to advise China to stop their hacking activities. After numerous cyber-espionage incidents, which clearly indicated Chinese affiliation, the US try to show some sort of global control mechanism to address the issues directly, up to a point where tension between the two great powers increases inevitably. As such it comes to little surprise that the Chinese government describes the US as the "real hacking empire"[2]. While the US government does not explicitly deny any engagements in cyber espionage, it is rather surprising to see how far their operations, more specifically the NSA's methods, reach. Until the summer of 2013, when former NSA employee Edward Snowden decided to disclose confidential information on the topic of global surveillance, including cyber espionage, officially the US government denied any existence of the secretive unit known as Tailored Access Operations (TAO), which can mainly be seen as the NSA's hacking division.

According to two former US government security officials the TAO "gathers vast amounts of intelligence on terrorist financial networks, international money-laundering and drug operations, the readiness of foreign militaries, even the internal political squabbles of potential adversaries"[2]. At least that's the information the public got until operations like *Prism* and *Tempora* were revealed. The whole topic of NSA's confidential work was always declared as classified, which is of course of little surprise, due to nature of a intelligence service's actions.

[1] Brazilian president Dilma Rousseff on US surveillance at the United Nations on September 24th, 2013
[2] [179]

Just prior to Snowden's publications the former officials stressed also, that those "from military units who've received specialized training, sit at consoles running sophisticated hacking software, which funnels information stolen from computers around the world into a 'fusion center', where intelligence analysts try to make sense of it all"[2]. Despite the fact that the NSA is prohibited by law "from spying on people or entities within the U.S., including non-citizens, or on U.S. citizens abroad", it comes to big surprise that none of it really matters.[2]

One problem is obviously how the US justifies their actions by saying:

> *some kinds of hacking are more acceptable than others—and the kind the NSA does is in keeping with unofficial, unspoken rules going back to the Cold War about what secrets are OK for one country to steal from another.*[2]

Edward Snowden's confidential documents

On June 7th, 2013 the British newspaper *Guardian* published an article on the top-secret NSA surveillance program Prism. One day before, the Guardian published another article describing how the telecommunication firm Verizon was forced by a US FISC[3] to hand over telephone data to the intelligence service NSA. According to the order, it serves "authorization requiring the production of certain call detail records or 'telephony metadata' created by Verizon"[4]. Affected are millions of US customers of Verizon, whose telephone records (within the US and between the US and other countries) are "ongoing, daily basis" given to the NSA[4]. This shows the extensive collection of vast amounts of data, regardless of suspicion under the Obama administration. According to the court order, included in the records are "numbers from both parties [...], location data, call duration, unique identifiers, and the time and duration of all calls", while the contents of conversation are not comprised[5]. Handing over the records to the NSA is described as quite unusual: "FISA court orders typically direct the production of records pertaining to a specific named target who is suspected of being an agent of a terrorist group or foreign state, or a finite set of individually named targets."[5]. Further, the data is classified as 'metadata', meaning transactional information instead of communications. Thus, it does not require specific warrants to access. The information the records provide "would allow the NSA to build easily a comprehensive picture of who any individual contacted, how and when, and possibly from where, retrospectively", as it explicitly states that this metadata does not include the contents of the messages or the names of the customers[5]. It is very likely that other similar court orders exist, forcing other enterprises besides Verizon, to give out their communication data.

On June 9th, 2013 the former CIA and NSA technical employee Edward Snowden revealed his identity as being the one responsible for disclosing confidential information about surveillance programs such as Prism, Boundless Informant and Tempora.

[3] signed on April 25th, 2013 granting authority ending on July 19th, 2013
[4] [33, p.4]
[5] [90]

5.2 Prism

Prism is a global surveillance program operated by the NSA and is their number one source of raw intelligence reporting. Everyone who uses US-internet services is a potential victim of this program.[6] Prism allows the NSA access to a variety of data, including:

- E-mails
- Chats
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video conferencing
- Notifications of target activity (logins, etc.)
- Online social network details
- Special requests

Basically, content that is created and exchanged over internet services such as Google Mail, Yahoo Mail, Facebook, as well as services from Microsoft and Apple is accessed. Again, the collected information can be used to create comprehensive user profiles, depending on the data the internet user (including smartphone and tablet users) provides about himself.

The collection of data is done directly from the servers of US service providers, and Prism allows other intelligence services to access data directly from the large companies' servers. The *Guardian* states that "the program facilitates extensive, in-depth surveillance on live communications and stored information." Further, "the law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US." It also makes it possible that communications, which are "made entirely within the US " are "collected without warrants."[6]

In contrast to collecting data from Verizon, which comprises only metadata, Prism can also include the contents of communications. According to internal and confidential presentation, some of the world's largest companies running internet services are part of the information-sharing Prism program. Again, allowed by the order of the FISA Amendments Act. Targeted communications are obtained without a request from service providers and more importantly "without having to obtain individual court orders"[6].

Following dates indicate, that the Prism collection started as early as 2007[7]:

[6] [93]
[7] [19]

- Microsoft - 9/11/07
- Yahoo - 3/12/08
- Google - 1/14/09
- Facebook - 6/3/09
- PalTalk - 12/7/09
- Skype - 2/6/11
- AOL - 3/31/11
- Apple (Oct. 2012)

The Prism program's costs are described as being around $20m per year.

The NSA presentation also claims that Prism "was introduced to overcome what the NSA regarded as shortcomings of FISA warrants in tracking suspected foreign terrorists"[8]. Official words from the presentation describe that FISA's constraints "restricted our home-field advantage", because FISA asked for specific "individual warrants and confirmations" that showed that the receiver and the sender "of a communication were outside the US"[8].

In a nutshell, while previously the NSA needed authorisations and confirmation of suspects actually being foreigners / outside the US, now all they need is a "reasonable suspicion that one of the parties was outside the country at the time of the records were collected by the NSA"[8]. In the document, the NSA praises Prism as "one of the most valuable, unique and productive accesses for NSA"[8].

According to the documents, obtained communications increased by 248% for Skype alone (2012), while requests for Facebook and Google data also increased by 131% and 63% respectively. The addition of the popular cloud service Dropbox as a Prism provider was planned at the time of the presentation.

As soon as the NSA decides to review a communication it believes benefits additional investigation, it marks it as a report. 77,000 of such intelligence reports have cited the Prism program.[8]

Microsoft's cooperation

One of the biggest US IT-companies, Microsoft, cooperates with US intelligence services, according to an article from the *Guardian*. Besides the NSA, the intelligence services FBI and CIA are also able to access information, collected by the Prism program.[9]

[8] [93]
[9] [94]

Backdoors in Skype, SkyDrive and Outlook

As an example, the communication service provider Skype is shown, which since 2011 belongs to Microsoft. While Skype was considered to be relatively safe among users, because it used to have an encrypted Peer-to-Peer solution and a technique, when computers of participants of the network represented nodes, forwarding chats and internet phone calls, it is now obviously considered unsafe.[10] Besides, in 2008 Skype representatives clearly stated that complying with police wire-tap requests was impossible, just due to the way the architecture was built: "In any event, because of Skype's peer-to-peer architecture and encryption techniques, Skype would not be able to comply with such a request."[11]

Instead of using the user's computers as nodes, after Skype's acquisition Microsoft went on to operate the nodes themselves through their own servers. According to the article, the NSA, FBI and CIA have access to VoIP and video recordings. The new disclosures show that Skype calls are not End-to-End encrypted.

Intelligence service backdoors appear also to be included in Microsoft's cloud storage service SkyDrive (250 million users worldwide) and the web-based mail service 'outlook' (previously known as Hotmail). In the case of outlook, professionals from the Special Source Operations (SSO), a NSA division, registered concerns several months before the start of the internet platform 'outlook.com' about the fact that encrypted chats are possible. After 5 months of 'working on the problem', on February 18th of 2013 www.outlook.com was released, backdoor inclusive.[12] As such, the outlook service provided the NSA with data, by helping it to bypass encryption, intercept chats and follow the users creating alias accounts.

How Prism works

According to a presentation published by the *Washington Post*, the data is acquired as follows: An NSA analyst enters a request into the program. The target is described as a 'selector'[13]. Another employee (supervisor) has to review "the selectors, or search terms" and sign it accordingly[14]. He or she must also confirm that there is a good reason (so called 'reasonable belief') that the target is neither American nor on US soil[14], due to legal restrictions.

Then, the data request runs through the FBI, which collects the information from the companies' servers directly and forwards the search results to the intelligence services (NSA, CIA or keeps inside FBI) for further review and analysis, simultaneously making sure the selected person is no American ('NO USPER'). The information is collected directly from the providers, using own installed intelligence equipment at the respective company's property. This equipment, which is maintained by the FBI, passes the NSA request directly to a private company's system. Depending on the services the company provides, file contents and metadata are returned.[14] Of course, this contradicts with the statements of the affected US companies, which explicitly stated that they haven't allowed direct access to their computer (storage) systems. At

[10] [94]
[11] [137]
[12] [94]
[13] selector refers to people, organizations or simple subjects
[14] [27]

the NSA the information runs first through a system called 'PRINTAURA', which "automates the traffic flow" and runs then through a number of systems e.g. 'Marina', 'Mainway', 'Fallout', 'Conveyance' or 'Nucleon', depending on the type of data (metadata or voice content).[14] Each of the programs is used to analyse a specific part of the data. For instance, Nucleon is responsible for the voice data, while Marina is responsible for the browsing habits and overall internet records, and Conveyance checks that US citizens are not monitored. The system Pinwale analyses all content regarding Digital Network Intelligence (DNI) content, including video data.[14] After the processing phase, the yielded results (e.g. login credentials, stored files, metadata) are automatically sent to the analyst who made the tasking request. The whole procedure between the request and the results can take between "minutes to hours"[15]. Though the surveillance of Americans is prohibited, it is stated that communications of these internet users are collected rather "incidentally during surveillance"[16]. As of April 5th, 2013 whole 117.675 active surveillance targets were stored in the Prism counter-terrorism database.

In the end, a case notation is assigned to each target, clearly identifying the Prism provider who provided the information, the content type (e-mail, chat, VoIP etc.), a fixed trigraph denoting the Prism source collection, the year the selector was established on, and a serial number. An example of a case notation would be[17]:

```
P4JSQC120000123
```

According to the presentation the NSA has even the authority to "receive live notifications", as soon as a target logs on the service, sends an e-mail, text, or uses a video or voice chat[17]. The NSA can then monitor the events live, which again requires the active cooperation of the Prism providers.

Regarding the deletion of records and the duration of storage, the article states:

> *If a target turns out to be an American or a person located in the United States, the NSA calls the collection "inadvertent" and usually destroys the results. If the target is foreign but the search results include U.S. communications, the NSA calls this "incidental" collection and generally keeps the U.S. content for five years. There are "minimization" rules to limit the use and distribution of the communications of identifiable U.S. citizens or residents.*[18]

Fairview & Blarney

Fairview is, according to whistleblower Thomas Drake, a former NSA senior executive, another project besides Prism and co., where companies are forced to provide backdoors to agencies for surveillance purposes. It targets the data by getting inside the system "before it's in the internet." Is's also yet another operation involving the tapping into fibre-optic cables. The whole Fairview operation is based on agreements with large international companies, like the Asian

[15] [80]
[16] [27]
[17] P4: Facebook, J: video, SQC: trigraph, 12: year, 0000123: serial number
[18] [80]

telecom concern Global Crossing, which provides the US government with access to data, when it's needed. Fairview is referred to as an 'umbrella' that the NSA would use to receive the information it has collected, and which allows the general data mining process. Beneath this umbrella, programs like Blarney would "collect and analyse the data that is made accessible by secret arrangements" with other companies.[19]

Blarney is more of a 'key access program', that exploits and grabs the metadata at these different junctions "as it streams past choke points along the backbone of the Internet"[20]. While Prism is targeted at the domestic area of the US, Blarney rather is used for interception of international internet space, similar to Tempora.

5.3 Upstream

On July 10th, 2013 another slide from a confidential presentation was published indicating another type of collecting data besides Prism, called Upstream. Officially suggested, Upstream is to be used jointly with Prism, specifically for collecting internet and phone data directly from fibre-optic cable (internet and telephone) networks. The slide's heading is 'FAA 702 Operations', which references to a 2008 law "that enabled, without an individual warrant from a court, collection on U.S. soil of communications of foreigners thought to be overseas, including when the foreigners are communicating with someone in the United States." The law states that the "collection may be for a foreign intelligence purpose, which includes terrorism, nuclear weapons proliferation or cyber-security."[21]

According to another article, the NSA operates "own cable-intercept programs tapping traffic flowing" both into and across the US, called Blarney, Fairview, Oakstar and Stormbrew, which are known as "Upstream collection"[22].

BND in possession of Prism

According to research by the ARD-magazine *Fakt*, the German intelligence service BND has knowledge and possession of the technology, that is based on Prism.[23] The only thing that is certain is the fact that the BND had acquired a Narus-software called 'Netwitness' in 2003, which is an eavesdrop-software. Through a cooperation between the NSA and one of the largest telephone groups AT&T, which used a surveillance system called Narusinsight, Narus became known as a software which is widely used for intelligence gathering. What exactly is processed by Narus and which version of it is used by German authorities however, remains unclear. In 2012, the federal government reassured that the software was not used for illegal 'Deep Packet Inspection'. NetWitness was exclusively used for forensic examination of already collected network data, and not for the purposes of recording. [24]

[19] [115]
[20] [84]
[21] [195]
[22] [26, section 3]
[23] [15]
[24] [40]

Also, the Bundeswehr (German army) is supposed to have used Prism for surveillance of terror suspects during their involvement in Afghanistan. According to a secret NATO document, the Command of the Bundeswehr in Afghanistan had been informed in September 2011 about the existence of Prism. The paper also shows that the program's function is the detection and monitoring of data.[24]

5.4 Boundless Informant

The US program Boundless Informant was also developed by the NSA as a tool to analyse the large amount of collected data. It is basically a data-mining tool, which can visualize details on the information, which is collected from all computer and telephone networks by allocating colour schemes on countries, ranging from green (lowest subject to surveillance), to red (highest subject to surveillance). It can count and categorize metadata, specifically the records of communications. That way, over a period of 30 days (February/March 2013), "almost 3 billion pieces of intelligence from US computer networks" could be identified[25]. Particularly, the tool helps the intelligence service to answer questions such as: "What type of coverage do we have on country X?" in almost real-time by asking the SIGINT infrastructure. By selecting a country, an employee gets insight into details like the amount of metadata volume, and views details about "collections against that country" as well as the amount of records and their type of a particular country[25]. As of March 2013, the tool showed full 97bn "pieces of intelligence" that the NSA acquired from worldwide computer networks. At that time, Iran (14bn) was leading in terms of amount of intelligence gathered per country, followed by Pakistan (13.5bn), Jordan (12.7bn), Egypt (7.6bn) and India (6.3bn). While it comes to no surprise that the 'enemy' Iran is leading, it's interesting to see Jordan up there, being one of the closest Arab allies of the US.[26]

In respect to their - as 'limited' regarded - data-mining capabilities, NSA's spokeswoman Emmel stated:

> *Current technology simply does not permit us to positively identify all of the persons or locations associated with a given communication (for example, it may be possible to say with certainty that a communication traversed a particular path within the internet. It is harder to know the ultimate source or destination, or more particularly the identity of the person represented by the* ***TO:****,* ***FROM:*** *or* ***CC:*** *field of an e-mail address or the abstraction of an IP address). Thus, we apply rigorous training and technological advancements to combine both our automated and manual (human) processes to characterize communications – ensuring protection of the privacy rights of the American people. This is not just our judgement, but that of the relevant inspectors general, who have also reported this.*[27]

[25] [92]
[26] [208]
[27] [92]

5.5 Tempora

> *Tempora is the first 'I save everything' approach ('full take') in the intelligence world. It sucks in all data, no matter what it is, and which rights are violated by it. [...] Right now, the system is capable of saving three days' worth of traffic, but that will be optimised. Three days may perhaps not sound like a lot, but it's not just about connection metadata. 'Full take' means that the system saves everything. If you send a data packet and it makes its way through the UK, we will get it. If you download anything, and the server is in the UK, then we get it. (Edward Snowden)*[28]

The British intelligence agency GCHQ was discovered being involved in extensive surveillance operations directly related to the NSAs intelligence scandal in summer 2013. In particular, it "gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process vast streams of sensitive personal information which it is sharing with its American partner"[29] . The main intention and ambition of the agency is described in a leaked document as "mastering the Internet and Global Telecoms Exploitation", which involves the collection of enormous amounts of data from online and telephone traffic[29]. One of it's abilities is "to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed"[29]. The whole operation, codenamed Tempora, has been running for about 18 months without any public notice. Similarly to one of NSA's most important systems, Prism, the collected data includes contents of e-mails, social media entries, phone call recordings and the user's history of visited websites. With this, the amount of metadata produced by the GCHQ is presumably even larger that the NSA's. At some point 300 analysts from GCHQ together with 250 from the NSA, "had been assigned to sift through the flood of data"[29]. In total, 850.000 NSA employees "and US private contractors with top secret clearance had access to GCHQ databases"[29]. The documents also revealed that at some point the GCHQ "was handling 600m 'telephone events' each day, had tapped more than 200 fibre-optic cables (of total 1,600) that cross the English territory and was able to process data from at least 46 of them at a time"[29]: unbelievably large numbers even compared to those of NSA's operations. Data contents are usually saved for up to 3 days, while metadata is up to 30 days. In numbers, the amount of information which was theoretically going through the 7-centimetres wide cables and as such was being targeted was equivalent to 21 petabytes[30] a day, at a maximum cable capacity of 10 gigabits per second. While this already is enormous, the "scale of the programme is constantly increasing as more cables are tapped and GCHQ data storage facilities in the UK and abroad are expanded with the aim of processing terabits (thousands of gigabits) of data at a time"[30]. The British agency has built its tapping operation over the course of five years and "under secret agreements with commercial companies", described as 'intercept partners'[30].

Presumably, the companies have been paid for their cooperation and were forbidden to disclose any information regarding the existence of such an operation, where the GCHQ had literally direct access to the cables.[31]

[28] [57]
[29] [131]
[30] 1PB is equal to 1000 terabytes
[31] [113]

While the amount of data is undeniably large, the resources to go through each one of it simply do not exist. Thus, for institutions like the GCHQ it is important to focus on the "small number of needles in a haystack", arguing with criteria such as organised crime, terror, security and economic well-being[31]. Most of the data is discarded without ever being looked at, while when the 'needle' is found, a log is created and handed over to the interception commissioner to make further analysis and decisions.

In terms of legitimacy, once again an old law was exploited and applied to a new technology. "The 2000 Regulation of Investigatory Powers Act (Ripa) requires the tapping of defined targets to be authorised by a warrant signed by the home secretary or foreign secretary". Yet, a clause exists, which "allows the foreign secretary to sign a certificate for the interception of broad categories of material, as long as one end of the monitored communications is abroad"[31]. The very nature of fibre-optic communications lead to a part of internal UK-traffic being relayed abroad and afterwards returning through the cables nonetheless. When the parliament passed the Ripa law to allow the GCHQ for the intelligence gathering, the sheer scale on which the GCHQ would operate could not be foreseen, because that was 13 years ago. While categories of intelligence material do include drug trafficking, terrorism and fraud, the criteria are secret "and are not subject to any public debate". Ironically, the agency's "compliance with the certificates is audited by the agency itself, but the results of those audits are also secret", underlining the legislative chaos.[31]

In cases when doubt comes up, intelligence agencies can provide some criminal intentions, which potentially can be supported with systems like Tempora or Prism.

What's also important to understand is the fact that satellite interception eventually became a minor part of the total network traffic. Most of the data nowadays "travels on fibre-optic cables", and the UK's position is mediating almost all traffic between Europe and the US, or the whole Atlantic for that matter (cf. figure 5.1)[31].

Tempora allows the agency to watch the data live and store it for 30 days, if its metadata, or 3 days "in the case of content"[31]. To filter out relevant information most efficiently, Tempora utilizes a sophisticated approach:

> *The processing centres apply a series of sophisticated computer programmes in order to filter the material through what is known as MVR – massive volume reduction. The first filter immediately rejects high-volume, low-value traffic, such as peer-to-peer downloads, which reduces the volume by about 30%. Others pull out packets of information relating to 'selectors' - search terms including subjects, phone numbers and email addresses of interest. Some 40,000 of these were chosen by GCHQ and 31,000 by the NSA. Most of the information extracted is 'content', such as recordings of phone calls or the substance of email messages. The rest is metadata.*[31]

In a nutshell, the whole surveillance program was running under legal conditions, having evidently led to several breakthroughs in detecting and preventing of crimes.

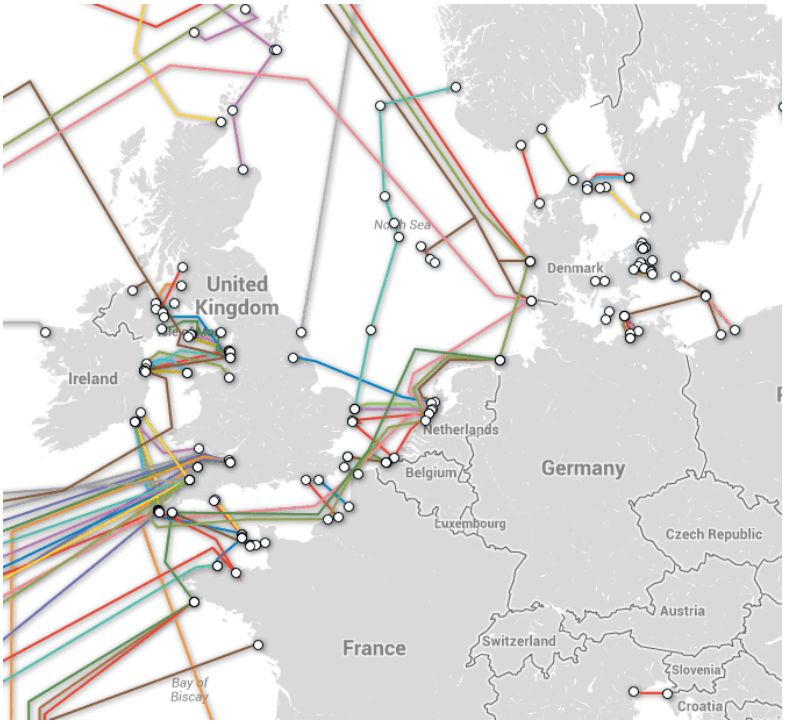


Figure 5.1: Submarine cable map centring on the United Kingdom's position (source: [194])

5.6 XKeyscore

XKeyscore (short: XKS) is another program for gathering intelligence. It reportedly "processes all signals before they are shunted off to various production lines that deal with specific issues and the exploitation of different data types for analysis - variously code-named Nucleon (voice), Pinwale (video), Mainway (call records) and Marina (internet records)."[32]

According to secret documents, the BND and the BfV are also using the NSA's spying software.[33] *Der Spiegel* reports about the software being used for supporting counter-terrorism, and that the BND was mainly responsible for the training of the BfV in operating the program. A presentation from February 2008 describes XKeyscore as an espionage tool, which enables almost total digital surveillance. With the help of metadata, for example, details can be recreated, depending on what keywords have been typed in search engines by the targeted persons. In addition, the system is capable of recording a 'full take' of all data for several days. 'Full take' is referred - at least partially - to contents of communications.

The NSA has access to about 500m data records from Germany, of which circa 180m have been acquired by XKeyscore in December 2012 alone.[33] The BfV explained, that the system is being tested in fact, and one would have no access to databases.

[32] [57]
[33] [192]

Disclosed internal presentations[34] of the NSA reveal some details about XKeyscore's features. The system itself seems to have several extensions and variants, varying from target to target. One graphic shows a male person, presumably a NSA-analyst in front of a computer, who queries a database, which contains metadata tables and logs, containing information like phone numbers, e-mail addresses, log ins, and user activity. With this data relationship networks, motion profiles and usage patterns of individuals can be derived and visualised. Metadata is generated also in search queries and can be assigned to a particular person. Thus, XKeyscore is able to extract and store events, which can then be "retrospectively queried", allowing for viewing those keywords that people have typed into search engines, as well as locations they have been looking for in Google Maps[34]. A slide shows, how a user searching with Google Maps can serve as a basis for gaining more information. On the slide there are also questions illustrated:

- *Can I use this information to determine his email address?*
- *What about the web-searches - do any stand out and look suspicious?*[34]

According to new leaked presentation slides, discovered by *the Guardian*, XKeyscore is primarily a "'widest reaching' system developing intelligence from computer networks", by the agency called DNI, which allows to search contents of digital communication, by using keywords of different (strong and soft) criteria (e.g. e-mail address, specific search string, language, content). The system also allows the recording of real-time interception of the targeted person's activities and to store all unfiltered data, that reach the system. A 'Rolling Buffer' keeps '*all* unfiltered' data for 3 days on average. Regarding data collection, all internet content ("full-take data") is recorded and indexed based on their metadata, so that the data can be easily queried afterwards. One query is able to scan all sites.[35]

Foundation-wise, the system's infrastructure is described as being a "massive distributed Linux cluster", with over 500 servers, which are distributed all over the globe. Additional servers can easily be added to the cluster.[36] Overall, there are 700 servers worldwide running XKS, at approx. 150 sites, mainly in the European region and in the Middle East.

According to the documents, a total of 300 terrorists had been captured with the help of intelligence provided by XKeyscore. Information that can be searched through the system is first filterable by using various inputs in fields, including "every email address seen in a session by both username and domain, every phone number seen in a session (eg address book entries or signature block), the web-mail and chat activity to include username, buddy list, machine specific cookies etc."[37]. The variety of results, which can be 'fished' from the traffic, include:

- Telephone numbers, login credentials, e-mail addresses, user names, buddy lists, cookies, google search requests including IP-address, language and used browser.
- Establishing of an encrypted VPN-connection.
- Search requests of locations on Google Maps, his other search inputs and e-mail address.

[34] [24]
[35] [36, p.3]
[36] [36, p.4]
[37] [91]

- Revealing users that use a different language from the region they are in online (e.g. German in Pakistan).
- Tracing back of a particular online distributed documents to the source.
- All online transferred documents, that contain specific terms (e.g. 'Osama bin Laden'), and even in different languages.[37]

The analyst can basically save everything, depending on his desire. Therefore, he just has to formulate appropriate search orders. According to a slide, savable is everything, "that you want to extract"[38].

The article reports also about additional surveillance options. For instance, XKeyscore users can query any IP address, from which particular websites have been accessed. Also, NSA personnel is able to view the contents of private Facebook conversations. Therefore, they only need to enter the user name of a Facebook member and select the period, when the conversation took place. US agents are able to search for suspects, who were previously unknown and will henceforth be monitored more closely, which illustrates a valuable property of the system. Potentially, this system targets everyone as a suspect, whether being a journalist who reports about a crisis region, development workers or diplomats, who write an e-mail in a foreign language from highly targeted country.[39]

The documents contain for the first time indications on systematic attacks on computer systems by US authorities in foreign countries. As such, XKeyscore allows for showing a list of all attackable computers in a specific area (country). The secret organisation TAO operates a database containing data about vulnerabilities of computer systems worldwide, which is naturally accessible by the NSA.

All the data at different NSA storage facilities worldwide can be searched from any point through XKeyscore. Data is collected mainly at 3 locations:

- F6-locations (F6 is known as Special Collection Service, a collaborative organisation of NSA and CIA).[40]
- Fornsat-locations (Fornsat stands for Foreign Satellite Collection, a system for interception satellite communication).[41]
- SSO-locations (SSO stands for Special Source Operations, a NSA-sub-organisation, which is one of many systems responsible for the collection of metadata).[41]

A slide shows also, that the Marina-database is accessible by XKeyscore, which serves the evaluation of metadata. Due to the immense amount of internet traffic of a particular country, the NSA is not able to copy all of the data. However, analysts are able to make metadata search queries directed at the particular location and get that way the 'interesting contents' from the location. Already in 2012, during a time frame of 30 days, 41bn entries were supposedly contained

[38] [36, p.13]
[39] [91]
[40] [89]
[41] [4]

in the XKeyscore database. According to *the Guardian* the databases Traffic thief (specifically selected metadata), Pinwale (contents based on keywords in search queries) and Marina (internet metadata) are all smaller in relation to XKeyscore.[42]

The program is even able to search inside e-mail bodies, "web pages and documents, including the 'To, From, CC, BCC lines' and the 'Contact Us' pages on websites"[42].

If an analyst decides to search for e-mails, he just needs to enter the individual's e-mail address into a simple search form. Moreover, he has to name justification reasons and the time period to filter the results. In return XKS "parses out everything it 'thinks' is an email address"[42]. The analysts then select the e-mail they want to read.

Especially the surveillance of individuals, who are staying on US soil, is seemingly limitless for NSA analysts. A document published by *the Guardian* shows a user dialogue for a surveillance measure. From a simple drop-down menu, the user first selects the purpose of monitoring, then the 'foreignness-factor' of the target person. One option for that is for example: "Phone number country code indicates person is located outside the U.S."[42].

Another option shows the reasoning, which appears to be sufficient for the right of applying surveillance: "In direct contact with target overseas, no info to show proposed target in U.S.". After completing the selection process, the target person is marked for electronic surveillance, meaning the analyst is able to view contents of the person's communication.

As mentioned previously, the XKS system is able to present contents from social media services. The NSA tool 'DNI Presenter', besides being used for reading contents of e-mails, "also enables an analyst [...] to read the content of Facebook chats or private messages"[42]. Facebook user name and date range are sufficient, in order to query contents of communication. Visualising internet browsing activities is also a function of XKS. The analyst can search HTTP activity by keyword, allowing to see "nearly everything a typical user does on the Internet", because most websites rely on HTTP. Furthermore, the analyst is able to "learn the IP addresses of every person who visits any website the analyst specifies"[42]. They just need to enter the particular website's URL they are interested in (e.g. show everyone in Sweden who visits a particular extremist web forum).[42]

The article states further, that "one NSA report from 2007 estimated that there were 850bn 'call events' collected and stored in the NSA databases, and close to 150bn internet records. Each day, the document says, 1-2bn records were added"[42]. Applying these numbers to the development of technology, storage capacities and transfer rates in particular, the amount of collected data can be significantly higher today.[42]

Due to the gigantic requirements of storage, contents usually are deleted from the system after 3-5 days, while metadata is stored for 30 days, similarly to Tempora-data. According to a document, the amount of data varies from site to site. Thus, it happens occasionally that 20+ terabytes are received a day and can only be stored for about 24 hours. To solve the capacity problem, the NSA "has created a multi-tiered system that allows analysts to store 'interesting' content in other databases, such as one named Pinwale which can store material for up to five years"[42]. According to that information, the database of XKS contains the "greatest amount of communications data collected by the NSA".[42]

[42] [91]

Again, while legislation-wise the "FISA Amendments Act of 2008 requires an individualized warrant for the targeting of US persons, NSA analysts are permitted to intercept the communications of such individuals without a warrant if they are in contact with one of the NSA's foreign targets"[42]. As such, it is clear, that each individual, whatever he or she may say about having nothing to hide from the government, can become a target, without even intentionally having done something 'wrong'.

Australia's and New Zealand's involvement

According to information from Edward Snowden, Australia is also deeply involved in US global surveillance. Four facilities contribute regularly "to a key American intelligence collection program", which refers to the NSA's collection program XKeyscore[43]. A number of different locations of US and allied signals intelligence collection sites have been revealed. Those sites "contribute to interception of telecommunications and internet traffic worldwide"[43].

New Zealand (Government Security Communications Bureau facility at Waihopai) is also involved in US global surveillance, which makes another partner of the Five Eyes intelligence alliance actively contributing to the program. There have also been reports of a construction of a new data storage facility "at HMAS Harman to support the Australian signals directorate and other Australian intelligence agencies"[43].

On August 29, 2013 it was discovered that Australia's electronic espionage agency, the Australian Signals Directorate (ASD), "is in a partnership with British, American and Singaporean intelligence agencies to tap undersea fibre optic telecommunications cables that link Asia, the Middle East and Europe and carry much of Australia's international phone and internet traffic"[44]. Previously commissioned in the year 2000, "the 39,000 kilometre long **SEA-ME-WE-3** cable is owned by an international consortium that includes British Telecom, SingTel Optus (owned by Singapore's government), Telstra and other telecommunications companies across Asia, the Middle East and Europe"[44]. Australia is accessing the **SEA-ME-WE-3** cable traffic from Perth. In cooperation with SingTel, Australia plays a huge role in the overall bulk interception of telecommunications and internet traffic by the British *GCHQ*. The overall telecommunications traffic can be retraced from the UK, over Oman, Dijbouti, Singapore back to Perth. Besides the **SEA-ME-WE-3** undersea cable, there is also the **SEA-ME-WE-4** cable that runs from Singapore to the south of France.[44]

In early November, 2013, the Australian *The Sydney Morning Herald* published an article, revealing information from a former Australian Secret Intelligence Service officer, that the Anglo Australian multinational mining and petroleum company BHP was one of the companies, who were being helped by Australian spy agencies "as they negotiated trade deals with Japan".[45] The information was secret intelligence containing market information directly given to BHP and other major companies, and as result benefiting them.

[43] [57]
[44] [55]
[45] [56]

5.7 Metadata - connecting the dots

Metadata represent information, which unfolds its real power, if the right associations and conclusions are drawn from it. The more metadata is available, the easier it is to make those conclusions. In the European Union a policy (2006/24/EG[46]) exists since 2006, after which companies must retain connection data (or metadata), including e-mails, SMS, MMS, and telephone conversations for a duration between six months and two years, in the event when investigators want to legally access it to fight criminality.

On July 9th, 2013, the European Court negotiated on the legality of the controversial EU-directive addressing data retention. Applicants from Ireland and Austria expressed their view, that the groundless storage of traffic data from telephone and internet users would violate their fundamental rights. The European Court now checks in a preliminary ruling, whether the EU-directive in fact does violate European law.[47,48] Metadata allows for quick automated analysis, which works quite accurately and fast, and with the right tools detailed information can be drawn from it. How much information can be drawn from simple metadata, can show Google's e-mail service GMail and Facebook:

- GMail researchers at the Massachusetts Institute of Technology have developed a program called immersion. This allows the tool complete access to the user's own private e-mails, and all contacts are analysed researching the questions: Who has announced with whom? With whom has one exchanged particularly many e-mails? What contacts are especially interrelated?[49]

- The search engine Wolfram Alpha is able to examine the user's Facebook friends. This results in basically two graphs, which show the relationships between Facebook friends. At the same time, Wolfram Alpha is able to recognize different groups of friends, for instance university buddies, school friends, friends from the sports club etc. The graph also shows, which contacts are especially important for the cohesion of the network and who is taking bridge functions between multiple networks.[50]

With all the data in their databases, the NSA is able to build a 'pattern of life', an individual's profile including associated people with him. There also doesn't need to be a terror suspect talking to the individual so that the NSA starts to analyse his communication data. "The agency is allowed to travel 'three hops' from its targets - who could be people who talk to people who talk to people who talk to you." According to a study of 2011, the average number of friends a typical Facebook user has is 190 and 14% of those friends are friends with each other[51]. As such the number of friends of friends (2nd degree) will be 31,046, while the number of friends

[46] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:DE:HTML

[47] [169]

[48] As of April 8th, 2014, the European Court decided that the EU-directive is not admissible (cf. http://malte-spitz.de/wp-content/uploads/2014/04/CP140054DE.pdf).

[49] [73]

[50] [86]

[51] [198, p.2]

of friends of friends is gigantic 5,072,916, which is just over the population of St. Petersburg, Russia.

What information is given out through metadata, is illustrated in figure 5.2.

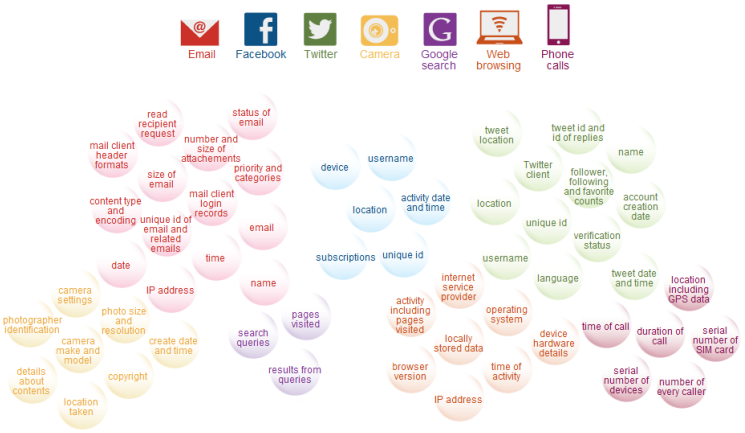


Figure 5.2: Personal information packed in Metadata: Comparison of mostly used internet services (reprinted from [26]).

The examples give a first indication on what individual companies know about their customers. Authorities can query this data (legally with judicial decisions), and merge for example the data from providers. ISP's often possess even more private information about their customers than IT-firms like Google or Facebook.

Researchers from Stanford University conduct studies on the amount and degree of detail of information metadata can provide. Surveillance activities from the NSA and other authorities are as such being examined scientifically. Interested users can download an app, which then transfers any metadata directly to the research group (see[52]).

5.8 US surveillance on European 'allies'

Documents leaked by the whistleblower Edward Snowden showed US intelligence service spying activities targeting the "European Union mission in New York and its embassy in Washington" and embassies of France, Italy, Greece, Japan, Mexico, South Korea, India and Turkey[53]. In total, the document lists 38 embassies and missions dating September 2010, which are spied on via a variety of spying methods including "bugs implanted in electronic communications gear to taps into cables to the collection of transmissions with specialised antennae". Dropmire is a codename for one of the bugging methods, which is "implanted on the Cryptofax at the EU embassy, DC". The machine is then used "to send cables back to foreign affairs ministries in European capitals". Presumably, the aim is to collect "inside knowledge of policy disagreements on global issues and other rifts between member states." This way the intelligence services make

[52] http://metaphone.me/learnmore

[53] [130]

sure to monitor written documents. Yet another layer of communication that is being under surveillance. The documents do not make exactly clear, whether the eavesdropping is done by the NSA, FBI, the CIA or a combination of them.[53]

It would not be a surprise, if the US would spy on their Five Eyes Alliance partners. After all, the US has been spying on their own American people.

NSA's ranking of intelligence priorities (espionage)

According to confidential documents dating April 2013 and leaked by Edward Snowden, the NSA uses a ranking of 'intelligence priorities' for other countries with a scale between 1 (highest interest) and 5 (lowest interest). Germany ranks in the secret list in the midfield, about on par with countries like Japan and France, while Italy and Spain are ranked lower. US intelligence service supposedly target the German foreign policy as well as questions about the economic stability and dangers to finance, which are marked with a 3. Other orders for surveillance comprise topics such as weapon exports, new technologies, highly developed conventional weapons and international trade, all of which are prioritised with a 4, whereas German counter-espionage is ranked with a 5, especially Germany's capabilities to use cyber attacks against US infrastructure. As expected, top targets include China, Russia, Iran, Pakistan, North Korea and Afghanistan.[54]

5.9 NSA and data from US citizens

While the NSA officially states that it destroys communication as soon as it is related to US persons, the same does not apply for encrypted communication. Encrypted data is retained by the agency, to further its research and assessment into cracking encryption (huge investments of $440 million a year in order to crack Secure Sockets Layer (SSL) and Transport Layer Security (TLS)[55]). Moreover, the NSA stores encrypted communications for any period of time:

> *In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.*[56]

Also, the use of the 'wrong' encryption program can make one a NSA target. 'Wrong' is hereby referencing specific types of cryptology that are from the NSA's standpoint associated to be used by individuals from foreign territories.[57]

Edward Snowden's documents revealed that British and US intelligence services have "successfully broken or circumvented much of online encryption"[58]. It was done not through the traditional way of code-cracking, but rather by making business deals with companies in the

[54] [32]
[55] [186]
[56] [28, p.5 sec.5.3a]
[57] [217]
[58] [26]

industry. Thus, they were able to introduce backdoors and weaknesses into commercial encryption. According to computer security experts, intelligence services that way, have compromised hundreds of millions computers of internet users, "and undermined one of their other key priorities - protecting the US and UK from cyberattacks"[58].

According to an article from the *Wall Street Journal*, the NSA's surveillance network "has the capacity to reach roughly 75% of all US Internet traffic", comprising various communication channels of foreigners and Americans[59]. Programs that were mentioned being involved in the system to filter and gather information at major telecommunication companies included "code-named Blarney, Fairview, Oakstar, Lithium and Stormbrew, among others", all systems mentioned, but not explained in detail, in the documents provided by Edward Snowden[59].

Loophole in FISA Amendmend Act 702

The FISA of 1978 was established to limit the NSA's ability to use its resources and power against Americans. For the first time it defined in law, "that the NSA was about foreign intelligence"[60]. In case of a suspicion about spies from foreign powers operating inside the US borders, intelligence services like NSA and FBI would be able to apply for a warrant in the FISA court. Since then, the work of intelligence services and especially their compliance with laws has become more and more secret. In 2012, the 2008 FISA Amendments Act was renewed, allowing the "collection of communications without a warrant, where at least one end of the communications is a non-US person"[60]. Considering the fact, that the FISA court "and its proceedings are secret", it is almost impossible to dispute its perception of the law[60].

According to an article from *The Guardian*, a loophole was found in Section 702 of the FISA Amendmend Act, "which gives the NSA authority to target without warrant the communications of foreign targets". A disclosed document revealed a previously secret rule change, that gives the NSA permission to search databases for specific US individuals' communications, provided the identifying information (e.g. name). The official passage states:

> *While the FAA [Foreign Intelligence Surveillance Act Amendments Act Section] 702 minimization procedures approved on 3 October 2011 now allow for use of certain United States person names and identifiers as query terms when reviewing collected FAA 702 data, analysts may NOT/NOT [not repeat not] implement any USP [US persons] queries until an effective oversight process has been developed by NSA and agreed to by DOJ/ODNI [Department of Justice/Office of the Director of National Intelligence].*[61]

So, while the NSA theoretically could have accessed databases with the intent to look for American's data without a warrant, it is stated that NSA analysts are forbidden from doing so until "effective oversight" is in place. However, there is no information that mentions if or when the 'oversight process' ever came into effect.[61]

[59] [87]
[60] [26]
[61] [37]

Crossing the line

The fact that the NSA has crossed its boundaries several times is described in an internal report of the intelligence service, leaked by Edward Snowden. According to the *Washington Post*, since 2008 every year the NSA has broken thousands of data protection rules, or at least exceeded its authority. Most of the violations have been occurred at unauthorized surveillance of Americans or other targets in the US. The NSA declared most of them as incidents by mistake or by accident, including presumable programming mistakes which resulted in the wrong calling code (Washington: 202 with Egypt: 20) or letting the program recording, although the particular permission already expired. The most serious incidents have involved the violation of a court order and the unauthorized use of data from more than 3,000 US citizens and green card holders. Moreover, in one of the documents NSA employees had been instructed to remove details from the reports directed at the Ministry of Justice and the head of the intelligence services, or at least choose more general formulations. In numbers, 2,776 incidents have been listed in a confidential quarterly report from 2012 for the last 12 months, counting in only the Washington area of the US. The numbers worldwide would turn out significantly higher. An incident is described as "unauthorized collection, storage, access to or distribution of legally protected communications.", which means that probably e-mails have been read, social networks analysed and communications viewed[62]. The systems most commonly used are XKeyscore and the NSA database Pinwale (see previous sections).

Violations happen, and if they happen they are mostly reported. But, sometimes they cannot be dealt with to be investigated by the FISC. This is illustrated through a statement by the FISC, which on request by the *Washington Post* said:

> *The FISC does not have the capacity to investigate issues of non-compliance, and in that respect the FISC is in the same position as any other court when it comes to enforcing [government] compliance with its orders.*[63]

In addition, the "leader of the secret court that is supposed to provide critical oversight of the government's vast spying programs said that its ability to do so is limited and that it must trust the government to report when it improperly spies on Americans." Trust is clearly a inappropriate term to be used in relation to intelligence services, as recent events have shown.

In an interview with the *Washington Post* a senior NSA official said: "We're a human-run agency operating in a complex environment with a number of different regulatory regimes, so at times we find ourselves on the wrong side of the line", which once more shows the lack of consciousness dealing with sensitive data of millions of people and the urgent need for a global reform.[64]

Again, this serves as a display of vulnerability for such large systems involving Big Data. Whether the surveillance of US Americans was intentional or not, the collection of that much information, involving hundreds and thousands of resources (both human and technological) results in incidents like these, which is undoubtedly a violation of privacy.

[62] [79]
[63] [124]
[64] [79]

5.10 Genie

According to an article from the *Washington Post*[65], 231 offensive cyber-operations have been carried out by US intelligence services in 2011, of which almost 75% were targeting "top-priority targets", including Russia, China, Iran and North Korea. Cyber-operations are defined by US agencies as activities designed "to manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves", according to a presidential directive from October 2012.[65]

The article from August 30th, 2013 also states that worldwide 85,000 computer systems are presumably infected by espionage software. The NSA would plan to control them as some sort of gigantic Botnet. Codenamed '**Genie**', the operation's target is primarily attacking the worldwide computer infrastructure. The infections are described as 'covert implants', basically trojans. NSA-software helps to control the infected systems unnoticed and to apply commands. The main purpose is to use malware on strategically selected targets, in order to gain control over whole networks. The installed programs are supposed to be able to copy data and record communication, as well as intruding other connected networks. This is not about targeted monitoring of certain systems because of suspicions, but about creating opportunities by making systems unsafe for no specific reason. Instead of warning the operator about security vulnerabilities, the NSA exploits them to be able to access the machine at a later time. At this point, the often proclaimed term 'trust' is devalued. The resources are developed by the NSA-unit TAO. According to the article, the organisation possesses a wide range of specifically developed malware, specializing on particular devices and security software. Also, the NSA is mainly responsible for developing their own viruses and trojans, but they also are presumed to have bought security holes externally from the grey-market, referring to investments for that purpose of 21.5 million dollars in 2013 alone. This creates a dilemma. The NSA buys an information advantage, when the authority gets knowledge of previously unknown existing vulnerabilities in often used software. However, if the NSA would decide to warn other manufacturers and experts directly afterwards, the agency would instantly lose their information advantage. Therefore, it makes more sense to make use of the knowledge and exploit the vulnerabilities, before they are revealed to the public. The need for more IT-security contradicts here with interests of the US government to effectively operate cyber attacks. Furthermore, the Genie program was controlling 21,252 computers in 2008, planning to reach 85,000 in 2013. Infecting the first computer usually allows access to most of the others in the network. The trojan would often create backdoors for later access, meaning the trojan would remain hidden and unnoticed. In 2011, 8448 computers have been 'exploited' of 69,000 infected systems in total, referring to the limited resources (1870 employees) that can be allocated at a time.[65]

Future plans include an automated system codenamed 'TURBINE', that is supposed to be able to control NSA's 'implants' and be used for active attacks or the collection of information.[66]

Genie rounds up reports about TAO's purpose for the NSA, using hacking attacks with sophisticated tools, which allow NSA analysts to analyse the data and derive conclusions from it.

[65] [82]
[66] [82]

Exploitation

Genie's main purpose is to exploit foreign systems. Exploitation is according to the intelligence budget summary defined as: "urreptitious virtual or physical access to create and sustain a presence inside targeted systems or facilities." Moreover, "system logs and processes are modified to cloak the intrusion, facilitate future access, and accomplish other operational goals"[66]. Besides designing their own tools for intelligence gathering, the NSA also invests $25.1m (2013) in "additional covert purchases of software vulnerabilities" from external sources, such as "private malware vendors, a growing grey-market industry based largely in Europe"[66].

According to the article from the *Washington Post* from August 30th, 2013, the operators from ROC and Genie concentrate their efforts on finding suspected terrorists in "extremist safe havens", including Pakistan, Iraq, Somalia and Afghanistan[66]. But not only the TAO at the NSA has increased its work efforts. The CIA also has an intelligence centre, called Information Operations Center (IOC), which is mainly employed to focus on cyber-security, shifting from their previous agenda dealing with counter-terrorism.[66]

In order to handle the increasing volumes of data, the NSA is building a massive new data centre in Utah. Another one is built at Fort Meade. Both are supposed to help with the sheer storage demands, as well as more efficient "analysis and intelligence production"[67]. Intelligence agencies should then be able "to evaluate similarities among intrusions that could indicate the presence of a coordinated cyber attack, whether from an organized criminal enterprise or a nation-state."[67]

USA's ROC

Remote Operations Center (ROC) is a NSA facility, where TAO's elite operators are based "to fight the cyber-war against the best of the NSA's global competitors"[68]. So any active operations are presumed to go out from that location. Alongside the ROC there work the CIA, FBI and the US Cyber Command "with overlapping missions and legal authorities", whereas the NSA's National Threat Operations Center focuses on cyber defence. One of the tasks of ROC teams in cooperation with the Cyber Command is to provide "specific target related technical and operational material (identification/recognition), tools and techniques that allow the employment of U.S. national and tactical specific computer network attack mechanisms"[68].

The total cyber operations budget in the US amounts to $1.02bn (2013). ROC's missions, with the support of the Genie infrastructure, cost $651.7m.[68]

5.11 Social Media Intelligence - SOCMINT

A new 17-man unit was discovered in June of 2013, undertaking extensive surveillance of public social media conversations of British citizens continuously since the London riots in 2011. As part of the Metropolitan Police, the National Domestic Extremism Unit (NDEU) takes advantage of the huge potential of social media, by collecting intelligence through services like

[67] [82, p.3]
[68] [83]

Twitter, YouTube and Facebook, where content and personal information is created daily. Social Media Intelligence (SOCMINT) is a new form of spying techniques, similarly to fundamental approach of SIGINT and HUMINT. The unit is operating 24/7 and uses "an alarming array of sophisticated analytical tools", including 'sentiment analysis' that is able to determine ones mood, 'horizon scanning' that tries to predict crime or unstable condition, facial recognition software, geo-location, as well as profiling[69]. According to the head of open source intelligence of the Metropolitan Police, Umut Ertogral, "[Social media] almost acts like CCTV on the ground for us. Just like the private sector use it for marketing and branding, we've developed something to listen in and see what the public are thinking"[69]. This was said during a private presentation at an Australian security conference. The main difference to the Prism program is the fact that SOCMINT focuses on information that is publicly available, "be it intentional or through ignorance". Thus, it is difficult to pinpoint the requirements for legal protection. Undoubtedly, privacy is an issue and demands for a proper protection through both legislations and regulations in order to prevent abuses. The fact that current legislation which is supposed to represent a guideline for such cases dealing with social media, such as the "Regulation of Investigatory Powers Act (RIPA), were passed at a time when Facebook and Twitter didn't exist", shows once again how slowly laws are adapted to the fast growing technology internet. Also, there is no clear framework whether targeting public social media data should require permission or a "ministerial sign-off", because the data is basically publicly available, though it is highly questionable that using techniques such as profiling and creating detailed analysis of private data should be allowed without any regulation and authorization. Most of the time such programs involving intelligence gathering are nevertheless operated in secret and on a massive scale, as shown rarely respecting the line between private and public information.[69]

Again, the reasons for such actions are described as being "necessary to protect communities" and that the police "have a duty to uphold the law and prevent and detect crime"[69]. According to an article from the *Guardian*, the NDEU "had a secret database that had labelled some 9.000 individuals [...] as domestic extremists".[69]

5.12 Resistance movements and control instances

In regard to the recent developments in global surveillance, several entities and groups have shown signs of resistance, denouncing the vast gathering of intelligence. Three respected British organizations - Big Brother Watch, the Open Rights Group and the English PEN - have announced to sue the British intelligence and the government, which is in charge of the GCHQ. They don't want to accept the million-fold intrusion (Tempora) in the secrecy of communication of not only the British but also of Europeans and Americans. It comes down to the fundamental question of whether the UK law and the practice of mass surveillance break international law. For the first time, the European Court of Human Rights will deal with questions, which appeared with Edward Snowden's revelations. The civil rights organization Electronic Frontier Foundation has already years ago initiated a proceeding (Jewel vs. NSA) in the US, when it was discovered that the NSA uses a program codenamed 'Upstream' to go through Internet traffic,

[69] [214]

filter information and partially store data. Since 2008, they are waiting for a decision. Hopefully this time around it will not take so long for the Europeans. Whether the American mantra is applicable in Europe, when during the search of a needle, first a haystack has to be hoarded, is, according to the wording and intention of the European Convention on Human Rights, doubtful.[70]

The German Control Panel

In Germany, eleven members of the Parliamentary Control Panel (Parlamentarisches Kontrollgremium) are interior- and security experts from all parliamentary groups (Bundestagsfraktionen). They meet in a bug-proof, windowless room in an outbuilding of the Reichstag. Since the work of intelligence services by nature is secret, the group is sworn to secrecy, even from other members.

True control over intelligence services is hardly possible. 11 parliamentarians are supposed to overlook what thousands of agents are doing at home and abroad?

In addition to the PKG (Parlamentarisches Kontrollgremium), there is also the Bundestags-based G-10 Commission, which is responsible for the control of intelligence services. The name of the Commission refers to the Article 10 Act (Artikel-10-Gesetz[71]). This committee also meets in secret. It has four members, who are appointed by the PKG and have to be members of the Bundestag.

The G-10 Commission has to give its approval, when intelligence services want to tap computers or phone to spy on German citizens. Also the search of communication data for specific keywords must first be approved by the Commission. In 2011, the board had approved a total of 156 domestic intelligence wire-taps. The reasons for this are set out in the Act; among other things, it describes the spheres of counter-terrorism, arms and drug smuggling and organized money laundering. However, the BND is also able to apply at the G-10 Commission to access Internet backbones for large-scale data collection. A comprehensive surveillance operation is prohibited, the law has set a limit of 20 percent. According to Commission chief Hans de With, the true number would be at 5%.[72]

5.13 Other activities

Monitoring German communications

In late June 2013 it was discovered that Germany is also targeted by NSA's surveillance programs. Presumably, about 0.5bn telephone communications, e-mails and SMS are monitored and metadata collected by the NSA every month. With these numbers, Germany represents the target which is monitored the most in the EU. According to an article from *Der Spiegel*, the NSA sees Germany as a partner, but also as a target. Accordingly, Germany belongs to the so called 'third-class' partners. Countries, which are excluded from this and belong to the second-class

[70] [120]

[71] law on the restriction of correspondence, posts and telecommunications secrecy

[72] [139]

category are Canada, Australia, Great Britain and New Zealand, all of them members of the Five Eyes alliance.[73]
This fact serves again as a reason for why the argument of fighting against terrorism is implausible. Although German and European officials, too, repeatedly express astonishment and rejection, no real actions are taken in regard to potential sanctioning. US intelligence services pursuit the total control, where only the own country and the other countries part of the Five Eyes matter and can be relied upon. As such the EU enqueues in an equally targeted position as countries like Russia, China, and meanwhile India are in.

French surveillance

France uses also surveillance programs, similarly to British and US programs that have been disclosed during the events of June/July 2013. According to French newspaper *Le Monde*, the French intelligence service Direction Générale de la Sécurité Extérieure (DGSE) uses similar techniques to collect data from digital communications. In particular, the article states that signals from computers as well as telephones are intercepted, including communications between France and foreign incoming or outgoing communications. While the contents of conversations are not targeted, the purpose of the surveillance operation is rather to create an overview or map, showing who communicates with whom. In doing so, the DGSE seems to act illegally, intercepting e-mails, SMS, connection data, and saving detailed information on the use of social media platforms like Twitter and Facebook for years. It is presumed that the DGSE stores all the collected data in the basement of their headquarters in Paris. Furthermore, all the other 7 French intelligence services are supposed to have access to the data, who, depending on their suspicions, are able to enter communications and eavesdrop on conversations.[74]

US hacking Hong Kong and China

According to whistleblower Edward Snowden, the US government, more specifically the NSA, has been using the Prism programme on targets in Hong Kong as well as mainland China. Since 2009, there were hundreds of such attacks. Worldwide the number even amounts to 61,000 attacks. The NSA would especially target large network backbones, in order to get access on communications from several thousand computer systems at once, instead of targeting each one individually. The attacks would target specifically important governmental, economical and educational institutions.[75]

Another article revealed, that during a four year period major telecommunication companies in China have been extensively hacked in order to access text messages. Included in the attacks were network backbones at one of China's premier Universities, and computers belonging to Pacnet - a pacific fibre optic network operator - located in Hong Kong. Pacnet "owns more than 46,000 kilometres of fibre-optic cables" and basically covers the whole Asia-Pacific region.

[73] [163]
[74] [71]
[75] [121]

Snowden also claimed "that data from Chinese mobile phone companies has been compromised, with millions of private text messages mined by the NSA."[76]

5.14 Industrial Espionage as part of NSA's mass-surveillance

After the disclosure of internal documents from the NSA and their partners, several operations have been discovered involving industrial espionage activities. The approach of the intelligence services to gather intelligence allowed for (cyber) espionage activities. The direct interception of communication data is possible at undersea cables, like we've seen in the chapter about Tempora; the same capabilities for espionage are provided by IT-service providers.

Cyber attack on Belgacom

Not only China is using hackers, in order to infiltrate foreign companies. Hackers in the service of the GCHQ have attacked the Belgium telecommunications company Belgacom, in order to get access to their special router for mobile-radio roaming for the use of surveillance measures. Apparently, a software by the NSA was used during the cyber attacks. According to insights of *Der Spiegel*, 'top secret' documents have shown that the GCHQ is operating a project co-denamed 'operation socialist'. The presentation is undated, however, it states that the access is established since 2010. In particular, the Belgacom subsidiary Bics, a joint venture with Swisscom and South African MTN, is targeted by British authority. Belgacom provides services to institutions like the EU-Commission, Council and Parliament. During the course of the NSA-related disclosures, the company had issued an internal investigation and had found cyber attacks, presumably executed by either GCHQ, the NSA or both, dating from two years ago. The cyber attacks presumably included monitoring of conversations and the collection of strategic information.[77]

According to the GCHQ slides, the attack ran across several Belgacom employees, who without a notice have got the spyware with the help of a technology called Quantum Insert (QI). Apparently, this is a method, which forwards their targets to specific websites without their knowledge while they are browsing, and then the malware is infiltrating their systems, which then serves for means of manipulation. That way, the authorities have gotten direct access to Belgacom's infrastructure and as such the whole company's network. As stated, the aim was getting access to the central roaming routers of the Belgians. Those routers serve for the handling of international traffic. Also, the GCHQ wanted to use their access for special man-in-the-middle attacks targeting smartphone users.[78] The presentation slides indicate an involvement of the GCHQ's Network Analysis Centre (NAC), the equivalent to the American TAO - an elite hacker unit inside the intelligence agencies.[79]

The complex nature of the attacks suggests that the target has not been Belgium, but rather the international organisations that are located around the area of Brussels.

[76] [122]
[77] [98]
[78] [30]
[79] [12]

This event serves as an example of a series of security vulnerabilities. First of all, Belgacom is an internet exchange point and probably the best way to get hands on communication data. For an intelligence agency, having there a backdoor means the most important monitor source available. Now, the British authority made targeted attacks at the systems of Belgacom's network engineers to get access to the switches. Therefore, one can conclude that network engineers have been the primary target from the beginning. Accordingly, engineers have to think about their operational security, meaning whether their systems should provide (administrator) access to the switches and perhaps access to e-mail, social media etc. This illustrates a perfect example, how systems are attacked with malware, to get access to the real target, the high-value infrastructure.

Spying on the G-20 summit

Another article mentioned spying operations by the GCHQ on participants of the G-20 summit meetings, which took place in London in 2009, comprising eavesdropping on computers and telephone communications. During the summit, several espionage techniques have been used, including[80]:

- Specifically set up internet cafés, where e-mails could be intercepted and key-logging software used.
- "Penetrating the security of delegates' BlackBerry phones" allowed the monitoring of e-mails and phone calls.
- 45 analysts were able to follow exactly who was phoning whom at any point of time.
- The Turkish finance minister including 15 others in his party were presumably targeted.
- NSA's made efforts to intercept and decode encrypted phone calls made by the Russian president Dmitry Medvedev and other Russian delegates from London to Moscow.

The operation was running for at least six months. The live feed of phone conversations and e-mail communications was realised using a new technique. The activities were displayed "on a graphic which was projected on to the 15-sq-metre video wall of GCHQ's operations centre as well as on to the screens of 45 specialist analysts who were monitoring the delegates"[81].

... and the United Nations headquarters

Similarly, the NSA had monitored the United Nations headquarters in New York, according to information from *Spiegel*. In summer 2012 the NSA succeeded to intrude the internal video conference system of the United Nations Organization (UNO) and to crack the encryption. According to a secret NSA document, this actions have been "a dramatic improvement of the data from video teleconferencing and the ability to decrypt this traffic"[82]. Within three weeks, the number of decrypted communications had increased from 12 to 458.

[80] [132]
[81] [132]
[82] [25]

In another case during that time, the NSA had also caught the Chinese intelligence spying. Afterwards, the NSA intercepted those communications, which had been previously eavesdropped on by the Chinese. Of course, those espionage operations have been and still are illegal.[82]

Special Collection Service

According to confidential information coming from NSA documents that *Der Spiegel* has evaluated in August 2013, the NSA maintains an own surveillance program, that is internally called Special Collection Service (SCS), in more than 80 embassies and consulates worldwide, of which 19 are located in Europe.[83] Frankfurt and Vienna are described as two of the many locations, where embassies or consulates have been functioning as surveillance spots. According to the internal documents, the existence of the eavesdropping units in these locations should be kept secret at all costs. If they were known, it may cause serious harm to the relations with the host-country. Furthermore, *Spiegel* reported that from the US embassy in Berlin, a secret special unit from the CIA and the FBI are able to intercept and monitor a part of the mobile phone communication in the government quarter, including the mobile phone of German Chancellor Angela Merkel. This reaches a new peak in terms of global surveillance and endangers the transatlantic partnership between nations. As a result, the planned free trade agreement between the US and the EU is questioned.

From a confidential NSA paper of 2010 follows that an elite unit called SCS operates in Berlin under the command of both the CIA and the NSA. The elite unit members are accredited as diplomats, employed in restricted areas of the US embassies and consulates. In general, any surveillance action outgoing from an embassy is illegal. The SCS operate tapping systems, which they use to basically eavesdrop on all methods of communications, including mobile phone communication, Wireless LAN networks and satellite communication. The necessary equipment is usually installed on top of the buildings, right on or near the roofs. Right beneath them are presumed to be working stations of the SCS members, including "serverracks" for the signal analysis. One of the antenna systems is codenamed 'Einstein' and the corresponding control device 'Castanet'.[84]

Besides the interception of communication, the equipment can be used to locate a targeted object. Some programs like 'Birdwatcher', which is directly operated from the SCS headquarters in Maryland, are geared to 'catch' encrypted communications in foreign countries and to search for possible access points. From some embassies, Americans have even smuggled sensors, which are able to react to specific keywords, into communication facilities of the respective host countries. There is no information on the kind of intercepted communications, whether everything was collected, the contents or just metadata. Besides, the US president signs the order of particular targets, and the ongoing surveillance presumably needs to be renewed roughly every 18 months.[85]

[83] [5, p.22]
[84] [5, p.22]
[85] [5, p.23]

In the end, this incident will result in new investments into the IT-infrastructure by intelligence services, in order to increase their own technical capabilities, because one fact is for certain: The NSA has one of, if not the best and sophisticated surveillance apparatus in the world.

Smartphone surveillance

The NSA is able to access user data of smartphones from all leading companies, including iOS, BlackBerry and Android devices. According to internal documents, accessed by *Der Spiegel*, it is enough to get access to a computer, which the user is synchronizing the smartphone with (e.g. iPhone).[86] Scripts afterwards allow the direct access to at least 38 iPhone applications. Also, the SMS-communication in the - regarded as relatively secure - BlackBerry was infiltrated and readable by the NSA back in 2009. After the BlackBerry company had introduced a new compression method in 2010, it took only a couple of months for the GCHQ to crack it. According to the article, the information provided to the newspaper concern leads to the conclusion that this approach is not necessarily used for mass surveillance, but rather is targeted at specifically constructed operations, without the user's notice.

The infiltration presumably goes as follows: The NSA breaks into the computer and infects it with some malware. The program is installed on the smartphone device as soon as it is synchronised with it. It is also imaginable that some malware is installed through an update. If there is an update channel, and the update company is located in the US, then it is possible that the NSA is able to infiltrate the device that way. There is still the risk involved in hacking the computer first though.[87]

Monitoring of international transactions

There are also enough examples that NSA's wide reaching surveillance not always indicates the hunt for terror suspects. For instance, according to reports, the NSA monitored money transfers via the international bank network SWIFT (is regularly used for data exchange between banks). The Brazilian oil concern Petrobras was also targeted by the agency, indicating the use of industrial espionage. Glenn Greenwald, the main publisher of Edward Snowden's leaks, said, he possesses some documents, which contain much more information about the spying of innocent people, of people who have nothing to do with terrorism or economic information.[88]

Another indicator is the monitoring of international payment transactions. According to a an article from *Der Spiegel* from September 15th, in 2013 the NSA collected 180 million data sets related to financial transactions, including those of VISA. The NSA branch 'Follow the Money' is responsible for financial data. The collected information is stored in NSA's finance database called 'Tracfin'. In 2011, 84% of the 180 million data sets have been credit card data.[89]

On allegations of economic espionage, director of national intelligence James R. Clapper stated the following:

[86] [99]
[87] [99]
[88] [191]
[89] [14]

We collect this information for many important reasons: for one, it could provide the United States and our allies early warning of international financial crises which could negatively impact the global economy. It also could provide insight into other countries' economic policy or behaviour which could affect global markets.[90]

What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of - or give intelligence we collect to - US companies to enhance their international competitiveness or increase their bottom line.[90]

Considering these statements and clear indicators shown in recent months and other statements from former agency-officials, it is highly doubtful, that the US would not use their intelligence capabilities for espionage purposes. It remains to be seen, what more information is to come out from Edward Snowden's documents in the near future.

5.15 NSA's budget

In late August 2013, Edward Snowden had leaked the 'black budget'[91], the congressional budget justification for fiscal 2013. The budget of intelligence services in general is kept secret, but it gives a good overview of priorities that are set and how much effort is undertaken to reach the goals. The secret document shows, "that 21 percent of the intelligence budget, around $11 billion, is dedicated to the Consolidated Cryptologic Program that staffs 35,000 employees in the NSA and the armed forces"[91]. That's just for dealing with cryptology (including encryption-breaking efforts). In total, the intelligence budget amounts 52.6bn dollars. James Clapper, director of National Intelligence, stated in the document: "we are investing in ground-breaking cryptanalytic capabilities to defeat adversarial cryptography and exploit internet traffic", showing clear intentions of set priorities to create encryption-breaking methods, and with that give the agency even more potential of violating privacy and conducting espionage[91]. The document also states that the counter-intelligence operations are targeting mainly following priority targets: "China, Russia, Iran, Cuba and Israel"[92].

The US comprises 16 spy agencies that belong to the US intelligence community, and which in total have 107,035 employees. The document also revealed that the CIA gets roughly 50% more budget than the NSA (10.7bn), amounting to 14.7bn dollars.[92]

The numbers also show that US have also invested more than $500bn on intelligence since 9/11. "The result is an espionage empire with resources and a reach beyond those of any adversary, sustained even now by spending that rivals or exceeds the levels at the height of the Cold War"[92].

[90] [47]
[91] [164]
[92] [81]

5.16 Trivialization associated with reasoning

The terms *terrorism* and *child's pornography* are often used in relation to the sheer collection of data. However, one study of many, e.g. the one done by scientists of the Max-Planck-Institute, haven't found an indication that data retention has been successfully used to prevent a terror attack or has yielded any great results in discovering child's pornography[93]. The Boston bombers in 2013, for instance, have been two men, fairly active on the internet (forums and social media), but have never been marked as suspects.[94] Reasoning from German Minister of the Interior Friedrich the program Prism would have been effectively used to prevent at least 5 terrorist attacks, shortly after had to be corrected to 2[95]. Crimes associated with computer fraud are probably elucidated better with the help of data retention, but does that also justify such an enormous impact on fundamental rights of all citizens? The terms of terrorism and child's pornography are used for one important reason, namely to force humans to react emotionally.

Meanwhile, the corresponding representatives of the EU level have to make sure that the US and at least Europe get the necessary reforms and guidelines, fitting today's far developed technology. In general, of course the term cryptology needs to be present in today's information society including individuals as well as companies to secure privacy and industrial/economic values.

Hackers have been warning the public for a long time of a total surveillance system, but it needed one man, namely Edward Snowden to make it official and present in everyone's minds[96].

In the end one thing becomes apparent: Namely, that the war on terror is a simply fictitious war.

5.17 Analysis

Authorities always try to argue that collections of data are necessary to search more effectively for terrorists and criminal suspects. But history shows that mistakes happen, and the more data is collected, the less privacy an individual can expect to have, the higher the risk of being targeted due to coincidental events. The system that US authorities have established is a system that doesn't fit in a democratic constitutional state, because it is an invasion of the privacy and fundamental rights of individuals at any time, without the existence of a true constitutional control mechanism. The NSA is military, and the intrusion on civilian communications through the NSA is basically nothing else than a "militarisation of domestic communications infrastructure"[97].

For the US it is not all about the security any more. It is all about the control of data and therefore of people, hurting privacy and freedom rights.

Back then, ECHELON represented a new approach. With the antennae in the white domes located at the various bases of the Five Eyes alliance not only telephones were monitored, but *all* telecommunication, which then was filtered with the use of certain keywords. The collection

[93] [170]
[94] [206]
[95] [77]
[96] [102]
[97] [93]

of data came first, then the filtering process. That way the whole worldwide satellite communication was under surveillance, except the internet, which due to limited capabilities was difficult to eavesdrop. Now, the programs Prism, Tempora and XKeyscore in particular, showed how this state has systematically changed over the years. The surveillance of fibre-optic cables became an important part of cyber espionage. Data that run through the internet are usually encrypted. In order to minimise the efforts of cracking the code, intelligence services let ISPs and IT-companies hand them over unencrypted data. And the collection of data does not end here. The US (Intelligence Community Comprehensive National Cybersecurity Initiative Data Center in Bluffdale, Utah (cf. [98])), as well as Great Britain (plans of increasing capacities to handle more fibre-optic cables) are investing billions (estimations are 1.5-2bn) of dollars to establish large surveillance centres, which contain immense server infrastructures in order to be able to analyse and evaluate data even more efficiently. The Data Centre in Utah for instance is supposed to create room of 100.000 to 150.000 square meters. 65 Megawatts of electricity and 4500 litres of cooling water are needed each minute. The IT-hardware itself is supposed to create space for yottabytes of data (1 yottabyte = 1bn terabytes).[98]

The internet is a global room for communication and a storage for private information for millions of people. Both intelligence services GCHQ and the NSA have created an all-seeing-eye codenamed Tempora, which allows to inspect the sheer volume of data that is exchanged over the internet and is stored on enormous servers. Both agencies cooperate in the surveillance of internet traffic, by directly intercepting data-flow that runs through fibre-optic cables, copying, storing and if necessary analysing it. The US government has even paid at least 100m British pounds of secret founding to the GCHQ over a period of 3 years in order to secure access to the intelligence and gain influence over "Britain's intelligence gathering programmes"[99]. Main reason being, that the UK is less regulated than the US, which made it a key 'selling point' for the British agency.

The irony is that the people responsible for these programs don't even take great care to deny their works. Everything seems to serve the greater good and thus is necessary to fight crime and hunt terrorism. But would a democratic public agree to a total surveillance system, the all-seeing-eye, only to observe a terrorist's actions? And would it agree to look at the facts only if an intelligence service analyst sees the importance of doing so? Probably not. As such, it can only be seen as a scandal of historical magnitude that the US, Britain and several other nations claiming to be democratic countries have created a world-wide surveillance system. Disclosed documents created a clear view on the systematic lies the government spread regarding topics and discussions about internet data privacy and data retention. And even if government officials are confronted with the facts, they either decline to answer or answered only half the truth. There is clear evidence on the one hand, on the industrial espionage operations and on the other hand, the systematic surveillance of the public. The following months will show whether the democratic public of the world is able to resist the boundless, totalitarian claims of Western intelligence. Considering how long legislation and governmental regulations have been lagging behind the development of the internet in the digital age, now is the time to do something about it.

[98] [160]
[99] [101]

The internet also showed a number of weak points, proving that no intelligence service in the world can guarantee for the data they collect. As such, no data on that scale should ever be collected and stored. The result of total security policy is that the public's security is endangered by means, that supposedly should have served to protect.

A step into the right direction would now be the control of the data infrastructure by European institutions and the protection of it. The freedom of data traffic nowadays counts as much as European freedom for money, services and goods. And this is only achievable by putting an end to the desire of systematic surveillance. It is the main task of national governments in Germany, Austria and other democratic nations that data, especially private information, is not subject to surveillance activities any more in near future.

Prism (and to some degree Tempora) is not about getting just some information from service companies like Google or Microsoft, it's all about tapping all the internet's information flows at the internet's core, the network nodes.

Edward Snowden has repeatedly stated that with his action he didn't want to endanger any person or legitimate operations. That's the reason why the documents don't reveal any names of persons or concrete operations. The documents mainly contained the features of surveillance programs operated by the NSA and their alliance partners. The advantage of the NSA leaks is that the world can see what today's technology is capable of. The downside to it is however, that authorities of other countries such as Australia (cf. [100]) and Russia (cf. [101]) feel they need to 'catch up' with the fast growing development we have been able to observe over the last couple of months and years.

Skype shows an example, how something is taken as being secure, then sold to the US, and now it's been made less secure on purpose. Belgacom illustrates another example, how it is not all about the fight against terrorism. The espionage operation targeting the telecommunication company has proven, that cyber espionage is more apparent than ever, and that technologies created for one purpose (fight criminality etc.), are - when necessary - used for other means as well. Privacy is violated, and with it human rights and fundamental freedoms. And just because of the secretive nature of this topic concerning intelligence services, one surely has just seen the tip of the iceberg.

[100] http://www.theregister.co.uk/2013/08/22/asio_beefing_up_telecoms_interception_teams/

[101] http://www.spiegel.de/netzwelt/netzpolitik/russischer-geheimdienst-will-internet-kommunikation-speichern-a-929033.html

CHAPTER 6

Risks associated with global surveillance and cyber espionage

In this chapter, a short overview is presented on several risk factors addressing governments, companies, educational institutions, providers of critical infrastructure and the individual, originating from the technological capabilities and opportunities that emerged alongside the internet.

6.1 Big Data

Big Data in general refers to the collection of data from various sources on to servers, where it is usually being analysed, e.g. for marketing purposes. In March 2013, the CIA's chief technology officer held a presentation in New York at a Data conference on CIA's work and mentioned Big Data as being an essential and necessary tool under the premise to protect national security. According to him, it's necessary to take advantage of all the data emerged on the planet. As such, it is important to "revolutionize Big Data exploitation", meaning to acquire, federate, secure and exploit any data available[1]. Big Data is a term describing the collection of all data, relations of which can be analysed to form conclusions. During the presentation, Big Data is also described as resulting from the combination of '*Social* + *Mobile* + *Cloud*', indicating that Big Data could emerge from those 3 main (digital) services / technologies. Hunt further said: "The value of any piece of information is only known when you can connect it with something else that arrives at a future point in time," and "since you can't connect dots you don't have, it drives us into a mode of, we fundamentally try to collect everything and hang on to it forever"[1]. On a slide from Hunt's presentation it says: "It is nearly within our grasp to compute on all human generated information", clearly showing how far Big Data already has come. Ironically, he also mentioned that "technology in this world is moving faster than government or law can keep up. It's moving faster I would argue than you can keep up: You should be asking the question of what are your rights and who owns your data." Clearly, all this information on CIA's and other governmental

[1] [189]

authorities' work expresses the need for public attention. In a democracy, like the US claims to be, privacy is one of the most fundamental rights a person can have, and thus the decision of how far it should be interfered with, must lie in his hands.[1]

Big Data can also be seen as a synonym for NSA's working methods. Big Data is often mentioned in relation to efficiency. Big Data promises more efficiency, allowing to create faster and more accurate results. Now, with the collecting mania of authorities, the prospect of efficiency has reached the governmental level. The nature of (democratic) governments is to work inefficiently, so that one can intercept it at the right time in order to prevent damage. Transparency to some degree also creates inefficiency. If a (unscrupulous) government now tries to reduce transparency, the idea of democracy disappears. As a result Big Data and democratic ideals cannot go hand in hand.

6.2 Objects turning 'smart' - customer surveillance

Gadgets and devices with internet access (3G, LTE, WLAN) are already used by companies to track their customers' habits. E-book readers allow the companies to follow the reader's taste and habits in order to create a customer profile as accurately as possible and show personalized advertising. Ideas already involve the tracking of students' reading behaviour to check if the required passages of content have been read & learned. The term 'Big Data' is more and more often mentioned in conjunction with surveillance. Development has already reached a point, where there are plans of insurance companies to introduce concepts, when good drivers shall pay less premiums than bad ones.[2] Smartphones are already equipped with always-on voice recognition, so the phone can be controlled by the user's voice commands from the start, which also creates vulnerabilities regarding privacy (e.g. misuse by criminals).[3] The next step is using Big Data in health insurance companies to track precise details of a customer's life habits. 'Big Brother' is not far away, he's already there. Consuming data is now creating data, and Big Data provides the opportunity to be able to connect the right dots and create profiles, which represent the customer in the most fearsome detail imaginable. Today, the search engines we are using, know more than our closest family members, and profiles are created and adjusted accordingly.

6.3 Safety of Cloud services

In recent years an increasing number of institutions and companies have utilized the practice to put their data into the cloud. Cloud computing became popular with the development of such services by large IT-companies like Microsoft (SkyDrive), Google (GoogleDrive) or Dropbox. Clouds offer the user the possibility to store and access a limited amount of data on an external server. Via internet, this data can viewed, changed, deleted and shared between users so that institutions profit from such technological offers, especially if business discounts are offered. Whereas each user has his own private access with his account to the cloud, it is only natural to assume that the account and the data in the cloud is only his (privacy). A report published on

[2] [118]
[3] [162]

November 27, 2012 named: “Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act”[4] indicates otherwise, namely that the US Patriot Act from 2001 allows governmental authorities to access data in the cloud from outside the US; This is mostly due to the reason, that market leaders, who offer cloud services, are either US companies or at least have business in the US and as such fall under its jurisdiction. According to Axel Arnbak, one of the authors of the report, it is the FISA Act in particular, enabled in 2008, which helps US authorities to bypass regional authorities and to order access to cloud data that belongs to non-US citizens, who live beyond the borders of the US. As such it fits that Microsoft argued in 2011, that there can not be a guarantee that EU-stored data “will not leave the European Economic Area”[5]:

> *Microsoft cannot provide those guarantees. Neither can any other company.*[5]

This lowered the credibility of US cloud service providers immensely. If a user is interested in storing his data in the cloud, he or she should seek out alternatives, which could be either regional (non-US) cloud providers or own ’self-made’ cloud solutions, based on cloud software such as ’own cloud’[6].

6.4 The presence of Cyber War

> *It’s fair to say we’re already living in an age of state-led cyber war, even if most of us aren’t aware of it. (Google’s CEO Eric Schmidt in his book ’The New Digital Age’:)*[7]

Reasons and possibilities of cyber war are easily described. The internet is an open network, in which numerous computer networks are connected to each other. Theoretically, it is possible to communicate from any computer of a network to another, as long as they are connected to the internet. The cyberspace includes the internet plus many other computer networks, which actually should no be accessible through the internet [8]. Some of those private networks do look like the internet, but are in theory separated from it. There is a number of other networks such as transaction networks (e.g. forwarding of cash flows, credit cards and stock exchange transactions) and control systems, which enable machine-to-machine communications. Well trained cyber units are able to access important networks - even if they have any kind of security system - and control them, including stealing of information, issuing new instructions or affecting the whole system to a degree where machines begin to lose their functionality (i.e. crashing by overload). Having a foreign network and system under control goes as far as being able to move money, force oil and gas leakage, set generators on fire, delete data, crash computers, derail trains, crash air crafts, affect stock markets or even change courses of armed rockets.[9]

[4] [202]
[5] [209]
[6] http://owncloud.org/
[7] [68]
[8] [48, p.103]
[9] [48, p.104]

Given those options, it is safe to say that well trained cyber units gain huge advantages over other countries in today's information society, where almost everyone and everything is somehow connected to a network, with increasing tendency in the near future. Those are in no way hypothetical scenarios, because they did really occur in the past, whether erroneously or on purpose. Indicators on cyber war activities have been the Stuxnet and Flame worm(s) in particular, explained in this thesis. This is why cyber warfare is an urgent and present topic. At the end of the day there is no fleet of war ships, army or intercontinental rocket, which can defend us from a distance, which affect the world we live in, beyond geographical borders as well as those of cyber space.[9] A reason why such complex networked systems allow being accessed externally is the fact that today's systems (including hardware and software) and their potential security mechanisms are built by humans. Humans do make mistakes, which give room for exploitations and misuse by others. Recent discoveries have also shown, that backdoors are built into hardware and software on purpose, in order to gain intelligence gathering capabilities. At the wrong time, for example when political tensions are present between two countries, the knowledge of such capabilities of one country to another can result in a conflict, which will be fought not only on the open battlefield, but also in the cyber space. The technological capabilities of state-affiliated agencies have already indicated, what is possible and what can be achieved through cyberspace, or the internet so to say. Often it is the case that networked systems, which should not be accessed from the public internet, in reality are open, sometimes even without the operator's notice.

In summary, cyberspace can be described having three following characteristics to make cyber war a real threat[10]:

1. Design flaw in the internet itself.
2. Hardware and software flaws.
3. Advancing integration of indispensable systems into the internet.

In the end the dependence of networked systems is not measured by the percentage of households with broadband connections or the number of smartphones per inhabitant. It is rather measured by the degree of how far critical infrastructure such as electricity grids, rail networks, pipelines and supply chains are dependant on networked systems without own backup systems.[11] As such, the US are way more vulnerable to attacks due to lack of proper cyber defensive measures and a higher dependence on networked systems than, for example, China or Russia.

Naturally, a public discussion of the relevant topics cyber war and cyber spying would be highly necessary, but it is also a highly critical sphere due to its utmost secretive nature.

The dilemma is obvious. While the arms race is ongoing, the attacker just needs to find one weak spot to make a successful attack, whereas the defending nation needs to be ready for everything.

Cyber attacks - in today's information society - can have devastating outcomes, that can lead to actions and violence beyond the cyberspace.

[10] [48, p.108]
[11] [48, p.196]

CHAPTER 7

Strategies of the European Union

7.1 Cyber Security Strategy

The European Union, having its political centre in Brussels, followed the ongoing technological progress and developed plans and strategies addressing industrial espionage exploiting the internet. Responsible for the discussion of the topic on cyber defence is the European Defence Agency (EDA). The EDA describes cyberspace as "the fifth dimension of warfare equally critical to military operations as land, sea, air and space"[1].

Such formulation indicates how seriously the EDA takes this topic. Armed human forces nowadays "both as a user and as a domain" rely immensely on the access to the internet to a degree, where the use of the cyberspace decides whether security and defence missions end up successful or not[1]. That in mind, the Cyber Security Strategy for the European Union was released in February 2013 with following emphasis:

> *Cyber security efforts in the EU also involve the cyber defence dimension.*[1]

Further, the cyber defence is described as "one of the ten priorities in the EDA capability development plan," which indicates the extent of involvement on this regard. Several actions are planned to be taken in order to create the cyber defence strategy[1]:

- First and foremost a group consisting of the project team of EDA and representatives of its participating Member States' are supposed to develop cyber defence capabilities within the EU (CSDP).
- A network consisting of EDA and Member-State research & technology (R&T) are supposed to support this work by delivering the required technologies at the right time.
- All of this is positioned next to existing and planned efforts by civil communities such as national and EU institutions, as well as the NATO.

[1] [65]

Due to multifaceted threats, an extensive approach has to be taken, with enhancing synergies between the civilian and military domains in protecting critical cyber assets. From a one-year study, which aimed at gaining a better understanding of cyber defence capabilities of each country from 20 participating member states of the EU, several recommendations have been derived, both for the EU and the member states.

In summary, the recommendations for the EU include overall improvement of response and intelligence capabilities, a closer cooperation with EC3 and European Network and Information Security Agency (ENISA)[2,3], and a creation of EU-wide data exchange network and of a culture of cyber security ("good practice, training and awareness-raising")[4]. Whereas recommendations for the member states involve the encouragement to develop own cyber defence doctrines (in coordination with other member states), increasing awareness and attention to cyber defence training and education in that field, and the exchange of equipment solutions and information, and overall closer collaborations between the member states. This follows directly from the fundamental idea of the European Union.

As explained in the document, the EU clearly endeavours creating various strategies to improve cyber defence on the whole EU level. Through the close cooperation of each member state one hopes for high quality defence systems, enhanced by each others know-how.

For the near future the EDA expects many actions to be derived from the study recommendations, especially in areas where the member states benefit from closer cooperation, while action already has been taken in the area of training and exercises towards building a European Cyber Defence Culture, as mentioned above.

The Agency is active in the fields of cyber defence capabilities and in the research & technology (R&T) domain. With that in mind the EDA works on several Cyber Defence Projects including[4]:

- Training (Cyber Defence Training Need Analysis in order to build a Cyber Defence Training Curriculum).
- Situational Awareness (Kits) (How to integrate cyber defence in the military operational planning process and thus provide a common and standardised cyber defence planning and management platform).
- Cyber Defence Research Agenda (CDRA) (to precisely target R&T efforts on specific military aspects. CDRA will consider these aspects and propose an R&T roadmap for the coming 10 years).
- APT Detection (Governments and their institutions are among the most prominent targets for APT malware, mostly aiming at cyber espionage. Intrusions are either discovered too late or not at all. Early detection is crucial to properly manage the risk imposed by APT. EDA is preparing a call for proposals for first analysis and ideas of possible solutions).

[2] "ENISA's role is to support the internal EU market by facilitating and promoting increased cooperation and information exchange on issues of network and information security, to enhance the capability of the community, the member states, and, consequently, the business community to prevent, address, and respond to network and information security problems"

[3] [106, p.437]

[4] [65]

- Technical Forum for Cyber Defence Technologies (The R&T forum 'IAP4' (related to communication and information technology - ICT) gives the member states a platform to discuss and prepare collaborative R&T projects on cyber defence).

Information Security support by the ENISA

ENISA is an institution, responsible for Information Security in Europe, based in Heraklion and Athens, Greece. It serves as a centre of expertise and is the EU's response to all issues of the European Union concerning cyber security.[5]

One of ENISA's tasks is to put policy and operational requirements closer together, creating a bridge and providing an objective European platform for information sharing amongst Member States of the European Union.

Its contributions to enhance cyber security involve the identification and analysis of new threats and trends, creating awareness in regard to security risks, improving warning and response times, the protection of critical infrastructures, policy implementation, promoting international cooperation, information exchange and many more.[6]

In terms of cyber attack activities, according to data from 2012 the majority of attacks fall into the category of cyber crime and hacktivism (cf. figure 7.1).

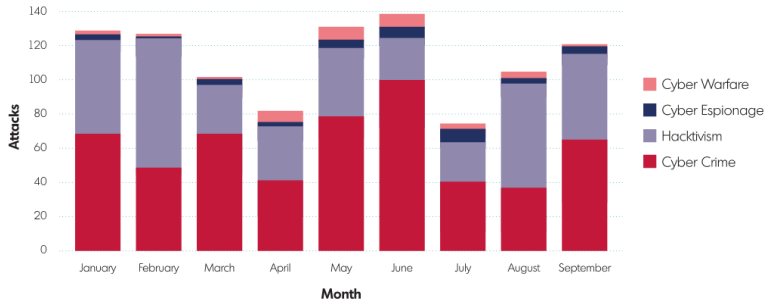


Figure 7.1: Attack distribution data for 2012 (reprinted from [63, p.11]).

While cyber espionage takes a minor part (also due to it being unnoticed or unreported) of the overall number of attacks, it is nevertheless seen as a major threat to industrial bodies, economy and individuals. In the ENISA Threat Landscape, Mid-year 2013 Report ENISA describes cyber espionage attacks as having "reached a dimension that went far beyond expectations"[7]. In particular the growing number of powerful mobile devices is mentioned, which would bring "a wide exploitation surface for this kind of threats," and that mobile spyware applications would presumably become stronger and become new tools for APT's.[7]

[5] http://www.enisa.europa.eu/about-enisa
[6] [63, p.9]
[7] [69, p.4]

European Cybercrime Center

The European Cybercrime Center (short: EC3) was established as a centre in Europol's headquarters in The Hague, Belgium and opened on January 1st, 2013. It focuses on several fields including[8]:

- The development of a "fusion center", where information on cyber-crime in the EU can be collected and Member State-specific investigations coordinated.
- The support of Member States in operational cases.
- Establishing special Cyber Departments for supportive analysis of threats.
- Initiating the "Research and Development" of investigative and forensic tools.
- In general, observe attacks on "EU-critical infrastructure".

Besides, the EC3 wants to coordinate their work closely with Interpol and various representatives from ENISA, EU Commission, EU Cybercrime Task Force and others. The aim is to connect with all stakeholders and to "focus on the criminal - not the crime"[9].

7.2 Reporting requirements in cases of espionage

Neelie Kroes, Vice president of the EU-Commission, in January 2013 announced plans (which should be developed in the following months) to combat rise in cyber-crime. These plans require "companies that store data on the Internet — like Microsoft, Apple, Google and I.B.M. — to report the loss or theft of personal information in the 27-nation bloc or risk sanctions and fines"[10]. Especially companies that run large databases and have high 'data values' due to running e-commerce, cloud services or social networks, should be affected. In addition, "the proposal directs EU countries to impose penalties on organizations that do not heed the notification rules", which would require specific 'disclosure laws' to be crafted on the national level.[10] At the time of the announcement details on how the plan is supposed to be carried out were not stated. However, mentioned were the affected industries, including banks, stock markets, energy-, health- and transport-industries. According to estimations of the Commission, the conditions would apply to around 44,000 companies. It is also proposed that authorities like the German Nationale Cyber-Abwehrzentrum (NCAZ) should be built all around Europe, and defensive strategies developed in coordination.[11]

The technology industry demands more specific guidelines "to ensure that notifications are required only when necessary and useful to consumers"[12]. After presenting the European Cloud Computing Strategy[13] in 2012 the European Cloud Partnership was created with the aim to bring

[8] [204, p.60-61]
[9] [204, p.61]
[10] [153]
[11] [180]
[12] [153]
[13] https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

industry and politics closer together. In this regard, Neelie Kroes has the intention to improve all aspects of data security in order to protect customer data more effectively. According to the German Federal Office for Information Security Technology (Bundesamt für Sicherheit in der Informationstechnik (BSI)) and Bitkom, more than 370,000 users have been victims of hackers between May and June of 2012. Moreover, 100,000 access data and 49,000 e-mail accounts have been hacked[14]. According to Reinhard Clemens, the CEO of T-Systems, several years ago the number of daily hacking attacks was around 10,000. Now it is ten times this number. The most frequently used cyber attacks are the 'Drive-by' Exploits, utilizing browser vulnerabilities to infect computers. Botnets and Phishing attacks are also mentioned as being popular.

Companies often make very late reports about them having become victims of cyber attacks (e.g. Sony, when user data was stolen in 2011[15]), mainly because they fear image loss. Listed companies also shy away from reporting requirements, because they fear the uncertainty of investors. In addition, there is mistrust towards competitors getting knowledge of own vulnerabilities as soon as the EU is notified. According to Kroes and German Interior Minister Friedrich, the self regulation of the economy is not longer sufficient.[16] Concerning the plans of the obligation to report, again one of the questions remains how the potential increase of protection should be financed. As such it is still a long way until the plans can become reality, more specifically whether the draft can and will be transferred to EU-law.

Data Breach Notifications

Since 2009, the German Federal Data Protection Act (Bundesdatenschutzgesetz) includes obligations to provide information in case of data breaches (so called "Data Breach Notifications")[17]. Similar regulations also exist in Austria (§ 24 Abs 2a DSG 2000[18]), whereas in Britain and Italy reporting is voluntary. The same goes for the US, where Web businesses "are not required to give notification of data breaches, and rules are enforced by state, not national, governments"[19]. It should be noted that § 42a BDSG (Bundesdatenschutzgesetz) mentioned above does not explicitly describe data breaches by cyber attacks using the internet, but represents a more or less general notification requirement. In regard to the aspects of data breaches in IT-security, the German inner ministry sent a draft bill[20] for a law "to improve the security of information-technological systems" in March 2013. According to the draft, operators of critical infrastructures in the fields of energy, water, information- and communication technology must meet minimum standards in IT-security and report significant security breaches. ISPs are also included in the list of the companies demanded to cooperate. Reported information is sent to the BSI, where it is analysed and evaluated in order to be able to advise and support the affected companies. Numbers about the costs that are required for the realisation of the project are not named.[21].

[14] [75]
[15] [178]
[16] [180]
[17] [52]
[18] http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597
[19] [153, p.2]
[20] German: Referentenentwurf
[21] [117]

Plans of the German BND

The BND also prepares to fight against cyber (espionage) attacks. As of March 2013, it wants to establish a department dealing with hacker attacks on "national institutions and the German industry", requiring about 130 employees with expertise in anti-virus programs. According to BND-chief Gerhard Schindler, Germany has to react to countries like China, who are attested to employ up to 6,000 people, and Russia, who are presumed to follow a similar aggressive cyber strategy, but where governmental hackers would operate disguised behind private firms.[22] It is very unlikely that individual hackers become employees of the BND, due to the high risks involved. Hacking is still part of grey zone. As soon as a hacker is working for the governmental authority BND, the grey zone disappears. Furthermore, hackers who start working for the BND will have a hard time to communicate (reputation related) with other self-employed hackers. In the end, due to lack of experts, the BND will be forced to buy software and know-how from external sources again, just like history with FinFisher has shown, diminishing the idea of using 'unique cyber tools'. While the BND is responsible for the offensive infrastructure, the BSI competence is building up the defence.

NCAZ

The NCAZ belongs to the BSI, an exclusion of the BND, and its purpose does not appear to be clearly defined. It is questionable whether the authority deals with foreign espionage attacks or represents a surveillance centre. Officially, the NCAZ employs 10 people, who are supposed to gather, analyse and evaluate information. A scenario is described as follows: The BSI gets knowledge of a new vulnerability and as a result informs the NCAZ. Simultaneously, the BfV finds out that a trojan has been trying to infiltrate critical infrastructure. The BSI starts to examine the trojan and finds its exploited security hole. Upon analysing, the NCAZ comes to the conclusion that the critical infrastructure is in fact in danger. Companies potentially affected by the malware are informed and are addressed to give feedback.[23] Of course, it is doubtful that such a scenario would follow the same steps, especially considering that 10 employees are supposed to handle and coordinate the whole information process. One should realize that both software companies including developers of AV and firewall software, and the ministry of the interior (in charge of national authorities) are eager to sell their products.

7.3 EU's penalties on cyber criminality

The EU parliament adopted EU-wide penalties on 'cyber criminals' in early July 2013. When information systems of a member state are under fire by cyber attacks, the maximum penalty for convicted offenders now stands at two years. The illegal interception of communications is sanctioned this way, too. However, so called 'mild cases' are not covered by the rules. The member countries themselves need to decide whether a case was 'mild'. This results in some confusion and clearly opens some unnecessary backdoors. According to a press release[24], in

[22] [78]
[23] [167]
[24] [171]

case of attacks on 'critical infrastructures' the offenders should have to reckon with at least five years of imprisonment. For the use of Botnets, at least three years in prison are due. The member states have two years to transpose the EU directive into national law. While recent events concerning the NSA and especially the GCHQ have shown involvements on European territory, it is still highly doubtful that both parties will be sanctioned one way or the other.

7.4 Analysis

There are several outcomes, when the draft about reporting requirements is adopted as law. Authorities as BSI and BKA receive more financial resources in order to improve the infrastructure and function as a communication centre (consulting & support of companies), which appears to be a good thing, because know-how has in an innovative country like Germany an important and immense value. After all, reliable data is needed in order to be able to discuss and deal with the problem of cyber espionage. If hacked companies conceal the incident, there is no real urge to invest in security and customers will not know, at which companies their investments or data is safe. One has to realise, that the reporting requirements are directed at the responsible authority (here: BSI) and not to the public. A company's quality of security compared to competitors will become obvious, but the truth will still be kept hidden from the public. This is an important factor in doubting the correctness of the whole draft. Another important factor is the role of the BSI in consulting companies. It would be preferable, if the BSI would rather create a sort of catalogue, containing attack classifications, so only real threats to critical infrastructure are handled and not any attempt of a hobby hacker (clear identification of an attack: e.g. dangerous attack, or civil disorder / demonstrative act). After all, the BSI is financed out of tax money, and a clear definition and classification of a cyber attack is missing in the draft. In times of publicly controversial topics like data retention, it is important to define clear rules and guidelines in order to be able to act quickly and most important, effectively in terms of hunting down real criminals and threats (such as targeting critical infrastructure). Real stimuli to improve one's IT infrastructure would include the public naming of companies who have become victims of cyber attacks. Then it's very likely that companies would act preventively instead of reactively in terms of information security. Further, explicitly all customers need to be informed as soon as a company has been hacked and private customer data loss has been experienced. Also, the BSI needs to define clear categories, when attacks are representing the term 'dangerous'. The BSI needs also to say which company was lacking in security and even go as far as saying the company was not ready to handle the sensitive data (and / or machines). That way you would force companies (major enterprises in particular) on the one hand take preventive measures and on the other hand to tell the truth. Maybe even sample taking by the BSI from different companies would be an option to consider.

Otherwise, at this point the danger remains that due to the lack of clear definitions and classifications the size of 'Big Data'-related databases continues to grow, companies still don't have the necessity to act preventively and cover up their mistakes. The public must get knowledge of companies' data breaches, because they are directly or indirectly affected by it.

In terms of EU plans to penalize cyber criminality, it is clear that such penalties need to exist, even for a longer duration than 'at least 2 years', because evidence has shown how much damage

cyber attacks can inflict on companies, governments and single individuals. The problem is, that, if the offenders are based in countries like Iran, Pakistan, China or even the US, European law may apply, but could be enforced easily. What will happen, and partly already happened, is finding out that the reports of Edward Snowden are in fact real, but legal ramifications will however be hardly seen. Political consequences at best. For as much complaining that comes from politicians in regard to eavesdropping in Germany and other countries, as much valuable information the BND, BfV and other foreign agencies get from the disclosed documents.

What is rather needed is an international agreement with the G-20 and proper adjustments of legislation to the present. Monitoring to such an extent cannot go out of hand further, and has to be limited and dealt with on a contractual basis. However, it is also doubtful that such an agreement will come in the near future - too different are the individual interests.

Both EDA and ENISA offer plans and support in regard to the topic of cyber espionage. It shows also, that the EU has many ideas to overall improve the cyber defence culture of companies and individuals in the European Member States. However, decision makers in the EU need to start to adopt legislative measures regarding crime in a way to achieve a proper balance, that is required in today's digital age: in order to achieve (global) security regarding the individual's privacy, as well as a company's know-how. Simultaneously, it is also necessary to guarantee that privacy including personal communications, data protection and information access and dissemination are fundamental rights in modern democracies.

CHAPTER 8

Scope of security measures

8.1 Defensive strategies

One of the reasons why companies neglect sufficient protective measures is in cases of fighting for sales. Each company should seek out experts who can give valuable consultation on how the company can protect themselves. Four fields are of biggest concern when it comes to the risks of espionage: The *internet*, the *human*, *business trips* and the *office*.[1] Especially the most valuable data containing innovative know-how should under no circumstances be saved on systems which are connected to networks and the internet.

Stuxnet, Prim and Tempora, they all have been not a real surprise to IT-related people, rather the extent especially of Prism and the level of sophistication of Stuxnet was not expected. But all these 'espionage programs' have changed and raised the awareness of the public. Security measures are not only necessary in small, middle or large-sized companies, but also in the industry to protect machines and control systems. In Germany for instance the cyber-protection centre (German: NCAZ) was established in February of 2011 as a cooperation- and communication centre of security services. Information is drawn from attacks in order to create effective protective measures for Germany's IT infrastructure. The BfV is responsible for the monitoring of activities directed against the democratic order of the Federal Republic of Germany; a protective authority against foreign espionage attacks; meaning that they represent the preventive part, having the resources to analyse the attacker's methods and from that derive valuable protection strategies.

Small-sized companies usually just don't have the resources to deal with the risks of (cyber) espionage, while a lot of large enterprises possess a sort of 'corporate security' department. Moreover, the BfV assures confidentiality in cases when companies decide to inform the authority about becoming victim of an attack. According to a representative of the state office, they "work after constitutional principles", and as such they are not obliged to forward the case to the

[1] [29]

prosecution, instead they utilize their resources for information gain and the company has not to fear direct potential reputation loss.[2]

Topologies (e.g. that the whole company network structure is connected) have to be divided and the rights managements must be adapted in a way that only the right people get the information they are supposed to access. Security is more or less an illusion, because no technical equipment can fully guarantee that only people get access to the data, which they physically need. AV programs do not help during targeted attacks. They detect only already known and identified malware. The management has to make the right decisions in favour of better protection even if it's costly. This includes state-of-the-art IT-software and hardware protection, but also and most importantly guidelines and policies for employees to follow.

8.2 Encryption of data

> *Encrypting a message involves scrambling it through a combination of a randomly-generated key and mathematical jumbling. The NSA and its UK counterpart GCHQ regard this as the biggest threat to their ability to view the vast quantities of communications data they collect.*[3]

Encrypting e-mails and devices such as hard drives should long have become standard in today's enterprise culture, in order to protect data. The encryption of data describes any effort "to conceal, scramble, encode, or encipher any information". Data (information) is transformed to an unintelligible form in a way "that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption)"[4]. The cryptographic transformation of data starts at the 'plaintext', and creates the 'ciphertext', which "conceals the data's original meaning to prevent it from being known or used"[4]. In today's technological society, data is digital, meaning all information is stored in a form of binary digits (1 and 0). Storage, exchange, and processing of digital data is done in "increasingly large quantities at virtually every level of government and in the private sector," especially in industrial and technologically advanced countries[5]. As such, the demand for encryption of data is almost unlimited, meaning that "anyone who transfers or stores important digital data has an interest in its security"[5]. Governments had always the biggest interest in data encryption, whether as users or attackers.

Method and purpose of Encryption

With the invention of electrical and electronic communications, the internet in particular, the banking sector was the one, which "first regularly used encryption to protect communications in the new area of electronic money transfers." Especially the all growing "internationalisation of the economy" has led to communications being protected, at least partly by cryptography.

[2] [215]
[3] [26]
[4] [106, p.290]
[5] [125, p.395-396]

Finally, the expansion of the internet and with underdeveloped countries gaining access to it, the number of (completely) unprotected communications increased and to this day keeps increasing. With it, the need for "private individuals to protect their messages from interception" increased accordingly.[6]

Security of encryption systems or when you can speak about a system being secure

In general, a 'secure' encryption system can mean two things[7] :

- It may be "essential and susceptible of mathematical proof, that the message is impossible to decipher" without the right key.
- Or it may be, provided the current state of technology, secure in terms of the code being regarded as unbreakable for a period of time, "which the message needs to be kept secret".

With the help of computers, encryption algorithms became so powerful, that for crackers (or 'codebreakers') it just doesn't seem feasible to decrypt a message in a realistic amount of time. Thus, nowadays, decryption usually involves the codebreakers to try out all possible keys.[8] This method is also known as '*brute-force attack*': "Brute force attacks rely on sheer computing power to incrementally try all of the [key] combinations"[9]. Of course this implies for, the longer the actual key, the higher the chance of the attempt failing. Another method used by intruders is that of using '*dictionary attacks*'. This form of attack makes use of a dictionary, that includes the most common words like places, objects, and names and tries them for guessing the password.[9] Both approaches show, why it is very important for internet users, whatever they do with data, to make sure that a proper key is chosen and an attack on this data can be thwarted. Therefore, present state of technology still allows for a sufficient 'secure' system/account etc., even if one can never say about encrypted data being 100% secure. Choosing the right and secure password is still a problem among the majority of users. After all, the most commonly passwords (from a sample of 2m) include passwords like '123456', 'password', 'admin', or '111111'.[10]

Overview of a selection of encryption tools

There is a wide range of services and tools that can help to provide at least to some extent protection against governmental spying. While end-to-end encryption still is rather complex to use on a daily basis, there is still a variety of technical possibilities to explore. Following list shows examples of software that can be used by the everyday internet user:

- Operating systems offer full encryption (e.g. BitLocker[11] for Windows, LUKS[12] and FileVault 2[13] for MacOS).

[6] [185, p.121]
[7] [185, p.122]
[8] [185, p.124]
[9] [49, p.98]
[10] [44]
[11] http://windows.microsoft.com/de-de/windows7/products/features/bitlocker
[12] http://wiki.ubuntuusers.de/LUKS
[13] http://support.apple.com/kb/HT4790?viewlocale=de_DE&locale=de_DE

- VPN services like TOR[14] offer a way to stay anonymous while surfing the web.
- E-Mail encryption is available through Enigmail[15] (Thunderbird) and Mailvelope[16] (Gmail).
- Chat communication in clients like Miranda and Pidgin is easily configurable with the OTR encryption[17] (Off the Record), which supports many chat clients.
- Encryption of whole disk drives or single files is possible with the popular Open Source tool TrueCrypt[18]. There are also PGP[19] and encfs[20] which are also viable options.

While all these tools offer great options to improve privacy protection on the internet, there is still more to it, like avoiding services from Microsoft, Google and Co. It is also doubtful, whether the use of those tools is really feasible in the public. Rather, those tools can be viable options for the use in companies, who - provided the user other well protected mechanisms (firewalls etc.) - can profit from these by increasing the level of protection. It can unquestionably be a step in the right direction.

In terms of Google's search engine www.google.com, which is known for tracking and saving the user's searching habits (e.g. history, connectivity with other Google services & profiles etc.)[21], there are other alternatives, which provide full anonymity, while searching the web. Such an alternative is https://duckduckgo.com/, which claims to not to track the user, and filter his results, promoting things Google *thinks* you like.

After the events disclosing Prism and other surveillance programs several websites were launched in order to inform users of alternatives to protect privacy. One of which is the website http://prism-break.org/, which offers a great selection of services and tools, sorted by categories.

In the end, nevertheless, the more viable and primary solution is to achieve change in the public's mind and politics.

Overall, anyone who is concerned about data requests from US intelligence services on e-mail providers should consider switching at least to a European provider. For example, there is the German provider Posteo[22], who can be paid with cash anonymously, and e-mail accounts can be kept without giving away personal information. Another one is the Norwegian based provider Runbox[23], who stresses not to save save log files. But in general, considering that the GCHQ in Europe could intercept communication, those who want to keep e-mail communication private, they should encrypt it on their own computer, i.e. by first writing the text in an editor, encrypting the text and then copying it to the e-mail program. A good way to do it is using

[14] https://www.torproject.org/
[15] https://addons.mozilla.org/de/thunderbird/addon/enigmail/
[16] http://www.mailvelope.com/
[17] https://otr.cypherpunks.ca/
[18] http://www.truecrypt.org/
[19] http://www.gnupg.org/index.de.html
[20] http://www.arg0.net/encfs
[21] [60]
[22] https://posteo.de
[23] https://runbox.com/

PGP-standard[24](Pretty Good Privacy) or S/MIME[25], which both, however, require both sides (communication partners) to use it.

The interest regarding e-mail encryption is there. This is shown by statistics from SKS-keyserver[26]. According to their data, the number of new uploaded PGP keys on the keyservers increased twofold, shortly after Edward Snowden's document leaks. As of October 2013 more than 3.400.00 public OpenPGP keys have been generated.

In general, there is no guaranteed protection against surveillance on the internet. The internet runs through backbones, which can be accessed by authorities, therefore, naively expressed the participation on the network internet results in sacrifice, to a degree, of your own privacy. In the end it is still up to the user, how much information about himself is shared. A privacy-friendly mainstream offer is missing and the demand is also lacking. Constitutional rights are not questionable in the fields of technology or the marketplace. The US surveillance programs run against democratic principles, automatically affect people all around the globe, just because US-based companies are economically at the highest level and have the respective amounts of customers.

There are hundreds of ISPs in the US, but there is only a handful of central internet network points called backbones, including AT&T, Verizon, Level 3, Qwest and Sprint. They all represent the 'Tier 1 Carriers', which means that they form a direct connection to most of the other ISPs in the country. These companies own the largest data lines reaching thousands of kilometres in the whole country. In fact over 90% of the whole internet traffic of the US runs through these Tier 1 Carriers. As such, it is highly unlikely to establish communication without crossing one of the backbones. In case of cyber security we can conclude that you can reach a high safety coverage of the majority of the internet infrastructure in the US and the cyberspace as long as the Tier 1 Carriers are protected.[27]

8.3 Intrusion Detection System

Intrusion Detection Systems are a viable and necessary extension of the IT-security infrastructure, increasing the internal surveillance of companies. They can help to recognize vulnerabilities on the network-, as well as the system-level (OS, apps) preventively and in real-time. In general, the architecture of such a system comprises three main components, which together are usually referred to as 'sensor'.

1. Data-collecting component (logs, network data), which shows information on state/health and resource allocations of the computer system.

2. Data-analysing component, which analyses all collected data on eventual changes / access (attacks), for instance by comparing to a rule-set (e.g. signatures).

[24] http://www.openpgp.org
[25] http://datatracker.ietf.org/wg/smime/charter/
[26] https://sks-keyservers.net/status/generate_key_chart.php
[27] [48, p.207]

3. Reporting component, which shows the analysis result, generates an alarm and offers options of further action, e.g. to initiate a 'Intrusion Response' (for instance sending an e-mail to all administrators).

Next, a Intrusion Detection System has several tools, allowing for the control of the sensors. This is usually the task of the 'management station', which is either a graphical user interface or a 'command line interface'.[28]

For the Intrusion Detection System to work effectively and to monitor the complete data traffic, it should be integrated into the network-segment. This is done by the Network-based Intrusion Detection Systems (NIDS). Over a 'sniffer-interface' all data, that is going through the network-cable can as such be read and transferred to the analysis module. There are also other types of Intrusion Detection Systems, that vary in features, like the Network Nodebased Intrusion Detection Systems (NNIDS), Inline Intrusion Detection Systems, and Application Intrusion Detection Systems.

However, Intrusion Detection Systems make use of the function of parsing (syntactic analysis). All signature-dependant systems such as Virus-scanners, or Intrusion Detection Systems which have an embedded heuristic, use parsing, because of performance issues. Sophisticated cyber attacks, nowadays are able to mask themselves with valid signatures and as such a technology like the Intrusion Detection System is faulty in cases of this sort of attacks.[29]

Therefore, Intrusion Detection Systems do have the potential to improve protection of specific areas of IT-infrastructure, provided the network manager has full knowledge about its functionality and restrictions, but nevertheless should not be regarded as an all-in-one solution.

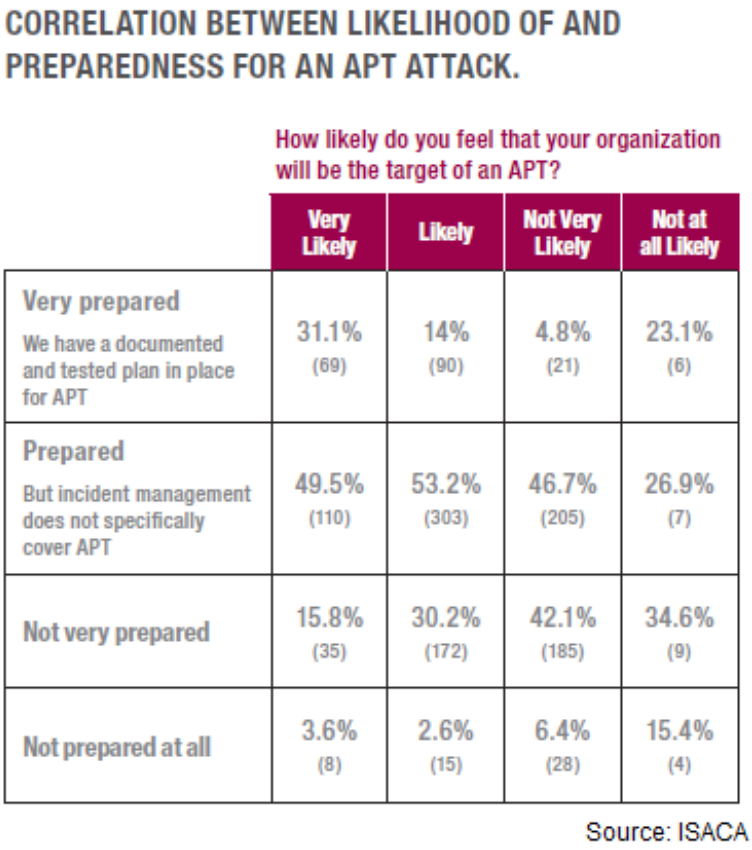
8.4 Are companies prepared for APT cyber attacks?

One important aspect of this thesis is to analyse whether companies have sufficient awareness regarding the threats to information security, and whether proper information security systems exist and are updated and tested on a regular basis. Naturally, one would presume that especially large companies have the resources and the aim to invest them in order to protect the company's valuable know-how from external intruders. In reality, the measures that are taken in regard to IT-security are lacking behind the 'state-of-the-art' of APTs.

This assessment of the situation is reflected in a survey by ISACA (Information Systems Audit and Control Association) of over 1,500 security professionals, who were asked the question: How likely do you feel that your organization will be the target of an APT? The results can be seen in figure 8.1.

While about 67% of respondents expressed they were familiar with APTs, roughly 50% said that APTs are recognized as being similar to traditional threats. As we have seen, APTs are in fact very unique and sophisticated versions of targeted cyber attacks, which include a variety of stealthy malicious techniques by hackers who seek to get as much information from the attack as possible. And this is achieved through the use of remote-accessing tools, which most of the time remain active and unnoticed for months and even years. Accordingly, most companies

[28] [95]
[29] [197, p.41-42]



CORRELATION BETWEEN LIKELIHOOD OF AND PREPAREDNESS FOR AN APT ATTACK.

	How likely do you feel that your organization will be the target of an APT?			
	Very Likely	Likely	Not Very Likely	Not at all Likely
Very prepared We have a documented and tested plan in place for APT	31.1% (69)	14% (90)	4.8% (21)	23.1% (6)
Prepared But incident management does not specifically cover APT	49.5% (110)	53.2% (303)	46.7% (205)	26.9% (7)
Not very prepared	15.8% (35)	30.2% (172)	42.1% (185)	34.6% (9)
Not prepared at all	3.6% (8)	2.6% (15)	6.4% (28)	15.4% (4)

Source: ISACA

Figure 8.1: Companies' assumptions of the own protective measures against APTs (reprinted from [182]).

still assume that the use of AV, anti-malware (both 95%) and firewall (93%) products would be sufficient enough to deflect APT attacks.

Still, after a great number of large companies such as Google, Walt Disney, Morgan Stanley, and energy and oil companies became evidently victims of APTs in the last years, "companies seemingly don't know how to change their security practices to fight them"[30].

Nevertheless, whole 60% of survey participants feel they are ready to fend off APTs. That is in fact more wishful thinking, because true nature of APT attacks is very often to exploit zero-day threats, which are at the time of the attack unknown vulnerabilities and thus APTs are able to enter the systems with the use of for example spear phishing.

According to ISACA director Jo Stewart-Rattray "APTs call for many defensive approaches, from awareness training and amending third-party agreements to ensure vendors are well-protected, to implementing technical controls" and that is true for all of them[30].

Interestingly, a high percentage of respondents answered to the question: "What do you believe to be the highest risk to your enterprise associated with a successful APT attack?" that

[30] [182]

Figure 8.2: Assumptions of the highest risks from APTs (reprinted from [182]).

realistically the loss of intellectual property is the highest threat, followed by loss of personal information and reputation damage (cf. figure 8.2).

67.3% of participants even said, that "they had not increased awareness training specifically relative to APTs", which shows the lack of risk awareness.

The study shows also the problem and difficulty, that many Chief Executive Officers CEOs see when it comes to investing in security and showing support to security professionals directly from the management level, due to the fact that security just doesn't "have an easily measurable Return on Investment (ROI)"[30]. Therefore, it comes to little surprise that within organisations, where the upper management has become more involved in security matters, a notable increase in policy enforcement (66%) and security budget (46.9%) could be seen.[30].

8.5 The Critical Security Controls for Effective Cyber Defence

The website of the SANS Institute provides valuable information on computer security and gives "twenty critical security controls for effective cyber defense", which can be accessed through: http://www.sans.org/critical-security-controls/. The controls focus on prioritizing security functions, that are regarded as being effective against APTs, applicable on services, architectures, processes and products, that have "demonstrated real world effectiveness". The SANS Institute claims, to reach a 94% reduction in security risk, by following the implementation of the 20 controls.

The controls include topics on how to differentiate with authorized and unauthorized devices/software, how secure configurations look like, details on malware defences, data recovery capability, data loss prevention and many more. Companies should consider following the guidelines, because it can help to reduce the risk of becoming victim of a cyber attack by Advanced Persistent Threats.

However, there is no "one-size-fits-all" solution. The actual implementation of all controls will vary, from the company's size, budget, need etc., and depending on the need to "address the most critical threats first", the order of implementation will differ.[31]

8.6 Where companies should put their focus on

Security is of course a diverse topic for companies and governments alike. Besides having great infrastructure, it is also important to focus on approaches that go beyond the process of prevention. One of the approaches is the 'kill-chain' approach, a methodology published by the US global security and aerospace company Lockheed Martin in 2010 (cf. [32]). The approach describes that "the adversary must progress successfully through each stage of the chain before it can achieve its desired objective; just one mitigation disrupts the chain and the adversary"[33]. An analysis of the chain, a shift of security from plain reaction to proactive anticipation is revealed giving the opportunity to estimate the effectiveness of the own defence. As the paper says, "vulnerability-focused processes are insufficient, understanding the threat itself, its intent, capability, doctrine, and patterns of operation is required to establish resilience". Therefore, the kill-chain "provides a structure to analyze intrusions, extract indicators and drive defensive courses of actions."[34].

Another approach can be the use of the 'Vocabulary for Event Recording and Incident Sharing'-framework(short: VERIS)[35] which allows to decompose units of an incident into a series of independent events and as such give the opportunity to analyse and select the most efficient and feasible option to apply additional security controls. This will improve detection

[31] [204, p.56]
[32] [103]
[33] [103, p.2]
[34] [103, p.12]
[35] http://www.veriscommunity.net/doku.php

and response time, which in today's information society are desperately needed.

Yet another approach for mitigating cyber attacks involves Microsoft's Enhanced Mitigation Experience Toolkit (short: EMET). This tool-kit "functions by blocking entire classes of exploits instead of only the specifics. In doing this, EMET helps shift security from being reactive to proactive and raises costs for attackers."[36]. EMET promises to reduce zero-day attacks, by protecting assets before a signature or patch (which mask malware) is released. The costs of EMET's deployment is in perspective to the kill-chain approach, especially for small-sized companies great, because it's free, probably requiring minor configuration management costs. It is also recommended by CSC.

All these approaches and tools have proved to be reliable in the fight against cyber attacks.

In general, companies should store data only if it is essentially necessary. Also, only highly protected computer systems and networks should be allowed to be connected to other internal/external networks or even the internet. Security measures, which are taken accordingly to the ISO/IEC 27000 standard[37], should be seen as just a minimum basis of protection. The most important programs software-wise should also be kept up-to-date at all times.

Is proper defence possible?

In regard to surveillance programs like Prism and Tempora you cannot guarantee that nobody can read your data as long as you are using the internet, which is provided by companies like Telekom. It lies in the nature of things, that although they won't read your data in practice, they however are obliged by law to keep open points for the police to keep the option available. That is not only true for the internet, but also for mobile communications. Nevertheless, nothing stops one from using data encryption tools. A basic example would also be using web mail-services which provide access through 'https'(Hypertext Transfer Protocol Secure), instead of 'http'(Hypertext Transfer Protocol). While it has nowadays become a standard, the security aspect has not got huge benefits from it, due to programs like Prism, which directly monitor data at the provider's servers.

The provider cannot reject court orders which force him to provide the data. Nowadays, you have to take care about the amount of information you make publicly available. This includes posting photos on Facebook, which in most cases are viewed by companies before a job interview. Social networks can also create opportunities for criminals to get on sensitive information, for instance, by masking one's identity as another and then contacting a target (i.e. manager in a firm). Encryption is only a tool that can provide protection measures. It doesn't help, if the person behind the system is willingly sharing information with entrusted people, who yet have other intentions.

Security measures require a number of different community responses, because there is no all-in-one solution to the protection from intelligence gathering and industrial espionage in particular. Improved collaboration between companies and national authorities is required, as well

[36] [204, p.59]

[37] part of ISO/IEC Information Security Management Systems (ISMS) standards, entitled: Information technology - Security techniques - Information security management systems - Overview and vocabulary. Available at http://standards.iso.org/ittf/licence.html

as legislation on international and national levels adapted to the newest technologies. These steps must be followed by the improved analysis and collection of cyber espionage activities to get a better understanding of present threats. Analysing weaknesses in corporations must focus on used hardware and software and apply regular updates and testing/evaluations and risk assessments. And finally, the intensifying of awareness training of each affected individual, and to a certain degree the public, of handling data and knowing the risks, is of importance.[38]

What should be done is also, to steer away from systems built in the US, which would be hard to accomplish at the beginning. But maybe it can be done in collaboration of countries. The principles of the EU should give opportunities to create alternatives. One alternative of many is without a doubt Open Source, because it is open, secure, often free, and without backdoors. As such, there are possibilities to go around the extensive surveillance, and in addition to that, one country has not to solve the problem by itself alone.

[38] [156, A1-A2]

CHAPTER 9

Conclusion

The internet has become a foundation for global surveillance. Accordingly, industrial espionage has also received a new layer - so to say - of tools of highly diverse types, including malware and backdoor exploitation. Not to say, that industrial espionage, known from the 'cold war' is not present any more. It is, but it has evolved tremendously with the potential to affect worldwide politics, economy and civilian population.

Undoubtedly, today we live in an information society, where a targeted cyber attack can involve tremendous consequences, which in the near future can even employ valid threat scenarios comparable to results from nature catastrophes. The threat to critical infrastructures and companies is apparent, but it can be avoided if right preventive measures are taken.

The rise of cloud computing means the loss of control of our own data (e-mail, photos, calendar, messenger, documents). Data - the new information - now is stored on servers belonging to Google, Microsoft and others. In addition, global data access is increasingly realised through devices that are tightly controlled by vendors (iPhone, Chromebook, Kindle). All this trends increase corporate power, by giving them more control over data, and therefore over the people. At the same time governmental surveillance has extended its reach coverage immensely.

The main clients of industrial espionage appear to be the US and China. China's role becomes visible, due to their rather careless information handling (e.g. some of the hacker (APT) group's employees use social media with their working accounts). The bigger picture regarding the US is on the other hand created through the help of people like Edward Snowden, who give detailed insights into the working mentality of intelligence services and into their wide reaching intelligence gathering apparatus. As such, it can be assumed that both, intelligence gathering and industrial espionage is conducted on a global scale; not only by the US and China, but also other countries, who undoubtedly are involved in similar activities.

Edward Snowden's revealing of cyber surveillance programmes had an impact on the whole virtual and physical world. Echelon, Stuxnet, Flame and other operations of recent years have only been a foreplay, and have only been in media, because they were discovered. Trust has been infringed, as well as the legitimacy of privacy, civil rights, and eventually even the global

economy. Thus, legal bases and sanction catalogues are necessary to limit the incidents. In addition, the variety of malware and the extent of the internet is evolving, and the law has not caught up to it, yet.

What became evident during the analysis, is the slight change in the target-selection of espionage attacks. While so far the finance sector was a valuable and popular target, because mostly money was involved, it shifted in recent years and months to targets in the fields of the production industry and politics. The control of know-how on the one hand and the control of infrastructure on the other is of similar importance to governments and companies today.

Increasingly, information about what we do on the internet today is being combined with other data about us. Almost everything we do now involves computer systems, which themselves produce new data as a by-product. Everything is being saved and correlated, in a way, that companies that collect the big chunks of data (i.e. Big Data), are able to make money from the individuals and build up profiles of their lives; namely, from all the various sources, that are interconnected with the internet. This also creates vulnerabilities in the individual's privacy, which is a fundamental right. Yet, it doesn't get the respect from foreign and domestic authorities it actually deserves. The lack of control of these authorities legislation- and institution-wise illustrates that all too well. In the short term, what is needed is transparency and oversight. The more knowledge exists about what the institutional power is doing, the more trust can be generated. Though corporate powers will not allow transparency (nature of competitive market), only laws would force them to accept insight.

The technological advancement in the upcoming years will promote processing power, artificial intelligence, storage capacity, internet speed and availability, and with it the extent of surveillance. The US, or the UK can hardly be seen as non-surveillance states any more.

The number of traceable tools has increased, whether it is concerning the e-mail, cell phone, search engine, tablet, web browser, and social networking. Everything has become a necessity, at least in business life. It would be naive to assume, that people would reject to use them, just because they don't like to be spied on; especially considering, that the full extent of espionage is hidden from us. Thus, even by showing all the encryption technologies and other tools to protect one's privacy, maintaining it on the internet is almost impossible.

So far, espionage was targeting state and company secrets and not people's privacy. In truth, the NSA's spying of German data servers differs fundamentally from the 'good old' espionage, which is known to (international) law. Countries are traditionally spying on foreign nations, and not on their citizens. Traditional espionage and cross-border surveillance of people are merging. In addition, a traditional spy takes always on the risk of being uncovered and punished for his action. Nowadays however, provided the resources and preparation, a 'cyber' spy works without any occupational risk. As such, the current (international) law is under these circumstances no longer maintainable and as a result needs a revision.

The real effective use of cryptography involves too much effort for the everyday user and is a rather complex process. Simple and intuitive concepts are needed that at the same time are transparent, so they won't contain the next exploitable backdoor. One must also steer away from systems produced in the US. While it is easier said than done, maybe an initiation by a

collaboration of countries can be started. Software-wise the solution is Open Source. This would guarantee open, free, secure and backdoor-free systems, so one can go around such extensive surveillance. For the individual the highest protective measure against institutional cyber spying is the use of encryption wherever possible. In addition, staying anonymous on the internet is one key factor to consider, especially when using social networks.

Today, it seems that only physical contact can guarantee the highest chance of exchanging information without it becoming compromised. Of course, the location must be secure, as well. As such, one has also to differentiate between information that is private, and what is confidential. This is even strengthened by the narcissism of million people, who share their information, and privacy online fully voluntarily, which eventually then is stored on servers of the NSA and other intelligence gathering authorities. Certain content just can not be communicated with other parties over the internet, for the sake of security.

Transparency is especially needed in the sector of infrastructure providers, internet node operators, and the providers of data cables and deep-sea cables. They all appear to play an important role in the extensive surveillance operations. At least the release of disclosed documents resulted in public attention and led to many internet users and companies deciding to develop and apply mechanisms to protect their privacy.

The early surveillance system Echelon has shown that intelligence services worked in cooperation, allowing partners to use collaborative contributed keywords in their own sphere of operations. In these days the approach has not changed, but only the technology developed very fast; too fast to be controlled by higher instances. Nowadays, the BND uses their partner's XKeyscore program, indicating that the NSA may have access to the same data sources, whether officially contracted or through espionage. Every detail is handled by the software, and the data flows unrestrictedly. Intelligence services have become uncontrollable. But intelligence services cannot be disbanded, because they are an important asset for the government, which wants to be informed about international activities and trends, as well as for the protection from hostile actions.

Given the huge amount of effective and versatile intelligence technologies and mechanisms, it would be naive to assume that companies would properly protect their sensitive data; especially, when one considers how dependant companies have become from network structures. Therefore, the problem must be tackled at the source, i.e. the governments of the world. Even if companies are threatened with sanctions and restrictions, an amalgamation of all the major companies and a rejection of the use of spying systems should be the goal. Companies who jointly go against it, cannot be sanctioned by the government, not in today's economy, where almost all leading companies come from the IT-sector (Google, Apple, Microsoft etc.).

Governments and unions of institutions will need time in the political process to adapt legislations to today's standards in technology, however, the discussion about intelligence gathering needs to stay present in the following years, laying focus on the establishment of alternatives to US-services and products, as well as on the need of transparency, in order to protect privacy and corporate information security. Start ups and companies, however, which concentrate on creating products and services on the internet, must make sure to encrypt everything, meaning data (e.g. user data), the data transport and the newest protocols, too.

Too little security is careless, while too much security is uneconomical. The target must be to find the right balance.

THE RESEARCH OF THIS THESIS IS BASED ON THE MAJORITY OF INFORMATION AVAILABLE UP TO OCTOBER 4th, 2013.

CHAPTER 10

Terms and Definitions

10.1 Terms and Definitions

Botnet refers to a collection of bots (or software robots), which run autonomously. The Botnet-controller can get access to foreign (previously infected) systems. The term can also refer to a network of computers using distributed computing software. Botnets are a popular tool to issue denial-of-service (DoS) attacks on other computer systems or networks, which result in a loss of service for the victims.[1]

Cyberspace "is the interdependent network of information technology (IT) infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[2]

Cyber War describes the use of data and software to carry out "attacks on computer systems and networks".[3]

Dropper refers to a software program, which performs basically two tasks at once. It "performs a legitimate task", and "installs a computer virus" or worm on a system simultaneously. It represents a carrier of the actual malicious software.[4]

Economic espionage "occurs when an actor, knowing or intending that his or her actions will benefit any foreign government, instrumentality or agent, knowingly: (1) steals, or without authorization appropriates, carries away, conceals, or obtains by deception or fraud a trade secret; (2) copies, duplicates, reproduces, destroys, uploads, downloads, or transmits that trade secret without authorization; or (3) receives a trade secret knowing that the trade secret had been stolen, appropriated, obtained or converted without authorization" (Section 101 of the European Environment Agency (EEA), 18 United States Code (USC) 1831)[5].

[1] [199]
[2] [156, p.7]
[3] [106, p.111]
[4] [200]
[5] [187, p.iii]

Honeypot in computer terminology is a set up computer system to attract and trap "unconventional or new hacking methods". It is specifically designed to identify malicious behaviour / activities.[6]

Industrial espionage, "or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner by: (1) stealing, or without authorization appropriating, carrying away, concealing, or obtaining by deception or fraud information related to that secret; (2) copying, duplicating, reproducing, destroying, uploading, downloading, or otherwise transmiting that information without authorization; or (3) receiving that information knowing that that information had been stolen, appropriated, obtained or converted without authorization" (Section 101 of the EEA, 18 USC 1832)[7].

Key-logger, also known as keystroke recording, are programs that create logs of all key strokes made on a computer system. The log file is saved on the hard disk drive and can be sent to other users. It is a popular monitoring tool, that can provide information on login credentials.[8]

Multi-factor authentication describes a security mechanism, where at least two (hence two-factor auth.) "types of credentials for authentication" are required. Besides the password, that a user has to memorise in order to get access to a restricted area (i.e. data), another method, such as an additionally required code sent to the user's phone number, provides a supplementary "layer of validation", reducing risks of security violation.[9]

Personal Data represents "any information" (i.e. content data and metadata) that is related to a distinct individual.[10]

Rootkit describes a software program (tool-kit), which grants full access (administrator/root) to a computer system, without being detected. That way, further modules (malware) can be loaded, and malicious operations performed.[11]

Sensitive Data represents information on an individual or object, that cannot be shared with other entities outside or inside "of an organization"[12]. This data often requires particular confidential handling and a security approach.

Social Engineering refers to the "practice of obtaining confidential information by manipulation" of humans. The exploitation of computer vulnerabilities is regarded to be more difficult, than "tricking people". Therefore, a social engineer misleads people by first building up trust, in order to get his victim to reveal "sensitive information" or other disclosures that might be "against typical policies".[13]

Trojan Horse describes attacks that are concealed inside otherwise innocent software. The user can be tricked into executing them in various different ways (e.g. free at Web sites, e-mail attachment, hidden in storage media, embedded in software). Computer viruses and worms

[6] [107]
[7] [187, p.iv]
[8] [106, p.181]
[9] [108]
[10] [106, p.119]
[11] [45]
[12] [106, p.119]
[13] [106, p.121]

represent forms of Trojan horses, but they usually reveal themselves as such in a more obvious manner. An important category of Trojan horses is spyware, or automated espionage in cyberspace.[14]

Virus describes a self-replicating program that spreads by inserting copies of itself into other executable code or documents. It is basically the software form of a biological virus.[15]

[14] [106, p.94]
[15] [106, p.6]

CHAPTER 11

Results and Discussion

In the previous chapters a situational analysis was done, giving insights into the newest discoveries in the area of governmental surveillance techniques and cyber spying leading to industrial espionage activities. The findings of the investigation shall be added into present literature and the results of the expert interviews give additional value to the limits and effectiveness of present security measures for companies, institutions and individuals. The purpose of the interview evaluation was to identify specific risks of know-how loss, and the existing and planned security measures against espionage, in order to be able to make statements about dangers of intelligence gathering, as well as about the resulting security measures.

11.1 Expert interview sample

Over the course of December (4th-19th) 2013, 7 Interviews with IT-Experts from various industry sectors have been conducted with the topic 'cyber espionage'(cf. chapter 12). The purpose of the investigation was to find out about risks that companies in today's information society are faced with. In addition, to discuss protective measures and to identify whether an appropriate level of awareness in the corporate culture can be noticed. Incorporating the results into present knowledge and the 'state of the art', shall help to develop measures that entities can use to protect themselves from the loss of sensitive information i.e. know-how. Outgoing from the question whether a viable protection from threats of cyber espionage and intelligence gathering is possible, over multiple companies have been contacted with the request of doing an interview with their IT-expert. In the end 7 interviews have been conducted.

The interviews on average took about 50 minutes and were targeted specifically on people with high responsibilities for the IT departments of their particular firm. The companies represented different industries, including a service provider for engineering, a service provider for risk management and insurance, an informatics service centre of an educational institution, a producer of energy- and automation technology, an operator of infrastructure, a producer of

security technology, and one of information technology. In addition, the interview participants have all come from either a middle sized (<250 employees)[1] company or a major enterprise (>250 employees). In the sample one company has been from a category of a middle sized firm, while the other six have been major enterprises (400-60.000 employees). Due to the very sensitive topic of cyber espionage all experts have agreed, that their identities as well as those of their employers are anonymized. Also, due to the rather small and - because of the circumstances - limited sample size, all the statements and the discussion should be viewed with respect to the restrictions and in the appropriate context.

11.2 The expert interview method

In this thesis the expert interview was selected as the primary qualitative data collection methodology.[2] The sampling process was more systematic than random, focusing on companies from particular cyber espionage endangered industry sectors, even though not all participants were affected by cyber espionage in the past. Expert interviews are a particular form of semi-structured interviews, where an expert is asked several questions according to the interviewer's compendium of prepared questions, in order to gather "expert knowledge", "facts" or "descriptions of processes"[3]. Occasionally the interviewer can ask other questions spontaneously, depending on answers from the expert, that might lead to other questions relevant to the topic of the thesis, or at least to delve more into detail and to "understand thoroughly the answers provided"[4]. Prior to the interview the IT-experts have been informed about the duration of the interview and the topic, and received a guided compendium of questions in order to get familiar with the particular topic. In all interviews basically the same - with only slight adjustments - compendium was used. With the experts' approval the interviews have been digitally recorded for easier transcription purposes (with one exception). Due to the questioned companies being located in Germany and Austria, all the interviews were conducted in German.

Interview: The topics

Risk analysis and evaluation

The loss of sensitive information (i.e. know-how) is an actual threat for innovative companies in particular. For all companies that do business, a network infrastructure and the internet are technologies that have to be used and relied on in today's competitive economy. To fight espionage and intelligence gathering in general, for companies it is necessary to analyse those risks adequately.

Within the scope of the interviews it becomes clear, that with the exception of the middle sized company (Transcript 1), all questioned companies have conducted a risk analysis at some point. However, the scope and classification vary considerably from company to company. It lies in the nature of business that smaller companies have to make decisions, that might neglect

[1] [34]
[2] [150, p.1]
[3] [150, p.24]
[4] [150, p.27]

specific areas of the company, such as information security, due to limited available resources. Nevertheless, the findings in this thesis yield various different results, even though the majority of questioned companies might appear one-sided in terms of company size. Throughout all the questioned companies different approaches can be seen, from the risk analysis and evaluation, over to policy regulations, information security, infrastructure, and up to the sensitization of personnel towards the topic of industrial espionage.

First and foremost, due to the sensitive topic all questioned companies have remained reserved on the topic of found vulnerabilities, derived from the risk analysis. In all companies there is a clear person responsible for information security. It is either the management or in other cases a Chief Information Security Officer (short: CISO), or IT-Manager (or similar), who are the responsible bodies for information security. Nevertheless, especially in major enterprises there are Information Security Managers, who delegate to the supervisor of their company's head department. In general, there is always one responsible individual or department in the area of information security (transcript 3, ll.9-20).

In terms of risk analysis and evaluation, all participants of the interview showed knowledge of the ISO 27001 certificate, but not all of them followed it's guidelines in order to get the certificate explicitly for their company/institution. For instance, the educational institution has plans to implement security policies in accordance with ISO 27002/2013 (t.2, ll.32-35), but not with the aim to get the certificate (instead, to implement it in best-practice). In another case in a major enterprise, the short term aim is not to get a ISO 27001 certificate, but to implement measures according to ITIL (Information Technology Infrastructure Library) and Sarbanes-Oxley, which requires appropriate processes and regular controls (t.3, ll.40-46). One would take partially requirements from several frameworks integrate and "live" a process that one is familiar with (t.3, ll.57-60). A risk analysis naturally starts with a Business Impact Analysis, which is conducted by the Division Managers and the Management (t.3, ll.64-68; t.6, l.41) on a regular basis. Another questioned company plans to follow a soon to come EU-directive in the data security or information security sphere, which derives several aspects of the ISO 27001/27002, but is not thriving for the certificate (t.5, ll.24-37).

In addition, risk analyses don't seem to cover the whole enterprise area, but are rather carried out on specific domains, like the personnel and finance sectors (t.2, ll.44-45). In one case, a company stated to have made a risk analysis, but focussed only on selective areas. However, there are considerations being done to conduct such an analysis over the whole company in the next year (t.5, ll.39-42). In regard to the areas with the highest risk potential, the security of the company's products (information technology), meaning customer care, was emphasized (t.5, ll.57-63), rather than the internal IT-security of the own company. In the educational institution there seems to be a considerable potential of improvement in terms of policies and measures regarding information security (t.2, ll.18-19).

After a risk (or security) analysis is conducted, naturally an auditor checks the resulting concepts annually (t.2, ll.44-46; t.5, l.413). Derived from the risk evaluation is a catalogue of measures, to counteract risks. In this regard it was stated, that one cannot view or predict all possible cases, that can occur. Moreover, it is often also a cost-benefit calculation on which the management would decide to implement such a measure or not. But overall, the "worst cases" would be covered (t.3, ll.75-78). There is also a difference, whether a company is "living" the

security process for a long time, or is just starting it. Namely, one would go from a situation, where measures have already been applied, and accordingly work from there on forward (t.3, ll.82-85). A particular example is, where design concepts already exist that include fail-over and redundancy. One would be protected to a degree against present and known threats, but if the time comes to do a refresh, one would need to look at the changed requirements and adjust accordingly (t.3, ll.85-91). One measure would be, for instance, to implement redundant systems so that data cannot be lost, when one system is failing. This goes further to disaster scenarios etc. (t.3, l.96).

The educational institution named data security and information security as the biggest risk factors in the SAP domain, where high volumes of person related data is run (t.2, ll.53-54). But also the potential risks to the know-how of bodies who are knowledge carriers was addressed (t.2, ll.57-58). With regard to priority lists that may have been derived from the risk evaluation, participants stated that such lists were not fully developed and executed, but there are plans to improve on that matter (t.2, ll.62-65).

In the case of the infrastructure provider, a risk analysis was conducted in the process of the corporate risk management, of which one segment affects purely the area of IT security (t.4, ll.28-29). The provider is IAES 3402 certified, which is certificate from the auditor's point of view. Compared to ISO 27001 this certificate is not quite that extensively, but goes more into detail. The risk analysis can be viewed as a matrix with two main parameters, amount of damage, and probability of occurrence, over a course of several years. The acceptance curve is then taken to derive measures. The risks are revised annually (t.4, ll.33-39). Unfortunately no statements regarding the sectors with the highest risks could be given, however, a classification of the risks has been done. One derived security measure has been the encryption of mobile devices such as smartphones and tablets, which are regarded as high security risks in the holding (t.4, ll.49-53). Another questioned company stated to use additional parameters in the evaluation, namely the recovery / repair time (t.5, ll.76-95), where the factors availability and reaction time play a major role. The same company also created priority lists (low to high risks), which are interpreted in a way, that only systems which are marked as being at 'low risk' can be compromised (t.4, l.101). The company emphasizes its technology and trademark protection, and the protection of their know-how, by having this rather sensitive information in segregated areas, cut off from the 'outside' (t.5, l.109). The Social Engineering aspect of industrial espionage is also mentioned, which is part of other scenarios and are even harder to manage (t.5, ll.111-121), due to incalculable factors such as the employee's (dis-)satisfaction. Derived from the risk evaluation have been several measures, which will be continuously applied in the near future. Therefore, there are considerations to make a new evaluation in order to reflect, whether the measures were effective or not (t.5, l.137). As an example, where measures need to be taken, the physical and digital access control to different sectors of the firm are mentioned (t.5, l.140). In this regard, emphasis must also be laid on the employees, who have to be sensitised on this topic individually (t.5, l.147).

Another questioned company stated to be ISO 27001 certified, however only for the Vienna / Austrian region (t.6, l.21). It was explained how a tool would calculate the total damage potential, including security measures (t.6, l.55-61). According to ISO 27001, measures must be conducted and the effectiveness must be verified. A security forum meeting is held every two

years to discuss this topic (t.6, ll.126-130).

Yet another questioned company said, that only after a case of internal sabotage (t.7, l.39), where the dissatisfaction of an employee played a role, the awareness in regard to information security on the management level increased (t.7, l.31). The company would be in the process of doing the risk analysis in accordance with ISO 27001, first specifically for the IT department only (t.7, l.60), and then for the whole enterprise (t.7, l.68). The whole certification process is described as lasting 2 or 3 years for the whole corporation (t.7, l.316).

Risks of business cooperation

Risks of know-how loss in business cooperation is apparent. NDA's are being signed with business cooperation partners (t.1, ll.36-43) to protect information leaks, but also trust plays a huge role (t.5, l.154). Recognised is also the need for protection, especially the outcomes that result from the cooperative activities, i.e. projects. However, strict protection is only done ad-hoc, rather than structured (t.2, ll.79-82). Others have a External Connectivity Guideline which declares, how the communication in connection to third parties should look like, also in regard to information security. This includes, for instance, that no external personnel is allowed to access the firm's network (t.3, ll.108-113). Business cooperation requires to look also on the security requirements of the partner, meaning which aspects can be controlled or what does the partner commit himself to do, so that mutual trust can exist and appropriate security standards can be actively implemented (t.3, ll.120-128). The infrastructure provider protects sensitive information by signing a NDA with his cooperation partner (t.4, ll.60-62). One company describes the situation more problematic, when data is handed over to a fellow affiliate, which does the production (t.5, l.160). Then, trust can only exist, when similar protection mechanisms or risk management systems exist on the partner's side (t.5, l.165). A major enterprise gives an example of how a project with another non-democratic country shows security problems, because the business partner demands security standards, that obviously provide him with communication monitoring capabilities (t.6, l.203). Since the NSA 'affair', no real confidential information would exist any more. Nevertheless, it is important to make the agencies' work as hard as possible (t.6, l.218). In another enterprise there is a lack of strict policies stated, that demand the signing of a NDA (t.7, l.109) and a rethink process on the management level.

Frequency and scope of cyber attacks

The middle sized company states to rely first and foremost on hardware firewalls of their provider, which seem to block most of incoming attacks (t.1, l.50). In one case, failed logon attempts from IP-addresses of Chinese origin have been reported (t.1, l.57). For the educational institution the analysis appears to be that the majority of attacks target the resources of the institution. This includes the bitcoin and primecoin hacks (t.2, l.87). In contrast to industrial espionage targeting the companies' sensitive information, the institution's massive resources are focussed. But also the risk of Social Engineering is present, which may happen occasionally, because employees might be unsatisfied with their job (t.2, ll.94-99). Cyber attacks do exist, especially worldwide, which affect major enterprises (t.3, l.132); even in form of Denial-of-Service attacks (t.3, l.142). In regard to cyber attacks, the infrastructure provider stated, that to his knowledge no cyber at-

tacks have been reported so far. He added, however, that the focus of such attacks in most cases is directed at confidentiality and accessibility (t.4, ll.65-67), which is of course of critical value for the provider and the city / country. One of the IT-requirements is that the data network is completely disconnected from the internet (t.4, ll.67-69), which is exemplary for a qualitative security measure in such a sector. In one case a questioned company stated that a major incident (some form of cyber attack) is happening every 3 years, even though there has been no event, where someone's target was to steal data (t.5, l.170). The incidents involved the company's resources, in order to use them to manipulate ratings at Google services, or in another case to use them as Spam-bots (t.5, ll.173-183). A simple way of doing espionage is described in using Social Engineering or poaching of employees, which in one case resulted in a lawsuit (t.5, ll.187-189). As a major espionage incident, Reverse Engineering is mentioned, which is in fact to the company's knowledge (t.5, l.204; l.210) was conducted by a regional competitor. Another company described one problem being the lack of awareness regarding cyber attacks, especially when considering that such attacks, espionage in particular, are very difficult to realise, when you can't consciously perceive them (t.6, l.151). Another representative of a major enterprise stated not to have the detailed statistics in regard to cyber attacks, due to multi-layered corporate security systems (t.7, l.124); however, there were ordinary activities on the firewall, which stay in solvable boundaries (t.7, l.135).

Communication with authorities

In regard to communication with authorities, the middle sized company said to have no knowledge, that authorities like an intelligence service (e.g. BfV) offer support and consultation in cases of cyber attacks (e.g. espionage) (t.1, l.64), whereas the educational institution to the knowledge of the IT expert is required to contact the police in specific cases (t.2, ll.103-106). This applies generally to all institutions that are financed with public funds. Major enterprises either do occasionally contact authorities (t.3, l.146). It is also stated that it's questionable whether Austrian authorities can really help effectively. That's something that eventually must be offered on a global level (t.3, ll.154-157). Quite surprising is the fact, that apparently no communication between the infrastructure provider and an authority existed (t.4, l.73).

In terms of reporting requirements, all participants pointed out its meaningfulness, but also the problems of reputation damage and other factors that come with it. Another critical topic is the existence of the danger, that someone, who reports cyber attacks, has a clear disadvantage to someone who doesn't report anything: In the end this results in reputation damage, and in the long run to a loss of market shares and finally financial loss (t.4, ll.75-79). Therefore, an EU directive would be necessary (t.4, ll.81-82) to address this issue.

One major enterprise states to have regular meetings (in specific cases, as well as informal), where information is exchanged between the company and an authority (t.6, l.176).

Personnel

All companies agree that personnel, or the human in general, is the highest risk factor (t.1, l.12; t.6, l.72). It must be addressed by sensitising employees (t.5, l.226) to the topic, including the risks of Social Engineering. Especially the negligence and the generally low awareness

in connection to the topic of security is a massive problem, that's often out-of-scope, which partially is not even regarded as a risk (t.6, l.74). Social Engineering tests would show, that although policies would exist, in practice the employee wouldn't have the matching awareness, that the policies would teach, which makes the topic really critical (t.6, l.80). The other problem that is described by a questioned major enterprise is the lacking continuity. One would put in effort, with respect to the upcoming audit only, and afterwards would neglect efforts again (t.6, l.90-100). Another factor is the neglect of the employee, due to the simple fact that for the longest time nothing severe happens, in order to raise awareness or at least keep it up-to-date (t.6, l.101). Companies would often also have too many policies (t.6, l.108), which would act counter productive. The interviewed expert illustrated a new approach in form of a security awareness training, which is a 3D training, where one would go through a virtual building and play through several situations at the workplace, including the topics of locking the display, password policies, data classification, the handling of data carriers etc. (t.6, ll.183-192). This course would need to be passed once a year, to ensure awareness. The employee's password handling is overall very difficult to monitor (t1., ll.13-15), even if the systems are well protected. Password changing is regarded as rather annoying and counterproductive. The middle sized company described trust as being one important factor (t.1, l.28), which is of course unsafe. The service provider for engineering stated that no particular education in regard to information security is done (i.e. following a policy), but rather the general information about risks during the business life is taught.

Education courses are also an outcome of the ISO 27001, and thus are planned to be introduced, according to another representative of a major enterprise (t.7, l.174).

There are security education courses and security awareness trainings in major enterprises (t.3, ll.163-164), which are obligatory for every employee who starts to work at the firm (t.5, l.234). Moreover, there are additional courses for managers (t.3, ll.168-170), as well as advanced information security courses for employees in the respective sectors. In those major companies there are security policies, including a software-asset-management policy, which declares that only a specific range of software is installed on a client's system (t.3, ll.177-181). Employees are not allowed to install Skype or other specific software, that could compromise sensitive information (t.3, ll.186-188; t.5, l.256).

There are partially further educations, which in general are improvable (t.2, ll.121-124). There is also a great degree of trust in the awareness of the employees, just out of the fact, that many would have educational background related to IT or an interest in that topic (t.2, ll.127-130), especially in the educational institution. In terms of education training, measures are planned, such as offering e-learning and videos to improve the employees' awareness (t.2, ll.136-138; t.3, l.172) and to sensitise them to approach information security more carefully, also in respect to the very high risks of social engineering (t.2, ll.330-344). Business trips and the risks of espionage vary of course from company to company, depending on its business culture, but in general is a topic that appears to be present in people's minds. Another company stated to introduce periodic workshops and courses in accordance with a new EU data protection directive, because employees would forget major information security aspects, if not taught on a regular (annual) basis (t.5, ll.246-251).

The infrastructure provider offers special education training with the topic of IT security (t.4,

ll.87-88) for its employees. In addition, the personnel is informed about security relevant topics over the Intranet (t.4, ll.88-89). Social Engineering plays also a role in the education courses. On business trips employees can use VPN tunnels, which are two-factor authenticated, and AES encrypted passwords.

During the application process no unusual or especially detailed research is done to the knowledge of the questioned interview partners. All questioned companies have policies that require personnel to sign a NDA agreement in their contracts (t.2, ll.118-120; t.5, l.234). One participant stated to go through Social Networks or other means during the application phase, to look what the applicant is doing, however, which is security on a rather low level (t.6, l.269).

In the event of termination of the service of an employee it is gratifying to see that all participants attach particular importance to the removal of any user access to the company's data at due date (cf. t.3, ll.114-119; t.5, l.324).

In terms of a protection requirement analysis that regulates which data / information is marked as confidential and the associated accesses requirements, the middle sized company stated, that they have particular authorisation levels for specific employees, especially during project work, where the authorisations vary (t.1, ll.129-134; ll.137-144). In another case in a major enterprise classification is being done during the business impact analysis, but not all too detailed (t.3, ll.223-224).

Regarding the structured removal of sensitive information, particularly paper, one participant states to prohibit to throw away relevant papers in the trash can (t.5, l.288). For the removal of data carriers, a certified external provider is commissioned (t.5, l.287).

Clean Desk Policy and Logging

A Clean Desk Policy is not really applied in any of the questioned companies or institutions (t.2, ll.153-154), or at least not strictly (t.3, ll.197-198), except in one major enterprise (cf. t.6, l.232). The Clean Desk Policy is especially for the provider of risk management and insurances of particular importance, where contracts are being made and potentially are openly put on the table (t.7, l.88).

The employees of the infrastructure provider, for instance, have instructions to lock the workplace, every time he or she leaves the room, as well as instructions to not leave confidential documents on the desk (t.4, ll.100-105). However, there are efforts to control the access to the building or specific rooms through doors that are locked or at least require the declaration. The stay of the visitor is logged, especially in the major enterprises.

When it comes to cleaning personnel or facility management care is taken, that the personnel is working under supervision and at least only during the business hours (t.3, ll.275-279; t.5, l.398). In the educational institution no further logging is done (t.2, ll.210-211). In one case, external personnel, who has to do maintenance, must sign a NDA (t.3, l.283).

Access

Especially the access to the Data Centre is restricted only to selected personnel (t.2, ll.195-196; t.3 ll.267-269; t.5, l.381-395), including IT-Managers and Management. The use of surveillance

systems is also an applied option (t.5, l.400). The middle sized company uses a centralised keyless system, which has proven its usefulness (t.1, ll.190-191). The infrastructure provider has access controls in form of card reading devices. Visitors get a card, which gives them access to enter specific areas. The entry is logged accordingly (t.4, ll.148-152; t.6, l.416). For the employees, VPN-connections are offered (t.3, l.193), however, their insecurity is also known to the personnel responsible for security.

Risks from data carriers and encryption of devices / data traffic

In terms of encrypting data carriers or data traffic (i.e. e-mail), the middle sized company once again relies on the employee, rather than implementing encryption solutions. One is aware about the risks from devices, but if someone wants to get the data, one would find a way to bypass such solutions to access sensitive data through other means (t.1, ll.170-177). Nevertheless, all questioned experts agree on the need of encryption solutions, especially the encrypted e-mail traffic. Some use it privately, some know that it is regularly used on the Management level (t.4, ll.138-140), but still it is something that needs more attention (i.e. through policies (t.1, ll.182-183)). Encryption today seems to work best in smaller project groups (t.2, ll.185-190). Encryption is a topic, especially when internet services are used (t.3, ll.230-231). If the necessity is given, the company is able to support the employee with encryption tools (t.3, ll.245-247). Threats coming from mobile devices like USB-drives are discussed in security awareness trainings. When it comes to encrypting devices, that is something that is planned to be offered to users. At the time, no throughout encryption of hard-drives is offered (t.3, ll.248-250). In regard to e-mail encryption, the employees have the possibility to enable a marker “confidential”, that activates encryption for a specific e-mail in their corporate e-mail program (t.3, ll.253-256). The encrypted exchange of messages with third parties is described as problematic, and thus is something to work on (t.3, ll.260-262).

No measures have been done regarding the risk of vulnerable data carriers (USB, external HDD etc.) according to the CISO from the infrastructure provider (t.4, ll.130-131), which illustrates an option for improvement. The infrastructure provider makes use of an application for their mobile devices that allows to encrypt data specifically on request (t.4, ll.140-142).

Another company states to use automated e-mail encryption with partners, who offer server-based encryption (t.5, l.342). This encrypts the communication over the internet, in fact within the whole company. The same company stated in regard to encrypted devices to have tried out a particular technology, but the cost-benefit ratio prevented a permanent integration (t.5, l.354). Especially in regard to security-related data, the emphasis must be laid on the sensitization of the employee (t.5, l.360). Moreover, strict care is taken not to put any security-related data on data carriers (t.5, l.367). The encryption with TrueCrypt is mentioned, an implementation of which in the end was neglected due to impractical reasons (t.5, l.372). The emphasis is laid on the internal firm’s network, instead of devices. Another major enterprise representative states to see lacking consequences, due to the compromise between usability and security (t.6, l.364). The blocking of USB ports or other numerous methods would be viable options to increase security, however, the administration or maintenance is rather complex, as well as impeding the work-flow (t.6, l.367). In the end, the implementation of such measures would fail due to the missing acceptance of security in business (t.6, l.371). There are plans to establish consistent

e-mail encryption, at least on the management level (t.6, l.384). The same company uses hard disk encryption on all their laptops (t.6, l.249).

In another major enterprise USB is regarded as a sensitive topic, which gets attention in accordance to the ISO 27001. In addition, laptops are encrypted. The e-mail encryption depends on the client's requirements / demands. In that case, Cryptshare would be used to secure the communication between the two parties (t.7, ll.227-237). Another requirement of a client can be to block USB devices, which is also a specification of ISO 27001 (t.7, l.280). The demand for this particular feature is increasing, especially in the financial service sector (t.7, l.284).

Another enterprise can not renounce the use of Skype, because in countries with poor connection in particular, the software would be needed (t.6, l.287). In this case one has to raise the employee's awareness about the program's lacking security. Overall Microsoft is regarded as a high risk factor in respect to state-affiliated monitoring (t.6, l.304).

Systematic password change

When it comes to password change big differences between the companies can be noticed. Some have strict policies that dictate the change to be applied regularly. Some change the passwords once every year (t.1, l.194), while others every 90 days for the most sensitive areas (t.2, l.216). At the infrastructure provider the normal domain user has to change his password every 84 days, and not only for one application (t.4, ll.162-166). Interestingly enough was the statement of the IT director of a service provider of risk management and insurances. He stated, that all employees have to change their passwords every 60 days (t.7, l.264). Moreover, it is ensured that all domains, including applications and devices are password protected (t.7, l.265).

According to a password policy, the password structure differs from company to company, but is often specified (min. no. of symbols, special characters etc.), as well as a history list, that checks, whether the password has been used previously (t.3, ll.292-300; t.6, l.445). At one company there are recommendations to use password managing software like KeePass (t.6, l.450). One particular problematic topic is described as being the ongoing fusion between private area, and business context, due to data becoming accessible from anywhere in the world, which brings risks (t.6, l.459). It also happens that especially passwords for the VPN access is given particular emphasis, and to the complex structure of the password (t.1, ll.195-196). Among the companies VPN is regarded as one of the highest IT-related risk factors (t1., ll.201-202), because it serves as a data access point, that represents a method comparable to a user who is sitting inside the company's building. As such the security of the building could be regarded as non-existent. In another case, VPN is restricted to a degree, where only 2 employees of the whole firm have access to it (t.5, l.273). The systematic change of passwords can also be a topic of discussion, as explained by one participant. A regular change of passwords would be pointless, just due to the fact that people would either forget them, or to counteract that issue, would write them down somewhere insecure or would choose a very simple structure (t.5, l.417). As such, the company decided to assign a randomised complex password (with a particular amount of figures) only once, that employees would need to remember. Simultaneously, any reuse of the password for other applications is prohibited (t.5, l.426).

Firewall, Anti-Virus, Anti-Spam

All participants have pointed out to have very good state of the art protection regarding Firewall, Anti-Virus and Anti-Spam software, partially stated to defend against almost 95% (t.5, l.440; t.7, l.275) of any cyber attack, including malware. Nevertheless, one participant has plans to improve these protection measures even further, even though arguing at the same time that already the effort for a perpetration would be immensely high, and for the sake of stealing data, other simpler and cheaper methods would be applicable (t.5, l.454). Many depend on multi layer (i.e. Firewall, Anti-Virus) protection, offered by the service providers (t.1, l.208). On all systems, where a user can access data, one has security mechanisms (t.1, ll.214-215). The infrastructure provider has a 3 level concept, where first at the firewall the data stream is opened. Then at the file-server, there is a scanner for both AV and AS. Finally, at the terminal devices there are also several different products available (t.4, ll.170-174). The infrastructure provider sees room for improvement in this sector, especially considering the highest threat coming from the data stream (in $\rightarrow$ out) (t.4, ll.176-178).

Updates and tests

All questioned companies have agreed on using regular software updates. In addition, all use semi-automated or manual update (cycles) (t.1, ll.260-266; t.4, ll.197-199; t.5, l.472-480; t.6, l.496) to prevent system failure caused by faulty software updates. Another security measure is described as not using a Microsoft network, including RPC, which would lead to at least 90% of the existing threats not to be distributed (t.5, l.483). In accordance with ISO 27001 one would use a predefined test environment, where security patches would be tested and deployed (t.6, l.497; t.7, l.292).

Some corporates have a centralised realisation of powerful solutions, so that the filter and thus the security systems can learn and adapt, reaching a good level of quality (t.3, ll.328-330). When it comes to regular announced or unannounced checks, meaning whether the realisation and efficiency of the security measures are working as intended, companies differ in their approach, but in general there is definitely room for improvement. If checks are done, the majority carries them out internally (t.1, ll.272). For instance, the infrastructure provider lets external providers to perform checks and penetration tests annually (t.4, l.203). Other companies use both, external providers, as well as an internal employee to conduct penetration tests (t.5, l.501; t.6, l.516). The middle sized company doesn't see itself endangered by cyber attacks (t.1, ll.230-232). Some also make use of an Intrusion Detection System (t.5, l.443; t.6, l.471; (t.7, l.271)), however, how much it really benefits is still controversial (t.2, l.236-240). In one case instead of a continuous Intrusion Detection System, selective examination (e.g. in form of a network analysis), and monitoring is conducted (t.3, ll.348-349). In this regard there is a security program that is adapted annually, which measures needs to be set in the security sector (t.3, ll.333-337). In the same particular case, there is also a vulnerability scanner mentioned, which additionally checks the security measures (t.3, ll.343-348).

Addressed is also the fact that the technical measure is rarely the actual security problem. Rather it is the sustainability and the management (t.6, l.477). In addition, there is the problem of evaluating the logging systems that many companies now have. The high data volume would

overwhelm many people, especially in making the right assumptions from the results of those systems (t.6, ll.486-494).

Another participant stated to have a missing of a true control instance, which would check security aspects on their effectiveness (t.7, l.300). The missing control mechanism goes down to the individual employee, also due to the lacking classification on the data level. But, the need for action is recognized and is planned to be implemented (t.7, l.306). The same company runs penetration tests monthly (t.7, l.310).

Risks of using mobile devices and cloud storage

Smartphones and tablets become increasingly powerful and cross-linked throughout the enterprise network. All interview participants agree that this topic needs attention, because sensitive data becomes available worldwide and the access to it requires special security measures. Mobile devices become problematic, especially where passwords are stored, when devices are poorly secured, and especially applications that give cloud access are seen as risk increasing factors (t.1, ll.246-250; t.6, l.306). As such, many companies renounce the use of cloud services during the business life (t.1, l.250) or even prohibit the use of it in general (t.5, l.256; t.5, l.519). However, in another case it is tolerated in exceptional cases (t.6, l.309). It is a problematic topic, because one would not exactly know how to deal with it. Especially, distinguishing between the private cloud use and the access to cloud data in the business network is difficult (t.6, l.312). One participant sees no possibility to protect mobile data, except by creating access through VPN (t.2, ll.282-285). All companies realise the power of cloud services and thus plan (t.2, l.292; t.7, l.364) the integration or already do utilise private (t.1, ll.253-254) (own-)cloud solutions. This cloud data is then exchanged with clients or in-between own employees. One participant states that the NSA 'scandal' has led to undertakings to realise an own cloud solution (t.6, l.316), where the data would stay within Austrian borders (t.6, l.323). The lack of legal certainty is also addressed, and the difficulty to assess the right legal measures on a topic, where personal data is involved (t.6, l.337). The very problem of the internet is not knowing which routes data is taking, and who can intercept this data (t.6, l.355).

Besides the obvious 'cyber' risks to mobile devices, there is also another aspect, namely the loss or theft of devices, which are becoming smaller and smaller (t.3, ll.364-367). This aspect is also part of the security awareness training. There have also been cases of theft. Thus, the corporation started to implement particular management-software on smartphones. Those devices are locked by default, and in the case of loss, the contents of the device can be deleted remotely (t.3, ll.374-376). There are plans to include similar functions on tablets. While the selection of mobile operating systems varies from company to company, iOS is regarded as being more secure, especially in the VPN domain (t.3, ll.389-391). The infrastructure provider for mobile devices mostly makes use of e-mail, contacts, and calendar applications on Windows Phones (only). For that, they have their own solution, a kind of container, which allows to separate private from business data. With this one can specify particular devices (and their OS). As such Android in the future will also be accepted as a business device the employees will be able to select (t.4, ll.183-190). In regard to 'public' cloud storage products it is emphasized, that there are clear legal requirements missing (t.4, l.217). The participants state also that the topic of cloud storage is a legal problem, because one doesn't know where exactly the data is located, and who may

have access to it (t.4, ll.224-227; t.5, l.257), which is a K.O. criteria to store sensitive data. This is a topic that is also long discussed in the EU, and still is not solved (t.4, l.227). Cloud solutions are nevertheless used, even though only if it is necessary (t.4, l.216). It is the task of the EU and other institutions to create general conditions and setting rules for today's problems regarding digital information (cloud, privacy etc.) (t.4, l.252). Another company states to not use any mobile devices at all (t.5, l.507), keeping risks low. One would focus on the internal computer network infrastructure, which is partially built up separately (t.5, l.514). The same company claims to use an own cloud solution in form of a MPLS (Multiprotocol Label Switching) network (t.5, l.525), which provides restricted mobile access. Thus no free internet access exists during the connection (t.5, l.533). Yet another enterprise emphasises on the organisational challenge, rather than the technical security aspects, which are easier to solve (t.6, l.535). Today's threats to information security would demand the commitment of the management to focus on one particular product / solution (e.g. Apple) throughout the whole enterprise, which would be more efficient, also in regard to support (t.6, l.540). Another expert describes having a selection of only two mobile systems, iOS and Microsoft. The Android OS would be regarded as very vulnerable (t.7, l.348). The same person states using HiDrive as an alternative to Dropbox and others (t.7, l.361).

Open Source as an alternative

Open Source products became present in media after the disclosed documents of Edward Snowden, indicating installed backdoors in commercial software and hardware, that provide national authorities like the NSA access to various data sources. All participants agree that Open Source on the one hand is a viable option, as seen from Linux (t.5, l.542). However, today those products still cannot compete with the established market leaders such as Microsoft on the business / enterprise level. Three Problems are pointed out. First, the possible incompatibility during data exchange (t.1, ll.264-266) between the client and the service provider, because the client may use and dictate particular products. Then, there is the cost factor (t.1, l.267), because Open Source is not always equals free. In many cases, especially on the enterprise level, there are license fees. The last factor is emphasized on being the risk of lacking support in the long run (t.4, ll.239-241). Companies today rely heavily on long term support, and Open Source products just cannot fully guarantee that (t.5, l.551; t.7, l.391). The educational institution in particular states to have a long Open Source tradition and thus agrees on its usefulness (t.2, ll.307-315). Not least, because the community knows the source code, which prevents potential backdoors. One major enterprise decided to implement Microsoft's SkyDrive Cloud solution, as well as Office 365, which will be made available to the employee (t.3, ll.396-406). In an international corporation, where the headquarters are based in the US, it is almost impossible to use software that is of non-American origin, meaning Open Source solutions cannot even be seen as an alternative (t.3, ll.413-416). Another aspect pointed out is the fact, that in most cases the weakest point of a linked structure, like a company's network, is attacked, if the intruder purposefully wants to get hands on data (t.3, ll.423-425). Another enterprise states that the are not enough providers to select an alternative from (t.7, l.380). Moreover, today the problem also lies in the installed hardware, which is developed in China or in the US (t.6, ll.551-557), and as such would represent a level of risk. For a US American concern, the question of an alternative doesn't come up

(t.7, l.380).

Insurance - an option?

In general, many questioned companies have never heard of insurance options like the cyber insurance, or the damaged trust insurance. The middle sized company stresses the fact that trust in the service provider sector plays a significant role in business. New clients would be won by good references. And trust is also a factor that plays a role in the application process, where employees are selected which give a very good feeling (t.1, ll278-282). It may be an option for the US market, but at the moment the companies in Austria don't seem to have knowledge of the existence of such insurances. Interestingly, the provider for insurances stated not to offer any insurances against espionage at the moment himself (t.7, l.403).

Possible counter measures

Companies stand before challenges to find the right balance in finding opportunities to reduce the risk potential, which don't limit the business activities. Security approaches also depend on the industry, in which the company does business. Therefore it makes sense to implement particular extensive protective measures in companies, where sensitive data is created, exchanged or transferred. In the following list a number of possible counter measures can be viewed as indicators to consider towards raising awareness, and as support to lower risks outgoing from intelligence gathering and espionage.

Organisation (Risk management)

- Conducting risk analysis and evaluation, in order to realise the security requirements and adapt the company's culture accordingly should be conducted by every company. Emphasis must be put on the aspects of information security and the human factor. In terms of potential threat scenarios, there should be as many possibilities considered as possible. Security concepts like ISO 27001 should be sought.
- Derived from the risk evaluation a catalogue of security measures should be developed. Priority lists would help to assess the right resources to the respective issues.
- Carriers of sensitive information, such as contracts or hardware (i.e. USB-drives) in general, should never be left unattended. This concerns the corporate area (building), and especially external stays (i.e. hotel).
- No longer required data and documents should be destroyed. Certificated external service providers can be commissioned, however, it may represent an additional risk.
- Security standards should be revised and tested regularly.
- Authorities such as the BfV may be consulted in terms of existing threats and protective measures. However, the use of software or hardware advised, should be taken with care. Security firms may be a good and secure alternative. The same goes for ENISA.

- Handling the risks to information security requires know-how and the right decision making. Communication between IT and overall senior management is key, so that the right decisions can be made.
- Introducing External Connectivity Guidelines and signing of NDA documents should always be a priority. This applies for business partners, employees, and external specialists.
- Worst-case scenarios should be defined, in order to be able to react goal-oriented.
- In general, security policies need to be created, however, one should not rely on the policies alone. Control mechanisms should review the compliance of policies regularly.
- Clear Desk Policy and strict ownership should be defined and applied.
- Objects that are not contributing to the business should be removed.
- Distinct communication pathways should be defined to increase security.

Personnel

- One should not purely rely on trust to the employee.
- Depending on the size of the company and the restricted access areas in different departments, a true identification of a person should be visible (i.e. identity card).
- In order to raise the awareness, regular education trainings and sensitization courses should be conducted. New forms of training can be e-learning, videos and virtual 3D games. The relevant topics should include:
  policies, malware, password changing, business trips, business cooperations, APT-recognition and social engineering.

IT-security

- Encryption of all communication and storage media should be aspirated.
- Electronic mobile devices such as laptops, tablets and smartphones are to be secured with appropriate security software. In addition, they should be password locked, and communication should be encrypted. One should also be able to delete the contents remotely in cases of theft. Especially laptops or netbooks should have the minimal configuration installed.
- The use of cloud storage and (Video) chat programs should be restricted or avoided completely. Own cloud solutions are to be implemented.
- The access to the data centre should have the highest security standards. The entrance needs to be restricted and the servers must be kept in a separated area.
- Is an Intrusion Detection System in use? The detection of APTs usually involves the implementation of network intrusion detection software.

- Are content scanners or sandboxes available to test malware, security updates, and to conduct penetration tests?
- Can a malicious file in an e-mail attachment be intercepted? Indicators are the sender, the list of recipients (if more than one); the subject and the attachment are all indicators which need to be analysed in detail. Archived files, pictures, PDF, DOC, EXCEL - all these potential attachments can contain malware and thus need to be handled with particular attention. The body of the message can already indicate 'red flags'. A particular look should be taken inside the e-mail headers. The headers contain detailed information such as the sender's IP-address and the ISPs information.
- Hard- and flash-drives like USB-drives can carry malware, as well.
- Gifts (i.e. USB drives) should be regarded with care in particular.
- Are there vulnerable systems existing (and still connected to the network), which could be compromised and exploited? A chain is only as strong as its weakest link.
- In terms of software, transparent solutions should be sought such as Open Source products, or at least products that are made outside the US or China. This includes service providers (e-mail etc.).
- Anti-Virus, Firewall and Anti-Spam software should preferably be multi-layer solutions and should be kept updated, but should not be regarded as all-in-one solution.
- All users and devices that are interacting with the network need to be declared and life cycle management policies and procedures need to be developed.
- Patching must be up-to-date. It must be made sure that important infrastructure systems are running at high efficiency.
- Sensitive data and critical infrastructure (i.e. control systems) in particular should be kept disconnected from the internet.
- Changes as to data access should be conducted regularly (i.e. changing account credentials). Two-factor authentication is a good option to consider, especially when remotely accessing VPN.
- For stronger network protection, the introduction of isolated security zones including computers and domains is a viable option to consider.
- The implementation of at least one 'honeypot' for early warnings should be taken into consideration, which are relatively low in cost, but have excellent detection capabilities for networks. The honeypots should never be touched after the initial installation in order to maximize the potential of detecting unusual behaviour.
- If possible, the selection of mobile devices and operating systems should be limited to only one particular manufacturer, preferably the one with the most security features.

- In respect to sensitive information, the use of electronic devices and systems should be avoided to a large extent.

Overall, today it is required that information security becomes a major part of the corporate culture, which must be integrated in the corporate strategy.

Outlook and Conclusion

In general, many security measures first and foremost depend on the policies outgoing from the management. In major enterprises or institutions, where many sub-departments exist, it also comes down to the single department manager or institutes, which have their own sub-territory. The interviews showed also, that companies in Austria seem to be rather rarely affected by cyber attacks; even though to make proper conclusions, the sample size has to be increased significantly.

All companies see room and potential for improvement in any sector related to information security, aside the 'already well secured' IT area.

The companies also differ in their approaches to create policies. Some policies go into detail of the IT security sphere (e.g. password structure, encryption), and others have only the basic regulations, which are neither controlled, nor repeatedly trained.

Regarding the discoveries all around the NSA, all security experts stated, that everything was more or less known, what would be technically possible. As such, it was not a big surprise to see the methods used by worldwide intelligence services (t.2, ll.319-322; t.4, ll.250-252), but it definitely helps to raise overall awareness on the topic of espionage (t.2, ll.343-344). Final conclusions are yet to be made, on how to protect the company against potential cyber spying from authorities. One questioned expert even mentioned ECHELON (t.5, l.566), that had already shown institutional capabilities of surveillance and of intercepting communication on a global scale: A system, which, as shown in this thesis, was neglected by governments and institutions to create first and foremost legal requirements to address the topic with the seriousness it deserves.

Lessons to take from the NSA's cyber surveillance program is for business to become more alert to the threat of cyber attacks and spying. Today one would not need to enter through the front door, because information can be gained through the internet and other means such as phone hacking and cyber attacks. In regard to personnel, there are two threats that become apparent. One is the demotivated employee, who can be a risk, as one interview showed. Another is for employers to remain vigilant to their employees' behaviour, that might give clues to their true intention. Penetration tests should be conducted to test security arrangements by all companies whether small, middle or large.

The interview findings show, that proper measures against industrial espionage are very diverse and thus difficult to implement, for middle sized companies, as well as for major enterprises. Throughout all the risks, the 'human factor' appears to be the one with the highest risk level regarding industrial espionage. This is especially so in the ever growing technological era, where the company's sensitive information is stored as data and is available from any point in the world through the means of the internet. However, many companies, first and foremost the management, have yet to reach an awareness level, that can ensure the maximum potential

of security in a company. Thanks to the discoveries in 2013, both management and the other working employees begin to notice what is technically possible and what is being done in terms of state-affiliated espionage. It is up to the management to introduce education and sensitization measures in order to improve overall information security. With further technological advancements and developments, as well as increasing competition on the global market, cyber espionage will increase further in the future; especially, considering global 'player' countries like China and Russia now had an insight into the intrigues of all the Five Eyes members. They all will strive for the increase of their own intelligence gathering capabilities. Threats are also outgoing from countries like France and even Germany. In the near future smart devices such as 'Smartwatches' may become standard, that could be used by visitors, cleaning services or employees of the facility management, and impose additional threats to information security. As such, besides conducting background checks on business partners or new applicants, a lesson taken from recent events may be to keep smartphones and laptops containing sensitive information at home. The same goes for business travellers, where risks of industrial espionage are particularly high.

Eventually, it is now the right time for decision makers to consult with IT-experts of their companies or established security firms on how to improve their own information security, and which methods are necessary to fight against industrial espionage, but also competitive intelligence. All too often, despite the existing threats no sufficient awareness exists, the risks are underestimated and prevention measures omitted. One can have the most advanced security measures, however, if the human in front of it, without having the appropriate awareness, is the highest risk factor, then in this case the best technological security is worth nothing.

CHAPTER 12

Expert-Interviews

12.1 Interview Transcripts

12.2 Transcript 1

Name:	Herr E.
Position:	EDV-Verantwortlicher
Branche:	Dienstleister für Engineering (ohne eigene Produktion)
Datum:	04.12.2013 13:50-14:30

Interviewer: Vielen Dank, dass sie sich für das Interview Zeit genommen haben! Ich werde nun einige Fragen zu den drei verschiedenen Bereichen Risk-handling, Personal und Sicherung und Kontrolle der IT stellen. Fangen wir mit den Risiko-behandelten Fragen an.
Gibt es eine Sicherheitsverantwortliche Instanz im Unternehmen? Wenn ja, ist diese organisatorisch mit der Geschäftsführung verbunden?

H.E.: Die Geschäftsführung.

I.: Da sie weder Risikoanalyse und Bewertung gemacht haben, können Sie zumindest aus Ihrer Sicht die größten Risiken nennen?

H.E.: Das größte Risiko ist sicher der Mensch. (...) Da gibt es sehr viele Faktoren. Man kann die Systeme einerseits „von - bis" absichern, aber wie die Mitarbeiter mit Ihren Passwörtern umgehen ist nur sehr schwer zu kontrollieren. (...)Es ist eine Gefühlssache. Schätzt man die Risiken richtig ein, oder ist man da auf der richtigen Spur.

I.: Primär ist natürlich die Kontrolle ein Problem, selbst wenn man Sicherheitsmechanismen in irgendeiner Form erstellt hat, die Mitarbeiter gleichzeitig zu motivieren und Vertrauen zu vermitteln.

H.E.: Man hat ja natürlich auch einen Zielkonflikt wenn man die EDV Systeme betrachtet, weil alles was Absicherung und Sicherheit ist, auch mit Mehraufwand verbunden ist. Zum Beispiel die lästigen Passwortwechsel von Firma B, welche wir zufälligerweise kennen. Wir versuchen da einen Mittelweg zu finden, damit unsere Mitarbeiter richtig können. Das heißt auch, dass wir den Mitarbeitern selber vertrauen und versuchen da einen Kompromiss zu finden (. . .). Man kann es nicht wirklich nur auf einer Seite optimieren. (. . .) Weil wenn man alles absichert bis ins letzte, dann können die Mitarbeiter nicht vernünftig arbeiten. Das habe ich oft genug erlebt.

I.: Sie haben ja angesprochen, dass es ist ein Dienstleistungsunternehmen ist. Inwieweit werden Unternehmenskooperationen denn auch als Risiko angesehen?

H.E.: Da ist es eigentlich überschaubar. Wir haben mit unseren Kunden Geheimhaltungsvereinbarungen und da darf natürlich nichts passieren. Wir müssen da Geheimhaltungsvereinbarungen unterschreiben, sobald wir einen Auftrag annehmen. Genauso müssen unsere Mitarbeiter Geheimhaltungsvereinbarungen unterschreiben. Das steht so im Dienstvertrag. Es ist für uns natürlich sehr wichtig, dass es da eben kein Know-how Transfer gibt, weil eben auch wir teilweise für konkurrierende Unternehmen arbeiten.

I.: Können Sie vielleicht etwas zu Häufigkeit, Umfang oder Systematik von Cyber-Angriffen auf Ihr Unternehmen sagen?

H.E.: Da bekomme ich eigentlich relativ wenig davon mit. Wir haben ein zweistufiges Firewall-System.
Einmal eine von unserem Provider gewartete Hardware-Firewall und hinten nachgeschalten noch einen Microsoft ISA (Internet Security and Acceleration) Server. (. . .) Diese Hardware-Firewall blockt eigentlich schon alles. Wir haben auch Systeme die nach außen offen sind, und da sieht man gelegentlich fehlgeschlagene Anmeldeversuche. Wir haben also ein spezielles System für Datentransfer mit Kunden, Lieferanten und Partnern. Das ist im Prinzip ein eigener NAS (Network Attached Storage) Server und da sieht man gelegentlich Angriffe durch chinesische IP-Adressen, also so etwas wie 5 fehlgeschlagene Anmelde-

versuche (falsches Passwort).

I.: Ok, d.h. es gibt zumindest Versuche von extern in das System zu kommen. Nun gibt es ja polizeiliche oder nachrichtendienstliche Sicherheitsbehörden, wie z.B. das Bundesamt für Verfassungsschutz, die Hilfestellung bzw. Support für Unternehmen anbieten. Gibt es (oder gab es) allgemein Überlegungen Ihrerseits Sicherheitsbehörden zu kontaktieren?

H.E.: Also das war mir gar nicht so bewusst, ehrlich gesagt. Man ist natürlich konfrontiert mit privaten Dienstleistern, die einen Service anbieten wollen, aber ich habe bis jetzt noch nie daran gedacht, diese in Anspruch zu nehmen. Wir haben einen lokalen Internet-Provider. Zu dem haben wir ein sehr gutes Verhältnis und daher auch ein gutes Vertrauen. Zumal dieser bei uns auch die Firewall macht und da geht es in die Themen rein wie Trojaner, Virenbefall usw. Sonst gibt es ja nichts mehr die letzten Jahre. (. . .)

I.: Was halten Sie von der Meldepflicht für Cyber-Angriffe?

H.E.: Also als erstes muss man einen Cyber-Angriff bzw. einen Verlust von Daten einmal feststellen. Da fängt es ja schon mal an. Da muss ja ein gewisser Standard da sein. Was ist ein Angriff und was nicht. Eine Meldepflicht wäre sicher sinnvoll, aber schwer umsetzbar. Da müsste es die Firewalls mit standardisierter Eindringungserkennung geben oder so etwas in der Art.

I.: Ok, kommen wir nun zum zweiten Bereich, und zwar dem Aspekt der Mitarbeiter. Sie haben ja Mitarbeiter kurz angesprochen. Gibt es dahingehend eine Schulung oder Sensibilisierung wie mit man mit Daten umzugehen hat?

H.E.: Es gibt da speziell nichts dazu. Für jeden unserer Mitarbeiter gibt es zu Beginn sowieso Schulungen, wo dann die ganzen Themen betreffend Geschäftsleben mitbehandelt werden. Also sowas wie: Wie werden Daten transferiert vom Kunden zum Kunden. Allerdings nicht nach einer Richtlinie o.ä.

I.: Nun gibt es ja erhöhte Risiken in Bezug auf Cloudservices und Malware die sich über E-Mail Attachements verbreitet. Das wird also, wenn überhaupt, auch nur grundlegend bei diesen Schulungen vermittelt?

H.E.: Ja, bzw., solche Dinge wie Malware haben wir generell schon sehr gut abgeblockt. Wenn ich dahingehend was sehe, dann über eine entsprechende Warnung. Generell muss man sagen, dass unsere Mitarbeiter Maturaniveau und aufwärts haben, und es sind schon Leute die größtenteils Technik- und Computeraffin sind, auf die man (. . .) auch weitgehend vertrauen kann.

I.: Haben Sie Regularien betreffend der Clean Desk Policy?

H.E.: Nein. Wobei unsere Büroräume selber ja nicht öffentlich zugäng-

lich sind. Besucher, so wie Sie, der wird dann vom Gastgeber begleitet. Wenn ein Kunde oder Externer jetzt in die Büroräume reingeht, dann wird das vorab bekannt gegeben, sodass da keine geheimen Unterlagen o.ä. ersichtlich sind.

I.: Also, wenn z.B. Laptops oder Speichermedien (auch über Nacht) mal auf dem Tisch liegen gelassen werden, dann ist die einzige Sicherheitskomponente die Eingangstür und die Berichte darüber, wer sich im Gebäude aufgehalten hat.

H.E.: Aber sowas werden Sie bei uns nicht sehen. Ich beobachte das ja auch so stichprobenmäßig. Sind die Computer wo die Leute dran angemeldet waren gesperrt usw. Die Leute sind schon bedacht drauf und dahingehend auch informiert, dass da natürlich das System nicht geöffnet werden sollte. Wir haben zusätzlich das Thema, dass Leute extern arbeiten oder zumindest mal lange Zeit beim Kunden sind oder überhaupt im Außendienst arbeiten. Wodurch wir denen zumindest einmal Zugang bieten. Zumindest mal zur Arbeitszeiterfassung über ein Web-interface oder bis zu VPN-Verbindungen die extrem gefährlich sind, wenn man nicht aufpasst.

I.: Findet im Rahmen des Personalauswahlverfahrens eine intensive Überprüfung der Bewerber statt (insbesondere im Bereich der IT)?

H.E.: Die üblichen Verfahren, wo es sich aber hauptsächlich um Qualifikation handelt. Wir hatten dahingehend auch noch keine Probleme, dass mal illegal Daten transferiert worden wären.

I.: Inwieweit wurde denn eine Schutzbedarfsanalyse durchgeführt, die für alle regelt, welche Daten / Informationen geheim, vertraulich oder offen zugänglich sind?

H.E.: Das ist sowieso durch die Berechtigungen geregelt. Bei uns passiert es auch mal, dass Externe beim Kunden arbeiten. Die haben dann auf unsere Geschäftsdaten keinen Zugriff. Genauso wie jetzt nur Mitarbeiter auf die entsprechenden Projekte Zugriff haben. Selbst dort gibt es auch verschiedene Mitarbeiterlevels.

I.: Wird der Zugriff dann über individuelle User Accounts & Passwörter geregelt?

H.E.: Ja, wobei auf Projektebene wir das auch nur wirklich machen, wenn das sehr geheime Projekte sind. Nachdem wir auch Großraumbüros haben, muss es auch eine Vertrauensbasis geben zu den Leuten und untereinander. Aber es gibt natürlich manchmal Projekte wo man halt verstärkte Geheimhaltung hat. Dann werden auch entsprechende Verzeichnisberechtigungen so gesetzt, dass

nur jene Leute Einsicht in die Projekte haben, die am Projekt arbeiten müssen. Also die Möglichkeiten haben wir sowieso alle, aber es muss auch im richtigen Verhältnis zum Aufwand stehen. D.h., dass der Administrationsaufwand da nicht explodiert. Wobei, wir auch schon nachdenken über so etwas wie Dokumenten-Managementsysteme und PDM (Produkt Daten Management), wo sich das Thema dann auch verbessert. Denn dann hat man das dann wirklich durchgehend.

I.: D.h. sie sehen dahingehend auf jeden Fall Verbesserungspotential?

H.E.: Ja. Das Thema ist nun mal bei uns und auch bei vielen anderen Firmen so, dass man Daten in vielen verschiedenen Systemen verteilt hat und da dann die Berechtigungen einzeln zu setzen sehr aufwändig ist. Und wir haben eben das Bestreben, dass wir das auf möglichst wenige Systeme zusammenführen. D.h. das wird ein ERP-System werden und dazu ein DMS (Data Management System) und dann gibt es im Prinzip nur noch diese beiden Systeme mit den Berechtigungen. Dann definier ich die Projektmitarbeiter und diese dürfen dann die Daten sehen. Es gibt sicher da noch Möglichkeiten das zu optimieren, aber das passiert jetzt nicht aus dem Grund, weil wir die Angst haben, dass es da Unsicherheiten gibt, sondern weil wir gerade beim Ablauf uns von der Produktivität Verbesserungen erhoffen. Wir werden aber sicherlich einen Vorteil was Datenverwaltung und Datensicherheit angeht daraus ziehen können.

I.: Inwiefern wird auf das Risiko gefährdeter Datenträger (USB-drive, HDD) geachtet und spielt die Verschlüsselung von Datenträgern und Datenverkehr (insb. E-Mail) bei Ihnen eine Rolle?

H.E.: Nein. Wir sehen es ja an unseren Kunden. Wir haben da einige große Firmen, die versuchen da bis ins letzte Detail abzusichern und zu reglementieren. Und man sieht es trotzdem, dass Leute ihre Wege finden da an die Daten zu kommen. Es kann ja durch-
aus vorkommen, dass wenn man mal schnell gehen muss, dann man mal eben den USB-stick jemandem übergibt und irgendein Computer fängt letztendlich einen Wurm. Also wir schauen schon da sehr auf die Mitarbeiter.

I.: Zutritts- und Zugriffsberechtigungskonzepte haben Sie ja schon angesprochen. Wie sieht der Zugang zu z.B. dem Rechenzentrum konkret dann aus?

H.E.: Sie haben es ja gesehen. Wir haben ein Schließsystem wo der Zutritt personenspezifisch geregelt ist. Wir haben die mittlere Führungsebene, die Rund um die Uhr Zutritt hat. Die an-

deren Mitarbeiter haben nur zu den Geschäftszeiten Zutritt. Und zum Serverraum haben eh nur ich, der Geschäftsführer und noch 2 weitere Personen Zutritt. Das ist eigentlich gegenüber dem Stand, den wir vor 5 Jahren gehabt haben, ein enormer Fortschritt. Für den Zugang zum Rechenzentrum haben wir ein zentralverwaltetes Keyless System. D.h. wenn ein Schlüssel verloren geht, dann kann man den sofort sperren. Das ist eine tolle Sache und hat sich auch schon bewährt.

I.: Wie oft gibt es einen systematischen Passwortwechsel und gibt es diesbezüglich Regelungen (z.B. minimale Anzahl an Stellen)?

H.E.: Ja, jährlich. Bei den Passwörtern haben wir keine allzu strengen Regeln. Wobei außer bei Usern, die extern über VPN Zugriff haben, da andere Standards gelten. Ich bin der Ansicht, ich muss da jetzt kein 16-ställiges User-Kennwort fordern, mit Sonderzeichen und Ziffern usw., wenn üblicherweise eh schon kein unberechtigter ins Haus reinkommt. Anders verhält es sich natürlich bei Leuten mit VPN Zugriff. Da schlage ich dann persönlich Kennwörter vor. Gerade in diesem Bereich sehe ich auch das größte Risiko. Mit einem Gebäude, das ein vernünftiges Schließsystem hat, hat man ja schon sehr viel verhindert. Aber natürlich ist ein VPN Zugriff genauso gut, wie als wenn er intern sitzen würde.

I.: Sie hatten angesprochen, dass Sie Firewalls nutzen. Also gilt das auch für die Anti-Virus und Anti-Spam Software genauso?

H.E.: Ja, also wir haben das grundsätzlich vom Provider her. Ist auch alles mehrstufig. Anti-Spam ist Providerseitig. Anti-Virus ist auch auf der Firewall. Die hat auch Wartung und Aktualisierung (. . .). Außerdem haben wir noch Clientseitig auf allen Rechnern zentral verwaltete Anti-Virus Software. Und am Exchange Server auch. Falls wer über Webmail zugreift, dann ist das auch abgesichert. Auf allen Systemen, wo man mit Nutzerdaten zugreifen kann, hat man Sicherheitsmechanismen.

I.: Werden Ihre IT-Systeme regelmäßigen Updates unterzogen, wenn ja, wie oft?

H.E.: Aktualisiert wird vollautomatisch, zentralverwaltet über unseren hauseigenen Updateserver. Wo wir uns etwas schwer tun, ist natürlich wenn Leute mit Laptops unterwegs sind. Da weiß man oft nicht, ob jemand jetzt eine Woche nicht da gewesen ist oder er den Anti-Virus abgeschaltet hat o.ä.

I.: Also das heißt, dass Geräte wie Laptops ausgegeben werden, und es wird darauf geachtet, dass diese immer „up-to-date" bleiben?

H.E.: Ja.

I.: Gibt es denn auch regelmäßige (un-)angekündigte Prüfungen auf

Umsetzung und Effizienz der Schutzmaßnahmen (z.B. Penetrationstests durch interne Stellen oder externe Dienstleister), wenn ja, wie oft?

H.E.: Nein, die gibt es nicht. Ich sehe das auch eher als Thema: Wie interessant ist man als potenzielles Ziel. Ich glaube da sind wir noch weitgehend unter dem Radar.

I.: Computersysteme, die Zugriff auf sensible Daten haben, sind daher auch benutzerabhängig geschützt?

H.E.: Jeder Mitarbeiter hat seinen eigenen User-Account. Allgemein-User gibt es nicht. Und es gibt auch für entsprechende Geschäftsbereiche jeweilige Benutzergruppen im Active-Directory. Und das ist dann auch nach Bereich selektiert, wie z.B. auf die Bürodaten, und welcher Mitarbeiter diese braucht. Das betrifft z.B. einen Techniker jetzt nicht, weil er keinen Zugriff auf irgendwelche administrative Daten hat. Das ist dann auf Freigabenebene geregelt.

I.: Wie würden Sie die Risiken des ungewollten Know-how-Abflusses mit der zunehmenden Verwendung mobiler (und leistungsstarker) Geräte wie Tablets und Smartphones ein?

H.E.: Ja, das ist ein ernstes Thema. Vor allem wenn es dann um Applikationen geht mit Cloudzugriff etc. Vor allem dort, wo die Kennwörter gespeichert werden. Das ist vor allem deshalb ein Thema, weil die Geräte teilweise auch noch schlecht gesichert sind. Wobei bei uns im Geschäftsbetrieb die Cloud nicht genutzt wird. Der mobile Zugriff betrifft eigentlich primär Email, also Exchange (Kontakte, Email, Kalender). Was den Datentransfer angeht, (. . .) da kann man sagen, dass wir eine Art private Cloud betreiben. Das ist im Prinzip ein Speicher, der von intern und vom Internet aus erreichbar ist. Ein Ort, wo wir eben Daten mit unseren Kunden austauschen und unterwegs auch mobil drauf zugreifen können. Das sind ganz spezifische Daten, die dort behandelt werden.

I.: Im Zuge der letzten Meldungen zu Abhörpraktiken wurde bekannt, dass angeblich Hintertüren in kommerzielle Software eingebaut wurde. Wäre die Verwendung von non-Amerikanischer Software oder von Open-Source Produkten - wenn noch nicht der Fall - eine mögliche Alternative für Sie?

H.E.: Da haben wir sogar schon allerhand ausprobiert. Das Problem ist leider, dass wir in unserem Geschäftsbetrieb als Dienst-

leister einfach mit der Software arbeiten müssen wie unser Kunde. Das ist ja auch ein Kostenthema. Es gibt natürlich auch viele (günstige bzw. gratis) Alternativen zu z.B. Microsoft Office,

aber wenn ich dann mit den Kunden und Lieferanten nicht optimal Daten austauschen kann, dann ist es nicht möglich. Der Kunde gibt es nun mal vor.

I.: Hat Ihr Haus eine Versicherung zum Schutz gegen Spionage abgeschlossen (z.B. Cyber-, Vertrauensschaden-, Computermissbrauchs-versicherung)?

H.E.: Wir arbeiten ja grundsätzlich nicht mit unserem Know-how, sondern es ist das Know-how des Kunden das schützenswert ist. Und von dem her gehe ich davon aus, dass es über unsere Projekthaftpflichtversicherung abgedeckt ist. Da bin ich aber nicht der Experte. In unserem Bereich ist es einfach eine Vertrauensbasis in unserem Geschäft. Neue Kunden erhält man meist über Mundpropaganda, d.h. gute Referenzen. Demensprechend wählen wir nur jene Mitarbeiter aus, wo wir ein gutes Gefühl haben. Und damit sind wir auch sehr gut bisher gefahren und hatten wenige Probleme.

I.: Damit wären wir auch schon am Ende des Interviews. Vielen Dank!

12.3 Transcript 2

Name:	Frau H.
Position:	Leiterin Zentraler Informatikdienst (ZID)
Branche:	Bildungseinrichtung U. (Forschung und Lehre)
Datum:	09.12.2013 10:00 – 10:40

Interviewer: Vielen Dank, dass sie sich für das Interview Zeit genommen haben! Ich werde nun einige Fragen zu den drei verschiedenen Bereichen Risk-handling, Personal und Sicherung und Kontrolle der IT stellen. Fangen wir mit den Risiko-behandelten an. Gibt es eine Sicherheitsverantwortliche Instanz im Unternehmen? Wenn ja, ist diese organisatorisch mit der Geschäftsführung verbunden?

F.H.: Auf der Universitäts-Ebene wäre das das Rektorat, also die oberste Managementebene. Wir sprechen ja von Informationssicherheit?

I: Ja genau.

F.H.: Der ZID ist schlussendlich die Instanz, die in der Verantwortung ist. Ich berichte direkt an den Vizerektor für Finanzen, also direkt an die Geschäftsführung wenn man so will.

I: Ok. Also hat der Informationsschutz dementsprechend einen hohen Stellenwert?

F.H.: Also prinzipiell ist die Kommunikationsschiene durchaus gegeben. Die Kommunikation ist gut. Bei den Maßnahmen und Regelwerken jedenfalls besteht massives Verbesserungspotential.

I: Sie als Sicherheitsverantwortlicher sind ja der primäre Ansprechpartner und Koordinator bei Sicherheitsangelegenheiten. Können Sie Ihre Aufgaben im Detail erläutern?

F.H.: Ich bin erst relativ seit Kurzem ZID-Leiterin und wir haben schon einige Mängel und Schwachstellen entdeckt und haben jetzt sogar konkret ein Inter-Universitäres Projekt zu dem Thema IT-Security gestartet, wo wir sagen, dass mehrere Unis gemeinsam es besser schaffen diese ziemlich große Aufgabe zu meistern. Und da geht es prinzipiell einmal um die Etablierung - ohne jetzt in Einstimmung mit ISO 27001 -, und darum die Politik und Strategie und auch die Rollen zu definieren. Und das soll jetzt in den nächsten Monaten in Anlehnung an ISO 27002/2013 umgesetzt werden. Wobei jetzt die Intention der Bildungseinrichtung nicht ist sich ISO zertifizieren zu lassen, sondern um Best-Practice umzusetzen. Wo wir jetzt schon mehr haben ist auf der Ebene der Sicherheitsrichtlinien und Sicherheitsstan-

dards. Also typisch für eine Bildungseinrichtung wie die unsere.

I: Um Know-how Schutzmaßnahmen effektiv ergreifen zu können, bietet sich eine Risikoanalyse an. Sie hatten ja ISO 27001 angesprochen. Inwieweit wurde bei Ihnen eine Risikoanalyse und Bewertung durchgeführt?

F.H.: Das ist nicht flächendeckend passiert, sondern in gewissen Teilbereichen. Da wäre zum Beispiel der SAP Bereich, hiermit also Personal und Finanz. Da gibt es solche Analysen und auch daraus resultierende Konzepte, die auch jährlich vom Wirtschaftsprüfer überprüft werden. Wir haben auch ähnliche Risikoanalysen bei anderen strategisch wichtigen IT-Bereichen gemacht. Zum Beispiel gab es bei unserem Campus Informationssystem so eine Sicherheitsanalyse und im High-Performance Computing Umfeld haben wir das auch gemacht.

I: Welche Bereiche wiesen die größten Risiken auf und wurden diese in irgendeiner Form klassifiziert?

F.H.: Unterschiedlich. In dem SAP Bereich jedenfalls der Datenschutz und die Informationssicherheit. Klarerweise gibt es da viele personenbezogene Daten; da geht es auch um Gehälter die ausgezahlt werden. Bei anderen Themen hatten wir das Problem bezüglich des Know-How, also dem Risiko bei Personen die Wissensträger sind, adressiert.

I: Wurden von Ihnen auf Basis der Analyse und Bewertung Prioritätenlisten zu Sicherheitsmaßnahmen entwickelt? Welche Maßnahmen zum Know-how Schutz konnten davon abgeleitet werden?

F.H.: Das war die Idee, aber ich glaube nicht, dass das so durchexerziert worden ist. Also das haben wir nicht in der ganzen Breite so wie es sich gehört bis Dato gemacht. Das soll in Zukunft auch wesentlich strukturierter ablaufen.

I: Inwieweit werden Unternehmenskooperationen als Risiko angesehen, insbesondere der Austausch von Zugangsdaten oder sensibler Informationen?

F.H.: Wir im ZID sehen das schon problematisch. Wo gibt es schon Konsequenzen. Die Bildungseinrichtung hat ja eine Tochterholding, die einen Mantel über verschiedene Sub-Firmen bzw. Spin-Offs bildet. Dort gibt es immer mehr eine Trennung der IT-Systeme, insbesondere der Verrechnungssysteme, Zeitschreibungssysteme und ähnlicher Dinge. Also da wurde das auch schon durchexerziert, um einerseits diesen Bereichen Schutz vor der eher sehr freikonfigurierten Wissenschaftsdomäne zu geben. Aber eben weil dort auch mehr externe Personen tätig sind. Unsere Bildungseinrichtung ist auch jene mit sehr vielen Wirtschaftsko-

operationen. Da gibt es schon Schutzbedarf, ganz klar. Weil Ergebnisse, die aus Tätigkeiten resultieren in so einem Projekt schützenswert sind. Passiert aber momentan nicht strukturiert meines Wissens nach, sondern ad-hoc.

I: Können Sie denn etwas zu Häufigkeit, Umfang oder Systematik von Cyber-Angriffen auf Ihr Unternehmen sagen?

F.H.: Also meine Analyse ist, dass die Mehrzahl der Angriffe das Ziel haben Ressourcen in den Griff zu bekommen. Also wir haben auch hier zurzeit die aus der Literatur bekannten Bitcoin und Primecoin-Hacks, und vor einigen Jahren noch mehr. Und da geht es darum einmal sich in diesem Top-Netzwerk sich etablieren zu können, weil man von dort aus sehr gute Zugriffsmöglichkeiten hat. (. . .) Anders als bei Firmen, wo es um Firmengeheimnisse oder Industriespionage geht, verfügt eine solche Bildungseinrichtung natürlich über große Ressourcen, „die eine gewisse Angriffsfläche bieten". Aber wir haben natürlich immer wieder auch die Probleme von Social Engineering oder von Internen, die aus verschiedenen Gründen Cybercrime begehen, weil sie frustriert sind, sich rächen wollen, oder irgendjemandem was Böses wollen. Das ist so. Gott sei Dank nicht sehr oft der Fall, aber passiert auch.

I: Gibt es (oder gab es) allgemein eine Zusammenarbeit mit Sicherheitsbehörden (Polizeilich o. Nachrichtendienstlich)? Wenn ja, in welcher Form?

F.H.: Also nach meinem Wissensstand haben wir nur in Anlassfällen klarerweise Kontakt mit der Polizei, dem Kriminalamt oder ähnlichen Organisationsformen, die bei Cyber-Angriffen zur Verfügung stehen.

I: Was halten Sie von der Meldepflicht für Cyber-Angriffe? Betreffende Parameter für Unternehmen sind finanzielle Risiken und (die nicht quantifizierbare Größe) imageschädigende Risiken.

F.H.: Wir sind eine Organisation, die mit öffentlichen Mitteln finanziert wird, und daher ohnedies nach meinem Wissensstand verpflichtet Anzuzeigen, wenn so etwas passiert.

I: Kommen wir nun zum Bereich Personal.
Inwieweit wird bei Ihnen eine Schulung / Sensibilisierung zur Förderung des Risikobewusstseins der Mitarbeiter bzgl. Umgang mit Informationen (insb. Email und Cloud, Chat / Skype) und Beachtung der Security-Policies durchgeführt?

F.H.: Beginnen wir bei der Vertragssituation. Unsere Mitarbeiter haben in ihrem Dienstvertrag gewisse Pflichten wie die Verschwiegenheitspflicht. Ganz klar ist, dass damit einmal eine Basis gesetzt ist. Des Weiteren haben wir, und das ist sicher

noch ausbaubar, natürlich im Rahmen auch der Erklärung, der hausinternen normativen Dokumente, eine Weiterbildung unserer Mitarbeiter(-innen). Wir haben natürlich auch im ZID Spezialisten, die sich schon vom Berufszweig sehr mit diesen Dingen beschäftigen, also insbesondere im Netzwerkbereich, aber auch in anderen Bereichen die betreut werden. Wir haben auch einige, die das mehr als Hobby machen oder als zusätzliche Aufgabe. Also gerade im ZID wird diese Kultur sehr gepflegt, und somit ist ein sehr hohes Bewusstsein dafür da, bei allen Beteiligten.

I: Und Sie hatten ja Social Engineering auch angesprochen. Wird auch dahingehend die „awareness" gefördert?

F.H.: Das ist im ZID auch schon sehr bekannt und präsent. Das Problem ist zumindest, dass das ZID von der Personenanzahl eine kleine Gruppe ist. Klarerweise und was wir jetzt auch in diesem Interuniversitärem Projekt ansprechen wollen ist, dass wir da gemeinsam awareness Maßnahmen entwickeln, bis hin zu „e-learning" oder Videos. Weil typischerweise diese Security Projekte genau dann dort aufhören, wenn man diese fachlichen Dinge erledigt hat und das an den Mann oder die Frau bringen will, ist das dann schon zu viel und passiert dann oft nicht, oder nicht regelmäßig. Also das glaube ich wäre der nächste Schritt, dass wir die ganzen Kollegen und Kolleginnen in der Verwaltung oder in den Instituten besser informieren und sensibilisieren. Diese Thematik ist auf jeden Fall ausbaufähig.

I: Inwieweit werden denn Mitarbeiter auch für die Gefahren von Geschäftsreisen sensibilisiert?

F.H.: Die Kollegen kennen das, aber es ist jetzt kein Thema, da wir auch nicht wirklich viele Geschäftsreisen machen.

I: Haben Sie formal fixierte Sicherheitsstandards wie Clean Desk Policy oder Bestimmungen zur Nutzung / Vernichtung von Informationsbeständen?

F.H.: Wir haben da relativ wenig zurzeit. Eine Clean Desk Policy haben wir definitiv nicht. Und der ganze Life-Cycle von Daten ist auch nur auf Bereiche und auch aufs Logging als bereichsübergreifende Datensammlung beschränkt.

I: Findet im Rahmen des Personalauswahlverfahrens eine intensive Überprüfung der Bewerber statt (insbesondere im Bereich der IT)?

F.H.: Keine intensive.

I: Wie wird bei Kündigung/Weggang eines Mitarbeiters verfahren?

F.H.: Das passiert für den zentralen Bereich. Es wird in den dezentralen Bereichen unterschiedlich gehandhabt. Keine unternehmensweit einheitliche Regelung. In solchen Fällen wird natür-

lich mit sofortiger Wirkung in unserer Zentraldatenbank sicher-

gestellt, dass sämtliche Zugänge für den Mitarbeiter deaktiviert bzw. gelöscht werden.

I: Ich würde jetzt zu den technischen Sicherheitsmaßnahmen übergehen.
Inwiefern wird auf das Risiko gefährdeter Datenträger (USB-drive, HDD) geachtet und spielt die Verschlüsselung von Datenträgern und Datenverkehr (insb. e-mail) bei Ihnen eine Rolle?

F.H.: Ja, also auch da noch nicht sehr reif. Es wird den Mitarbeitern delegiert gewissermaßen, dass sie clever genug sind. Also da gibt es keine verbindlichen Regelungen. Leider.

I: Also auch hier besteht Verbesserungspotential?

F.H.: Absolut. Diese Prozesse bzw. Regelwerke sind noch in den Kinderschuhen.

I: Wie sieht es mit der Verschlüsselung aus?

F.H.: Ich persönlich bin sehr dafür. Ich mache das seit vielen Jahren mit PGP und S/MIME und es ist mühselig. Das ist das Problem, aber es macht schon Sinn. Wir werden es auch in diesem Projekt durchaus in den Richtlinien thematisieren. Aber das wird eine Soll-Bestimmung sein oder eine Empfehlung. Keine Verpflichtung. (...) Verschlüsselung funktioniert gut vor allem in kleineren (Projekt- o. Special-Interest-) Gruppen, um damit sensible Daten auszutauschen, und um nicht persönlich vorbei kommen zu müssen und die CD mit den Daten zu übergeben. Aber der Einsatz von Verschlüsselung skaliert zurzeit einfach nicht. So für Projektteams ist das durchaus geeignet.

I: Wie sehen die (auch räumlichen) Zutritts- und Zugriffsberechtigungskonzepte (insb. Zugang zum Rechenzentrum) für sowohl firmeneigenes als auch firmenfremdes Personal bzgl. gefährdeten Daten und Objekten aus?

F.H.: Also wir haben natürlich einen strikt eingeschränkten Zutritt zu unseren Systemräumen. Die sind auch im Sinne der Verfügbarkeit redundant ausgelegt. D.h. wir haben redundante Rechenzentren. (...) Im Prinzip gibt es 3 Zonen die wir haben. Wir haben zum einen unseren ZID Bereich, wo alle ZID Mitarbeiter reinkommen. (...) Und dort gibt es noch Sicherheitsmaßnahmen in Form von verschließbaren Schränken. Und wir haben einen „Serverhouse" im Bereich, wo typischerweise Institutsrechner abgestellt werden, und benannte und bekannte Institutsmitarbeiter Zutritt bekommen. Der ist aber physisch getrennt von den zentralen Installationen.

I: Wie sieht es bei Reinigungskräften und Sicherheitsdienst mit

den Zugangsbeschränkungen aus?

F.H.: (. . .) Reinigungskräfte kommen nur in Begleitung rein. Aber es gibt auch das „facility management". Diese haben auch Zutritt klarerweise, und die tun es einfach. Das wird auch nicht weiter protokolliert zurzeit.

I: Wie oft gibt es einen systematischen Passwortwechsel und gibt es diesbezüglich Regelungen (z.B. minimale Anzahl an Stellen)?

F.H.: Es gibt da unterschiedliche Regelungen, und so etwas gibt es eigentlich nur in den hoch-sensiblen Bereichen. Das was man sich so darunter vorstellt, also alle 90 Tage zum Beispiel. Im SAP Bereich wird das gerade implementiert für die user. Und ansonsten gibt es nur Empfehlungen.

I: Wie sieht es mit Passwortschutz auf Rechnern und Laptops aus?

F.H.: Da muss man wieder relativieren. Der ZID betreibt hier, bei anderen Bildungseinrichtungen macht man das ganz anders, eine ganz kleine Anzahl von Rechnern, nämlich Arbeitsplätzen. Das ist typischerweise in der Verantwortung der Institute. Und auf den Rechnern, die wir servisieren gibt es zwar die Grundeinstellung, aber die Benutzer haben Admin-Rechte. Diese können also im Endeffekt das wieder ändern. Es gibt keine Form von Device-management wo solche policies erzwungen werden.

I: Inwieweit verfügen Sie über Schutzmechanismen wie Firewall, Anti-Virus und Anti-Spam Software? Findet bei Ihnen ein Intrusion Detection System Verwendung?

F.H.: Das ist sicher eine unserer Stärken. Da wir schon sehr sehr lange ein gutes Netzwerk haben, welches auch mal Ziel von Attacken war. Also da haben wir schon ausgeklügelte, teilweise schon 20 Jahre lang existierende Schutzmechanismen für den Netzwerkperimeter, insbesondere Firewall. Wir haben ziemlich komplexe Konstrukte zum Erkennen von Spam Mail. Wir haben punktuell zum Schutz unseres Campus Informationssystems z.B. auch ein Intrusion Detection System. Wie viel das hilft, ist bei uns umstritten. Es ist eine sehr komplexe pattern. Und momentan ist das nur ein Detection System und kein Protection System. D.h. wir beobachten, aber schalten nichts aus. Und Virenscanner, ja. Bei der zentralen Email-Infrastruktur gibt es das auch und es hilft auch.

I: Also glauben Sie, gerade in diesem Bereich technischer Schutzmaßnahmen sehr gut aufgestellt zu sein?

F.H.: In diesem Bereich sind wir sehr gut, ja.

I: Zu den Rechnern, die hier zu Bildungszwecken zur Verfügung gestellt werden: Können Sie dazu etwas sagen? Sind diese ebenfalls ausreichend geschützt?

F.H.: Ja, wir haben da ein hochsegmentiertes Netzwerk. Wo eben genau solche Segmente wie die Benutzerräume für die Studenten eigene Subnetze sind die geschützt sind. Die Studentenrechner die der ZID betreibt sind diskless. D.h. da gibt es sowieso nach jeder Session einen Reset. Wie gesagt, netzwerktechnisch ist dort schon das Optimum raus geholt. Noch einmal die Einschränkung: Es gibt noch mehr als den ZID in dieser Bildungseinrichtung, und somit mehrere Einheiten die solche Services anbieten.

I: Werden Ihre IT-Systeme regelmäßigen Updates unterzogen, wenn ja, wie oft?

F.H.: Die werden regelmäßigen Updates unterzogen, z.B. nach ITIL. Allerdings sind wir noch nicht so weit, dass wir die Betriebsprozesse sauber abgebildet hätten, also insbesondere das change-management. Es funktioniert trotzdem gut, weil die Leute gut sind und engagiert sind, und nicht weil es dafür das Regelwerk gibt. Das ist auf in solchen Bildungseinrichtungen traditionell so, aber es wird nicht so bleiben. Also insbesondere diese Weiterentwicklung des IT-Betriebs kommt mit dem Betriebs- und Entwicklungsprozess.

I: Gibt es regelmäßige (un-)angekündigte Prüfungen auf Umsetzung und Effizienz der Schutzmaßnahmen (z.B. Penetrationstests durch interne Stellen oder externe Dienstleister), wenn ja, wie oft?

F.H.: Nein, nicht regelmäßig. Nur fallweise wird das intern gemacht.

I: Hatte jede Fakultät (netzwerktechnisch) per se Ihr eigenes „Hoheitsgebiet", das in sich geschlossen ist?

F.H.: Der ZID bietet allen die Netzwerk-Infrastruktur an. Und Institute und Forschungsgruppen sind frei darin, ob sie sich Firewalls, also einen gesicherten Perimeter schaffen wollen. Und der ZID bietet sogar Unterstützung dabei an.

I: Wie schätzen Sie bei Ihnen die Risiken des ungewollten Know-how-Abflusses mit der zunehmenden Verwendung mobiler (und leistungsstarker) Geräte wie Tablets und Smartphones ein?

F.H.: Es gibt keine Maßnahmen um diese Daten auf den mobilen Geräten zu schützen, außer, dass wir die Möglichkeit der Zugänge über VPN etablieren, also über sehr viele Weblösungen, wo man möglichst versucht zero footprint auf den mobilen Geräten zu gewährleisten. Also momentan nur Infrastrukturmaßnahmen, aber keinerlei darüber hinausgehende Kapselung von Daten oder ähnlichen Dingen.

I: Inwieweit finden externe Cloud-Lösungen (GoogleDrive, Dropbox usw.) bei Ihnen Verwendung? Haben Sie sich Gedanken gemacht eigene Cloud-Lösungen zu entwickeln?

F.H.: Da haben wir den Plan der own-cloud, welches langsam in den Regelbetrieb übergehen soll. Sozusagen als Dropbox Ersatz wenn man so will. Das ist also die erste Ausbaustufe und das ist ein ganz heißes Thema im ganzen akademischen Netzwerk. Weil, wir haben ja viel Mobilität auch bei Studierenden und die technische Expertise auch. Also werden diese Cloud-Services massiv verwendet. Und wir wollen für relevante Services in diesem akademischen Netzwerk Angebote schaffen. Als Bildungseinrichtung, aber auch mit anderen Bildungseinrichtungen in Kooperation.

I: Im Zuge der letzten Meldungen zu Abhörpraktiken wurde bekannt, dass angeblich Hintertüren in kommerzielle Software eingebaut wurde. Wäre die Verwendung von non-Amerikanischer Software oder von Open-Source Produkten - wenn noch nicht der Fall - eine mögliche Alternative für Sie?

F.H.: Also es gibt ja auch den Bundestrojaner in Deutschland. Es ist nicht nur die NSA, vor der man sich schützen muss. Wir haben grundsätzlich ja eine sehr lange Open Source Tradition. Es ist ein Thema und ich glaube wenn Sie 3 Leute hier nach einer Lösung fragen, dann werden Ihnen 2 eine Open Source Lösung vorschlagen. Wir können das und wir tun das. Und das ist auch aus mehreren Gründen sinnvoll, also nicht zuletzt auch aus dem Grund, dass die Community den Source kennt und allfällige Hintertüren hoffentlich schnell entdeckt. Ja, es ist eine Alternative.

I: Nun sind ja einige Botschaften anderer Länder in unmittelbarer Nähe. Wird das mittlerweile nach den letzten Meldungen zu Abhörpraktiken als neues Risikopotential angesehen?

F.H.: Nicht direkt. Ich glaube in unserer Community ist dieses Thema schon länger bekannt, was technisch möglich ist und was gemacht wird. Interessant ist, dass das jetzt konkret irgendwo nachzulesen ist. Mich hat das nicht besonders überrascht.

I: Hat Ihr Haus eine Versicherung zum Schutz gegen Spionage abgeschlossen (z.B. Cyber-, Vertrauensschaden-, Computermissbrauchsversicherung)?

F.H.: Ich wusste nicht, dass es so etwas gibt. Muss ich mir jetzt näher anschauen.

I: Nochmal bettreffend der letzten Meldungen zu Abhörpraktiken: Haben Sie sich da allgemein bei Ihnen im Unternehmen damit befasst? Gerade im Hinblick auf die Informationssicherheit.

F.H.: In so einem offenen Kontext, wie der nun mal bei unserer Bildungseinrichtung gegeben ist, schätze ich das Risiko von Social Engineering oder dem einfachen Reinsetzen von Personen, die direkt Daten abschöpfen viel Größer ein. Solche Bildungseinrich-

tungen haben grundsätzlich so wenig Geld, sodass wenn ich da an die Daten wollte, dann ich Leute dorthin setzen würde, wo ich sie haben will. Es ist aus meiner Sicht für solche Bildungseinrichtungen nicht so dringend notwendig das mit technischen Mitteln zu machen. Man sagt ja auch, dass das Social Engineering eine sehr effiziente Methode ist um an Informationen zu kommen. Aber das ist auch ein Bereich wo wir besser werden wollen. Hier geht es um awareness. Dass auch Wissenschaftler und Verwaltungsmitarbeiter ganz klar wissen, dass die Information ein Gut ist, das schützenswert ist. In diesem Sinne hilft die Diskussion seit dem letzten Sommer massiv.

I: Damit wären wir am Ende des Interviews. Herzlichen Dank!

12.4 Transcript 3

Name:	Herr H.
Position:	Information Security Manager
Branche:	Energie- und Automationstechnik
Datum:	10.12.2013 09:00 – 10:00

Interviewer: Vielen Dank, dass sie sich für das Interview Zeit genommen haben! Ich werde nun einige Fragen zu den drei verschiedenen Bereichen Risk-handling, Personal und Sicherung und Kontrolle der IT stellen. Fangen wir mit den Risiko-behandelten Fragen an.
Gibt es eine Sicherheitsverantwortliche Instanz im Unternehmen? Wenn ja, ist diese organisatorisch mit der Geschäftsführung verbunden?

H.H.: Es gibt einmal eine Sicherheitsverantwortliche Instanz, einen IT-Security Manager im Konzern, also für die ganze Unternehmensgruppe. Und es gibt einen IT-Security Manager - Verantwortlichen jeweils in jedem Land. Und es gibt auch rundherum im Prinzip ein Security Team im weitesten Sinn. Also es gibt einmal den Manager und auch Mitarbeiter in den entsprechenden Bereichen, die sich um Informationssicherheit kümmern. Man muss aber auch unterscheiden zwischen Informationssicherheit, d.h. sich um die Security des eigenen Unternehmens kümmern, sich zu schützen gegen externe Bedrohungen, gegen Internetbedrohung, gegen Bedrohung jeglicher Art und zwischen dem was man unter dem Begriff Cyber Security versteht. Das wird bei uns etwas getrennt behandelt, (. . .) auch wenn die beiden Bereiche zusammen arbeiten. Aber Cyber Security betrifft eigentlich den Sektor, dass wir die Produkte in unseren Dienstleistungen, die wir für die Kunden erbringen, auch unsere Kunden dabei unterstützen diese sicher zu betreiben und auch die entsprechenden Rahmenbedingungen dafür zu schaffen. (. . .) Mein Aufgabenreich liegt in der IT Security im Unternehmen selber und nicht das Thema Cyber Security. (. . .)

I.: Und Sie kommunizieren direkt zur Geschäftsleitung?

H.H.: Im Prinzip von den Verantwortlichkeiten ist es so, dass die EDV dem CFO unterstellt ist und damit das Reporting dorthin erfolgt und das ist sicherlich ein Teil der Unternehmensleitung. Das ist im Konzern so, und bei uns lokal ebenso.

I.: Um Know-how Schutzmaßnahmen effektiv ergreifen zu können, bietet sich eine Risikoanalyse an. Inwieweit wurde bei Ihnen

eine Risikoanalyse und Bewertung durchgeführt (ggf. gemäß ISO 27001)?

H.H.: Also gemäß der ISO Norm haben wir es nicht zu 100%, d.h. wir sind nicht ISO 27001 zertifiziert. Das ist auch nicht unbedingt unser kurzfristiges Ziel. Wir haben eigentlich ein Prozessframework das auf der einen Seite aus der ITIL (Information Technology Infrastructure Library)Seite kommt und davon abgeleitet ist, und auf der anderen Seite haben wir als börsennotiertes Unternehmen, das mit Aktien an der US-Börse handeln möchte auch die Notwendigkeit für Sarbanes-Oxley. D.h. wir haben hier SOX taugliche Prozesse und Kontrollen. Wir werden von SOX auditiert. Das ist eigentlich unsere primäre Latte. Natürlich ist die Zielsetzung von SOX eine etwas andere und hat einen etwas anderen Schwerpunkt als die ISO 27001 und da entnehmen wir sicherlich Teile der ISO 27001-Anforderungen heraus, um das zu ergänzen. Also wir haben jetzt bei unserer Gestaltung der Prozesse nicht nur die reinen SOX Anforderungen abgedeckt, sondern auch Teile der ISO 27001. ITIL spielt wie gesagt mit und es spielt die ISO 9000 mit. Wir sind nämlich ein ISO 9000 zertifiziertes Unternehmen und auch hier müssen wir, wenn wir auditiert werden, die entsprechenden Kontrollen erbringen und Definitionen für die Vorgaben leben. Und die Kunst mehr oder weniger ist, bei den ganzen verschiedenen Frameworks, die es am Markt gibt, einen Prozess zu haben den man lebt, den man auch auf den Boden bringt. Und auf der anderen Seite eben dann auch eine ISO 9000 zu haben, die gelebt wird und irgendwann vielleicht auch eine 27001 Zertifizierung zu haben.

I.: Und was ist mit der Risikoanalyse?

H.H.: Ja, die wird gemacht. Das beginnt natürlich mit einer Business Impact Analyse, die bei uns, bei den Division Managern und dem Vorstand passiert. Die ist gemacht worden und die wird auch zyklisch wiederholt und überarbeitet. Das steht uns dann auch nächstes Jahr wieder bevor.

I.: Bei der Risikobewertung, haben Sie da gewisse Parameter in Betracht gezogen wie Schadenshöhe und Eintrittswahrscheinlichkeit? Hatten Sie noch weitere Parameter mit einbezogen?

H.H.: Das wird schon bewertet, was als riskant oder wahrscheinlich gesehen wird. Unterm Strich kommt dann einfach ein Maßnahmenkatalog heraus, welche Maßnahmen man setzt um diesen Risiken entgegenzuwirken. Welche Fälle man betrachtet; Man kann glaube ich nie alle Fälle vorhersehen und ist auch wieder eine Kosten-Nutzenrechnung bei diesen ganzen Sachen dabei. (. . .) Aber die massiven Szenarien sind entsprechend abgedeckt.

I.: Sie hatten den Maßnahmenkatalog angesprochen, das wird dann dementsprechend klassifiziert, dass man zwischen low-risk und high-risk unterscheidet?

H.H.: Ja, wobei da ja noch hinzu kommt, dass wir hier nicht bei 0 anfangen, sondern das leben wir schon seit vielen Jahren, d.h. man geht eigentlich von einer Situation aus, in der bereits Maßnahmen getroffen wurden. In dem es bereits Designkonzepte gibt, die Fail-over und Redundanz beinhalten. Und daher gegen gewisse Ausfälle ich schon gewappnet bin, bis zu einem gewissen Grad natürlich. D.h. es geht vor allem, wenn man den refresh macht, schaut man sich an, was sich alles an den Anforderungen oder an der Landschaft verändert hat und wo muss ich bereits bei den gesetzten Maßnahmen nochmal nachjustieren.

I.: Können Sie etwas konkreter auf die Maßnahmen eingehen?

H.H.: Die Maßnahmen liegen im redundanten Design, die Maßnahmen, dass Information entsprechend nicht nur in einem Punkt lokal ist, sondern sichergestellt ist, dass man keine Daten verliert. Und geht hin bis hin zu Desaster-Szenarien, dass dieser Standort nicht mehr existiert. D.h. es gibt Vorkehrungen für einen Ausfall des Rechenzentrums, wo binnen 48 Stunden die wichtigsten Dienstleistungen wiederhergestellt werden.

I.: Sie hatten ITIL angesprochen. Was genau kann man sich darunter vorstellen?

H.H.: ITIL ist ein Framework für die Prozessgestaltung im Service Bereich für IT Services.

I.: Inwieweit werden Unternehmenskooperationen als Risiko angesehen, insbesondere der Austausch von Zugangsdaten oder sensibler Informationen?

H.H.: Es ist natürlich die Frage was man mit den Third Parties macht und wie die Kommunikation konkret ausschaut. Es gibt eine klar definierte External Connectivity Guideline. Eine Konzernvorgabe, wie im Fall mit Kommunikation in Verbindung zu Dritten umzugehen ist. Und d.h. da gibt es ein Regelwerk oder Empfehlungen und die werden dann einfach lokal umgesetzt. Heißt einfach, dass kein externer in das Firmennetzwerk kommt und solche Dinge und welche Notwendigkeiten und Vorbedingungen es sind, um direkten Datenaustausch mit Dritten durchzuführen. Das betrifft dann klassisch das Internet, VPN Verbindungen usw. Aber wir haben auch Standleitungen zu Partnern, die wirklich dediziert nur für bestimmte Zwecke gehören (...). Da gehört auch wie gesagt nicht nur die technische Umsetzung dazu, sondern auch die Security Voraussetzung des Partners. D.h. welche Voraussetzung hat er, was kann ich von ihm annehmen, wie kann ich das

kontrollieren, wozu commitet er sich. Da gibt es auch bei der Herstellung der Verbindung vertragliche Aspekte, die berücksichtigt werden müssen. D.h., dass sichergestellt wird, dass der Partner Sicherheitsmaßnahmen wie aktuellen Virenschutz bei sich auch umsetzt. Dass ich mal zumindest davon überzeugt bin, dass mein Partner einen gewissen Mindeststandard an Security auch bei sich aktiv umsetzt.

I.: Können Sie denn etwas zu Häufigkeit, Umfang oder Systematik von Cyber-Angriffen auf Ihr Unternehmen sagen?

H.H.: Wenig. Allzu viel kann ich natürlich nicht dazu sagen. Ich kann nur sagen, ja es gibt sie. Es gibt sie vor allem im Konzern (weltweit). Es ist eigentlich so, dass man immer mit irgendwelchen solchen Dingen beschäftigt ist. Man darf auch nicht vergessen, dass wenn es Vorfälle gibt, auch wenn es nur sehr banale Vorfälle sind, ich gar keinen bekannten Effekt hat, dass irgendwas abhanden gekommen ist, also passiert ist. Nur man hat ja schon auf den ersten Stufen erwischt, ist eine forensische Analyse hintennach notwendig. Die kann einem Wochen oder Monate beschäftigen. Das ist auch sehr sehr aufwendig. Für Österreich kann ich sagen, dass wir Gott sei Dank noch keine groben Sachen, aber auch da sind Dinge wie Denial-of-Service ein Thema.

I.: Gibt es (oder gab es) allgemein eine Zusammenarbeit mit Sicherheitsbehörden (Polizeilich o. Nachrichtendienstlich)? Wenn ja, in welcher Form?

H.H.: Habe ich in Österreich nicht etabliert, nein.

I.: Was halten Sie von der Meldepflicht für Cyber-Angriffe?

H.H.: Im Prinzip ist das eine Sache, die mich bis jetzt noch nicht betroffen hat. Wenn es Inzidenz gibt, dann gibt es auch eine Eskalationspflicht, die ich habe an die entsprechenden Konzernstellen. Und es gibt ein Incident-Response Team, das sich um diese Dinge kümmert und wo diese Dinge behandelt werden. Einen Vorteil einer Meldepflicht für ganz Österreich, ist halt die Frage welche Behörde für uns wirklich da behilflich sein könnte. Meistens sind diese Dinge für uns auf globalem Level angesiedelt und da wird sicherlich auch Unterstützung gesucht, wenn es notwendig ist, aber sicherlich nicht bei einer Behörde in Österreich.

I.: Kommen wir nun zum Bereich Personal.
Inwieweit wird bei Ihnen eine Schulung / Sensibilisierung zur Förderung des Risikobewusstseins der Mitarbeiter bzgl. Umgang mit Informationen (insb. Email und Cloud, Chat / Skype) und Beachtung der Security-Policies durchgeführt?

H.H.: Natürlich gibt es die. Es gibt zum einen eine Security Schu-

lung und ein Security Awareness Training. Das ist verpflichtend für jeden Mitarbeiter, der bei uns neu beginnt. Das gehört zum Einstiegsprogramm, dass er das Training zu absolvieren hat. Es gibt differenzierte Trainings, also typischerweise gibt es das für jeden Mitarbeiter Endbenutzer. Es gibt aber auch zusätzlich noch spezielle Trainings für Leihmanager, die Führungsverantwortung haben. Und darüber hinaus noch spezielle Trainings für Mitarbeiter im IS Bereich, die noch einmal ein erweitertes Training bekommen. Diese Trainings sind interaktive e-learnings mit abschließendem Fragebogen, den man zu einem gewissen Prozentsatz zumindest bestehen muss. (...) Es gibt die Security Policy, es gibt verschiedene andere Policies im Haus, die einzelne Securityrelevante Themen abdecken. Es gibt eine Software-Asset-Management Policy. Bei uns ist es also so, dass es einen Applikationsstandort gibt, also ein Set von genehmigten, freigegebenen Anwendungen, die das Business für ihre Arbeit benötigt. Und darüber hinaus ist auf einem Client keine andere Software gestartet. Wenn es einen Bedarf gibt, dann gibt es einen Standardisierungsprozess, der einzuhalten ist und das wird erweitert und es ist ok. Aber irgendwelche Programme, die sich jedermann von irgendwo runterladen und installieren kann, das ist das Thema, dass wir das versuchen einzudämmen und zu unterbinden, weil man weiß ja nie, was dabei alles mitkommt. Speziell Skype ist ein Thema, das bei uns im Konzern nach wie vor noch untersagt ist.

I.: Wird dabei auch das Thema Social Engineering und die Gefahren von Geschäftsreisen angesprochen?

H.H.: Ja, auf jeden Fall.

I.: Bieten Sie auch VPN Möglichkeiten an?

H.H.: Ja, das haben wir auch.

I.: Haben Sie formal fixierte Sicherheitsstandards wie Clean Desk Policy oder Bestimmungen zur Nutzung / Vernichtung von Informationsbeständen?

H.H.: Es gibt keine echte Clean Disk Policy in diesem Sinn. Es gibt natürlich die Awareness, auch im Rahmen des Awareness-Trainings wird auf das Thema Clean Disk hingewiesen und, dass dort im Wesentlichen im Schulungsinhalt sehr wohl eben auch das Thema behandelt wird, also insbesondere Confidential Sachen usw. Dass solche Sachen entsprechend zu versperren sind. Das gilt auch für die Nutzung von Informationsbeständen und wie mit sensiblen Daten umzugehen ist.

I.: Findet im Rahmen des Personalauswahlverfahrens eine intensive Überprüfung der Bewerber statt (insbesondere im Bereich der IT)?

H.H.: Ja, ich denke schon, wobei das eher ein HR Thema ist. Daher kann ich das ihnen nicht genau beantworten, was dort genau gemacht wird. Es gibt den HR Bereich, einen Personalchef und ich weiß, dass da gewisse Maßnahmen getroffen werden, aber in welcher Form oder im Detail, darüber kann ich nichts sagen.

I.: Wurde eine Schutzbedarfsanalyse durchgeführt, die für alle regelt, welche Daten / Informationen geheim, vertraulich oder offen zugänglich sind?

H.H.: Hängt natürlich auch mit der Business Impact Analyse zusammen. Weil ich muss auch dort wissen, welche Daten sind für die Erbringung der Geschäftsprozesse wesentlich. Und welche sind besonders schützenswert. Dazu kommt eben noch, welche müssen da als vertraulich oder confidential oder strictly conf., oder welche Klassifizierung man da am Ende anwendet gelten. Und auf welchen Systemen sind sie dann gespeichert. Das gibt's im Prinzip ja. Nicht zum 100%igen Detaillierungsgrad, aber im Allgemeinen gibt's das.

I.: Ich würde jetzt zu den technischen Sicherheitsmaßnahmen übergehen.
Inwiefern wird auf das Risiko gefährdeter Datenträger (USB-drive, HDD) geachtet und spielt die Verschlüsselung von Datenträgern und Datenverkehr (insb. E-Mail) bei Ihnen eine Rolle?

H.H.: Natürlich spielt Verschlüsselung eine Rolle, vor allem dann, wenn man halt die services irgendwo im Internet verwendet. Dann ist der Datenaustausch und die Datenkommunikation über viele Plattformen auch verschlüsselt. Was jetzt die gefährdeten Datenträger angeht, das ist auch Thema des Security Awareness Trainings. Wir haben hier im Haus eine Reihe von Mitarbeitern. Die im Service tätig sind oder die Entwickler sind. Mit den Anforderungen von deren Business ist es einfach notwendig, dass ich USB drives oder externe Wechseldatenträger auch zulassen muss. Ich kann keinem Entwickler den USB port wegnehmen, und auch nicht die devices, (...) die zur Kommunikation genutzt werden. Das funktioniert bei uns einfach nicht diese Einschränkung zu machen, so wie das in anderen Branchen gemacht wird, wie z.B. bei den Banken, wo das ganze Usus ist. Das funktioniert also nicht, daher ist es ein Thema des Security Awareness Trainings, damit der Nutzer weiß, wie er damit umzugehen hat. Es gibt auch durchaus Möglichkeiten zur Verschlüsselung, die wir dem Nutzer geben können, also wenn die Notwendigkeit

besteht. Das ist ein Punkt, der auf meiner ToDo Liste steht. Wir haben noch keine durchgehende Verschlüsselung von Festplatten der Clients. Das hat viele verschiedene technische und praktische Prozessgründe. Daran arbeiten wir noch, eine Lösung zu etablieren. Aber im Prinzip wird es auch schon diese Richtung gehen. (. . .) Im Hinblick auf die Mail-Verschlüsselung, kann man bei unserem Mail-System den Marker „Confidential" setzen als Klassifizierung eines Mailinhaltes und das bedingt, dass der Mailinhalt verschlüsselt übertragen wird. Hat seine Einschränkungen, also wirklich gut funktioniert das nur innerhalb des Konzerns, wo das Mailsystem das Selbe ist. Und da wo ich auch die Verschlüsselung und Entschlüsselung die auf Zertifikaten entsprechend basiert, leicht handeln kann. Mit Third Parties haben wir da noch unsere Probleme und auch das ist ein Thema, an dem gearbeitet wird.

I.: Wie sehen die (auch räumlichen) Zutritts- und Zugriffsberechtigungskonzepte (insb. Zugang zum Rechenzentrum) für sowohl firmeneigenes als auch firmenfremdes Personal bzgl. gefährdeten Daten und Objekten aus?

H.H.: Es ist vollkommen klar, dass die Datenräume oder das Rechenzentrum, wo es eine klar definierte Liste von Personen gibt, die nur Zutritt haben. Es gibt einen Zutritt, der mit 2 Komponenten gesichert ist. Der auch elektronisch protokolliert wird. Und dieser Zutritt wird auch sowohl von den Berechtigten, als auch von den tatsächlich erfolgten Zutritten entsprechend monitored und ist auch eine Kontrolle von SOX. Also auch in diesem Zusammenhang ist es ein relativ relevantes Thema hier einen wirklich geschützten Zutritt zu haben. (. . .) Für firmenfremdes Personal in der Regel ist es so, dass die für irgendwelche Wartungsarbeiten nur in Begleitung mit einem zuständigen Mitarbeiter, der die Berechtigung hat, das Rechenzentrum betreten. Und sich dort aufhalten. Mit Ausnahme von Sonderfällen, es gibt einfach einen Dienstleister, der sich um das Environment des Rechenzentrums kümmert, was Energieversorgung, Belüftung, Löschanlage diese Dinge betrifft, da gibt es ein entsprechendes Agreement und Geheimhaltungsvereinbarungen, das die Leute unterschrieben haben, wie sie sich da drin zu verhalten haben. Das wird individuell geregelt. Aber im Allgemeinen, wenn jemand von einer externen Firma irgendwer kommt und was machen möchte, ist irgendwer als Aufsichtsperson dabei.

I.: Haben sie vielleicht sogar abhörsichere Räume?

H.H.: Nein, so geheim sind wir nicht.

I.: Wie oft gibt es einen systematischen Passwortwechsel und gibt

es diesbezüglich Regelungen (z.B. minimale Anzahl an Stellen)?

H.H.: Ja es gibt eine Passwortpolicy bei uns, die umzusetzen ist. Primär betrifft das eigentlich die active directory, wo das Passwort nach einiger Zeit abläuft und forciert wird dann neu zu setzen, wo es entsprechende Regeln für die Gestaltung des Passworts gibt, wie das aufgebaut sein muss, es gewisse Längenanforderungen gibt. Es gibt Beschränkungen, wann oder wie das Passwort geändert werden kann und es gibt auch da eine history liste, die sicherstellt, dass ich alte Passwörter nicht wiederverwende. Diese Regelungen sind hier umgesetzt und viele Applikationen in unserem Umfeld haben schon die Möglichkeit also mit active directory Accounts single sign-on in den jeweiligen Applikationen zu machen, sodass auch für viele Applikationen auch schon nur mehr ein Passwort gilt und dieses zu verwenden ist und auch unsere active directory ist so aufgesetzt, dass es auch weltweit funktioniert. D.h. wenn ich auf eine andere Niederlassung nach Amerika fliegt, oder sonstwohin kann ich mich von dort aus genauso anmelden, habe die gleichen Einstellungen und Möglichkeiten innerhalb des Firmennetzes.

I.: Inwieweit verfügen Sie über Schutzmechanismen wie Firewall, Anti-Virus und Anti-Spam Software? Findet bei Ihnen ein Intrusion Detection System Verwendung?

H.H.: Anti-Virus ist natürlich Pflicht, und zwar auf sämtlichen Systemen. Wird auch gemonitored, dass es aktuell ist. Mit verschiedenen Mechanismen auch wirklich überprüft wann dort welche Aktualisierungen drauf kommen und, dass man wenn da etwas an Updates schlagen sollte, dass man darauf kommt. Also aktueller Anti-Virus, aktuelles Patching, (. . .) das ist tägliches Geschäft. Firewall gibt's natürlich gegenüber Third Parties, Internet völlig klar. Entsprechende state-of-the-art Firewallsysteme, die uns einfach gegen Traffic von Außen schützen sollen. Anti-Spam gibt es auch. Entsprechend gute und Leistungsfähige Lösungen, die werden aber vom Konzern zentral realisiert und erbracht. Also sobald sie eine Mail bekommen oder schreiben, geht sie direkt den Konzern Anti-Spam Filter durch, wobei der Endbenutzer sehr wohl die Informationen bekommt, wenn jetzt etwas in die Quarantäne kommt, dass er es individuell prüfen kann und Feedback geben kann; Ja ist erwünscht / unerwünscht. Damit lernt auch dieser Filter wieder und dadurch, dass es die globale Ebene betrifft, haben wir eigentlich eine gute Qualität zurzeit. Intrusion Detection haben wir nicht in dieser Form laufend. Zumindest nicht in Österreich etabliert. Es gibt hier punktuelle Prüfungen, also Analysen oder Überwachungen,

die aber nicht laufend passieren, sondern nur zu einem bestimmten Zeitpunkt. Es gibt ein Security Programm, was jährlich neu definiert wird, welche Maßnahmen zu setzen sind im Security Bereich und so etwas gehört dort dazu. Aber wir haben kein laufendes Intrusion Detection System zu diesem Zeitpunkt.

I.: Sie hatten Prüfungen angesprochen. Gibt es regelmäßige (un-)angekündigte Prüfungen auf Umsetzung und Effizienz der Schutzmaßnahmen (z.B. Penetrationstests durch interne Stellen oder externe Dienstleister), wenn ja, wie oft?

H.H.: Ja, es gibt Vulnerability Scanner die im Einsatz sind, die einfach die Systeme prüfen zusätzlich zu den gesetzten Schutzmaßnahmen einfach nur noch mal prüfen, ob da noch vulnerabilities drauf sind und erkannt werden und dann entsprechend behandelt werden. Also da sind wir ganz in Ordnung aufgestellt würde ich mal sagen. Wie gesagt, sowas wie Netzwerkanalyse passiert nur punktuell, wo man sich einfach mal anschaut wie schaut mein momentaner Traffic aus. Den analysiert man, aber das ist eher eine einmalige Betrachtung, wo man genauer schaut ob es gewisse Auffälligkeiten gibt in einem gewissen Zeitintervall. Und ein nicht laufendes System.

I.: Wie schätzen Sie bei Ihnen die Risiken des ungewollten Know-how-Abflusses mit der zunehmenden Verwendung mobiler (und leistungsstarker) Geräte wie Tablets und Smartphones ein?

H.H.: Im Grunde genommen muss man sich weitgehend auf die Mitarbeiter verlassen können. Weil sobald ich ihm zulasse, dass er einen USB Stick anhängen kann (...), hat er schon einmal technische Möglichkeiten Daten mitzunehmen und wir sind einfach mobiler und nehmen immer mehr Information mit. Da ist die Technologie, ob das irgendwelche Smartphones oder Tablets noch sind eigentlich gegen vorsätzlichen Informationsabfluss unerheblich. Gegen die Gefahr durch unbeabsichtigten Informationsabfluss, weil ich das Gerät verliere o.ä., ist natürlich bei mobilen Anwendungen durchaus gegeben. Je kleiner die Geräte sind, desto höher die Risiken des Diebstahls. Das hatten wir ja schon bei den Notebooks so. (...) Es gibt natürlich wieder die Security Awareness Trainings, wo es gewisse Regelungen gibt, wie mit solchen Geräten man umzugehen hat (...). Der jeweilige einzelne Mitarbeiter aber immer wieder gibt es entsprechende Vorfälle, dass ein Gerät dann gestohlen wird. Was die Smartphones betrifft ist es so, dass wir entsprechende Managementsoftware haben. Das Gerät ist an und für sich per default gesperrt und im Verlustfall kann die ganze Information remote gelöscht werden. Die Tablets haben sich noch nicht verbreitet,

aber ich gehe davon aus, dass dort sich ähnliches einbürgern wird. Die werden sicher in ähnlicher Form zu behandeln sein. (. . .)

I.: Da Android Geräte primär anfällig für Cyber Attacken bzw. Datenmissbrauch sind, gibt es vielleicht bei Ihnen Regelungen, die bestimmte OS Versionen vorschreiben?

H.H.: Nein, gibt es nicht. Es gibt also bei uns einen Standard an Geräten, die man sich als Mitarbeiter, der jetzt sagt ich brauche ein Firmenmobile, wünschen kann. Das ist sowohl die iPhone Ebene als auch die Android Sachen, als auch Windows Phones. Es gibt also bei uns alle 3 Möglichkeiten, für jede dieser Plattformen, gibt es jeweils Hardware Empfehlungen und das kann man sich dann aussuchen. (. . .) Es ist aber so, dass das iOS auf der VPN Seite etwas securer eingeschätzt wird, und dass es da gewisse Vorbehalte gibt, dass das bei Android Geräten in Punkto VPN das nicht zulässig ist. Also da gibt es schon kleine Unterschiede unter den Plattformen.

I.: Inwieweit finden externe Cloud-Lösungen (GoogleDrive, Dropbox usw.) bei Ihnen Verwendung?

H.H.: Wir sind dabei im nächsten Jahr auf die Microsoft Cloud Lösung umzusteigen. Wir werden also Office 365 und SkyDrive verwenden und damit wird SkyDrive die empfohlene und möglicherweise einzig zulässige Plattform sein, die wir für unsere Mitarbeiter dann zur Verfügung stellen. Es gibt natürlich Ausnahmen oder Probleme dabei wenn ein Kunde kommt und sagt, ich habe meine Daten jetzt da auf dem GoogleDrive liegen oder auf dem Dropbox, dass man dann auf seine Daten drauf zugreift, aber wir werden es von uns aktiv nur eine Plattform geben. Und eine Plattform betreut werden, wo wir unsere Informationen zur Verfügung stellen für den Austausch von Daten, und das wird SkyDrive sein.

I.: Im Zuge der letzten Meldungen zu Abhörpraktiken wurde bekannt, dass angeblich Hintertüren in kommerzielle Software eingebaut wurde. Wäre die Verwendung von non-Amerikanischer Software oder von Open-Source Produkten - wenn noch nicht der Fall - eine mögliche Alternative für Sie?

H.H.: Es liegt nicht in unserer Macht dies zu entscheiden. Es ist ein Multinationales Unternehmen, bei dem ein Drittel der Mitarbeiter in Amerika hat, stellt sich diese Frage nicht. D.h. diese ganze Konzernsoftware, die wir hier einsetzen, ist es keine ernstzunehmende Alternative. Also nicht aus dem Hintergrund NSA usw, zumal wir hier in Österreich keine Forschungs- und Entwicklungsabteilung haben, wo ich sage da sind die Geheim-

nisse von übermorgen drinnen und das Know-How und was immer es woanders gibt. Dass wir da nicht im Fokus stehen, von Spionage und solchen Dingen. (. . .) Wobei man natürlich im Security Sinn sagen muss, das Eindringen in das Netzwerk macht man dort wo es am einfachsten ist. D.h. das schwächste Glied der ganzen Kette gibt die Festigkeit der Kette und d.h., dass wenn wir das Netzwerk des Konzerns schützen, dann ist es auch für uns das Thema.

I.: Hat Ihr Haus eine Versicherung zum Schutz gegen Spionage abgeschlossen (z.B. Cyber-, Vertrauensschaden-, Computermissbrauchsversicherung)?

H.H.: Soweit ich weiß nicht. In Österreich zumindest ist mir das nicht bekannt.

I.: Damit wären wir am Ende des Interviews. Herzlichen Dank!

12.5 Transcript 4

Name:	Herr S.
Position:	IT Security Officer
Branche:	Infrastrukturbetreiber
Datum:	10.12.2013 14:00 – 15:00

Notiz: *Der Interviewpartner war gegen eine Digital-Tonaufnahme des Interviews. Daher werden seine Antworten auf Basis der gemachten schriftlichen Notizen hier veröffentlicht. Der interviewte hielt sich mit den Informationen relativ bedeckt.*

Interviewer: Vielen Dank, dass sie sich für das Interview Zeit genommen haben! Ich werde nun einige Fragen zu den drei verschiedenen Bereichen Risk-handling, Personal und Sicherung und Kontrolle der IT stellen. Fangen wir mit den Risiko-behandelten Fragen an.
Gibt es eine Sicherheitsverantwortliche Instanz im Unternehmen? Wenn ja, ist diese organisatorisch mit der Geschäftsführung verbunden?

H.S.: Da muss man zuerst etwas differenzieren. Als Infrastrukturbetreiber sind wir zuerst einmal eine Holding und betreiben mehre-

re Unternehmen aus verschiedenen Branchen. Die Holding selbst besitzt natürlich eine Konzernleitung, der wir als Strategische IT direkt unterstellt sind und somit mit ihr auch verbunden sind. Es gibt aber auch einen eigenen IT Bereich, der alle Branchen, die Teil der Holding sind umfasst. Hinzu kommen einzel-

ne IT-Stellen, die an den einzelnen Sub-Unternehmen angegliedert sind. Dabei sind diese IT-Stellen primär jeweils für die IT-Sicherheit der Endgeräte und deren Applikationen zuständig. Wir im Bereich der Strategischen IT kommunizieren direkt mit der Konzernleitung, die gewisse Konzernrichtlinien (sog. Code of Conduct) vorgibt. Die Strategische IT kümmert sich darum, eine IT-Richtlinie zu formulieren, die unternehmensweit für Infrastruktur und alle Mitarbeiter zu befolgen ist.

I.: Um Know-how Schutzmaßnahmen effektiv ergreifen zu können, bietet sich eine Risikoanalyse an. Inwieweit wurde bei Ihnen eine Risikoanalyse und Bewertung durchgeführt (ggf. gemäß ISO 27001)?

H.S.: Ja, eine Risikoanalyse wird im Zuge des Corporate Risk Management durchgeführt. Davon ein Teil betrifft explizit den Bereich IT-Sicherheit. Wir sind ISAE (International Standards for

Assurance Engagements) 3402 zertifiziert. Dies ist ein Zertifikat aus Sicht der Wirtschaftsprüfer. ISAE 3402 hat den früheren Standard SAS 70 ersetzt. Im Grunde ist dieses Zertifikat im Vergleich zu ISO 27001 nicht so umfangreich, aber geht durchaus mehr in die Tiefe. Die Risikoanalyse kann man sich so vorstellen, dass wir eine Matrix haben, wo die Schadenshöhe der Eintrittswahrscheinlichkeit gegenüber steht. Dabei wird ein gewisser Zeitraum (z.B. 10 Jahre) betrachtet. Aus der berechneten Akzeptanzkurve leiten wir dann Maßnahmen ab. Die Risiken werden bei uns regelmäßig einmal im Jahr überarbeitet.

I.: Welche Bereiche wiesen die größten Risiken auf und wurden diese in irgendeiner Form klassifiziert?

H.S.: Die Daten werden durchaus klassifiziert und in der „oberen Policy" verwendet. Genauer kann ich auf die Bereiche zwecks Geheimhaltung nicht eingehen.

I.: Wurden von Ihnen auf Basis der Analyse und Bewertung Prioritätenlisten zu Sicherheitsmaßnahmen entwickelt? Welche Maßnahmen zum Know-how Schutz konnten davon abgeleitet werden?

H.S.: Zumindest wird aus der Risikoanalyse ein Maßnahmenkatalog abgearbeitet, eben nach der jeweiligen Klassifikation. Eine Maßnahme die zu nennen ist, ist z.B. die Verschlüsselung auf mobilen Geräten. Damit stehen auch Smartphones und Tablets, die bei uns im Fokus der IT-Sicherheit stehen.

I.: Inwieweit werden Unternehmenskooperationen als Risiko angesehen, insbesondere der Austausch von Zugangsdaten oder sensibler Informationen?

H.S.: Unternehmenskooperationen gibt es vor allem Im Verkehr, d.h. dort wo es um das Thema Mobilität geht. Es wird durchaus als gewisses Risiko angesehen, und zwar in organisatorischer Weise. Mitarbeiter von Kooperationspartnern müssen mit dem Diensteintritt eine Vertrauenserklärung unterschreiben, die eben jenen Austausch von sensibler Information schützt.

I.: Können Sie etwas zu Häufigkeit, Umfang oder Systematik von Cyber-Angriffen auf Ihr Unternehmen sagen?

H.S.: Cyber-Angriffe sind uns konkret keine bekannt. Der Fokus von solchen Angriffen richtet sich zumeist an die beiden Bereiche Vertraulichkeit oder Verfügbarkeit. Es gibt bei uns Vorgaben bei der IT-Security. So ist zum Beispiel das Datennetz vom Internet getrennt.

I.: Gibt es (oder gab es) allgemein eine Zusammenarbeit mit Sicherheitsbehörden (Polizeilich o. Nachrichtendienstlich)? Wenn ja, in welcher Form haben diese Sie unterstützt?

H.S.: Nein, es gibt keine.

I.: Was halten Sie von der Meldepflicht für Cyber-Angriffe?

H.S.: Das Thema sehe ich kritisch, weil die Gefahr besteht, dass jemand der Cyber-Angriffe meldet einen klaren Nachteil demgegenüber hat, der die ganze Zeit nichts preisgibt. Das sorgt dann natürlich für Imageschäden und dadurch längerfristig zu einem Verlust von Marktanteilen und zu finanziellen Schäden. Es müsste ein gleiches Maß für alle geben. Und zwar nicht nur innerhalb der jeweiligen Branchen, sondern international muss das über eine EU-Richtlinie vorgegeben werden.

I.: Inwieweit wird bei Ihnen eine Schulung / Sensibilisierung zur Förderung des Risikobewusstseins der Mitarbeiter bzgl. Umgang mit Informationen (insb. Email und Cloud, Chat / Skype) und Beachtung der Security-Policies durchgeführt?

H.S.: Es gibt bei uns auf jeden Fall eigene Schulungen zum Thema IT-Sicherheit. Dazu werden Mitarbeiter auch über das Intranet mit Informationen regelmäßig versorgt. Da sind dann Einträge zu den unterschiedlichen Themen. Social Engineering spielt bei den Schulungen natürlich auch eine wichtige Rolle.

I.: Inwieweit werden denn Mitarbeiter auch für die Gefahren von Geschäftsreisen sensibilisiert?

H.S.: Das Thema wird auch behandelt. Was die Laptops angeht, so bieten wir VPN Zugänge mit 2-Faktor Authentifizierung und Passwörtern mit AES Verschlüsselung.

I.: Haben Sie formal fixierte Sicherheitsstandards wie Clean Desk Policy oder Bestimmungen zur Nutzung / Vernichtung von Informationsbeständen?

H.S.: Wir haben Sicherheitsstandards, die in unseren Konzernrichtlinien gefordert werden. Was Clean Desk angeht, so haben wir lediglich Anweisungen, alles zu versperren, sobald der Arbeitsplatz verlassen wird. Das gilt insbesondere für die Zimmertür. Des Weiteren gibt es klare Anweisungen keine vertraulichen Dokumente auf dem Tisch zu lassen. Was die Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen angeht haben wir auch Richtlinien, an die sich der Mitarbeiter zu halten hat.

I.: Findet im Rahmen des Personalauswahlverfahrens eine intensive Überprüfung der Bewerber statt (insbesondere im Bereich der IT)?

H.S.: Es wird lediglich das Vorstrafenregister geprüft. Ansonsten gibt es keine weitere intensivere Prüfung.

I.: Wie wird bei Kündigung/Weggang eines Mitarbeiters verfahren?

H.S.: Bei Kündigung läuft der Prozess in allen Unternehmen unterschiedlich ab. Zum Austrittsdatum werden natürlich alle User

Accounts sofort gesperrt und alle Zugangsmöglichkeiten wie Karten eingefordert. Bei Entlassung wird entsprechend sofort verfahren. Bei einer geplanten Kündigung, wird der Mitarbeiter per Schreiben informiert, was er alles tun, also abgeben muss.

I.: Wurde eine Schutzbedarfsanalyse durchgeführt, die für alle regelt, welche Daten / Informationen geheim, vertraulich oder offen zugänglich sind?

H.S.: Ja.

I.: Ich würde jetzt zu den technischen Sicherheitsmaßnahmen übergehen.
Inwiefern wird auf das Risiko gefährdeter Datenträger (USB-drive, HDD) geachtet und spielt die Verschlüsselung (encryption) von Datenträgern und Datenverkehr (insb. e-mail) bei Ihnen eine Rolle?

H.S.: Wir haben keine expliziten Maßnahmen dazu durchgeführt, was das Risiko gefährdeter Datenträger angeht. Wir haben auch mal eine Kostenkalkulation durchgeführt, was das Ausbauen von CD Laufwerken bzw. USB ports aus Geräten wie Laptops gemacht. Herausgekommen ist, dass es teurer ist etwas mit ausgebauten Features zu bestellen, als diese mit Standard-Features zu erwerben. Wir suchen allerdings noch ein tool, dass man verschiedene Geräte per remote deaktivieren kann. Data-leakage prevention ist bei uns ebenfalls ein Thema. Was die E-Mail Verschlüsselung angeht, so machen wir das extern grundsätzlich nicht, sondern nur im hohen Management wird es angewandt. Bzgl. mobilen Datenträgern ist noch zu sagen, dass wir eine Applikation haben, die es uns erlaubt Daten spezifisch auf Wunsch zu verschlüsseln.

I.: Wie sehen die (auch räumlichen) Zutritts- und Zugriffsberechtigungskonzepte (insb. Zugang zum Rechenzentrum) für sowohl firmeneigenes als auch firmenfremdes Personal bzgl. gefährdeten Daten und Objekten aus? (auch: Reinigungskräfte + Sicherheitsdienst)

H.S.: Am Eingang gibt es Zutrittskontrollen in Form von Kartenlesegeräten. Besucher erhalten Karten, mit denen Sie Zugang erhalten. Der Eintritt wird protokolliert und geschieht für Besucher nur, wenn sie eine terminliche Vereinbarung mit einem Mitarbeiter haben. Der Zutritt zum Rechenzentrum ist streng gesichert. Ich nehme an, dass da niemand allein rein darf. Was Zutritt für Reinigungskräfte oder ähnliches Personal angeht, so haben diese ebenso besondere Vorschriften. Z.B. dürfen sie zugesperrte Räume nicht aufsperren und auch nur zu den Geschäftszeiten ihren Dienst verrichten.

I.: Gibt es vielleicht sogar auch abhörsichere Räume?
H.S.: Nein.
I.: Wie oft gibt es einen systematischen Passwortwechsel und gibt es diesbezüglich Regelungen (z.B. minimale Anzahl an Stellen)?
H.S.: Alle 84 Tage gibt es einen Passwortwechsel für den normalen domain-user. Dabei muss beachtet werden, dass das Passwort mindestens 8 Zeichen lang ist und aus 3 v. 4 Zeichensätzen besteht. Nach 10-facher Falscheingabe wird die Anmeldung für ca. 3 Stunden gesperrt. Ähnliche Regularien gibt es für jede Applikation.
I.: Inwieweit verfügen Sie über Schutzmechanismen wie Firewall, Anti-Virus und Anti-Spam Software? Findet bei Ihnen ein Intrusion Detection System Verwendung?
H.S.: Wir besitzen ein 3-stufiges Konzept. Auf der Firewall wird der Datenstrom aufgebrochen. Am Fileserver, respektive E-mails gibt es einen Scanner (Anti-Virus und Anti-Spam). Und am Endgerät gibt es auch eine Reihe unterschiedlicher Produkte. Ein Intrusion Detection System gibt es bei uns nicht.
I.: Also sehen Sie hier auf jeden Fall noch Verbesserungspotential?
H.S.: Ja, Verbesserungspotential ist sicherlich gegeben. Wobei gerade bei dem Datenstrom von innen nach außen, die größte Bedrohung ausgeht.
I.: Inwieweit achten Sie auf die Sicherheit von Smartphones? Unterscheiden Sie auch zwischen verschiedenen OS-Betreibern, auch im Hinblick darauf, dass Android im Vergleich relativ anfällig ist, was die Informationssicherheit angeht?
H.S.: Ja, tun wir. Wir differenzieren durchaus zwischen den verschiedenen OS. Wobei die grundlegende Frage immer noch ist: Wofür setze ich das Gerät ein? Wir setzen primär die Applikationen E-Mail, Kontakte und Kalender ein. Wir haben da eine eigene Lösung, nämlich eine Art Container, damit dienstliches von privatem trennbar ist. Damit kann ich Geräte spezifizieren. Auch Android wird dabei zukünftig zulässig sein, sodass eben dank des Containers keine wirkliche Risikobedrohung bestehen kann. Unser Standard war bis Dato die Nutzung von Windows Phones. Prinzipiell sind wir auch zufrieden damit, jedoch gibt es kaum Apps im Vergleich zu iOS oder Android.
I.: Werden Ihre IT-Systeme regelmäßigen Updates unterzogen, wenn ja, wie oft?
H.S.: Ja, wir nutzen WSUS (Windows Server Update Services), speziell für die Microsoft Updates. Dabei kann man sagen, dass wir relative strukturiert Patches aufspielen, bis hin zu sehr zeitnahen Installationen in kritischen Fällen.
I.: Gibt es regelmäßige (un-)angekündigte Prüfungen auf Umsetzung

und Effizienz der Schutzmaßnahmen (z.B. Penetrationstests durch interne Stellen oder externe Dienstleister), wenn ja, wie oft?

H.S.: Ja, die gibt es. Einmal im Jahr führt ein externer Dienstleister Prüfungen, inklusive Penetrationstests durch. Wir vertrauen da auf das 4-Augen Prinzip.

I.: Wie schätzen Sie bei Ihnen die Risiken des ungewollten Know-how-Abflusses mit der zunehmenden Verwendung mobiler (und leistungsstarker) Geräte wie Tablets und Smartphones ein?

H.S.: Die Gefahr ist definitiv größer. Der mobile Bereich ist vergleichbar mit dem Windows vor 10 Jahren.

I.: Eine große Gefahr geht von Malware aus. Aber auch davon, dass Daten immer und überall zugänglich sind.Inwieweit finden externe Cloud-Lösungen (GoogleDrive, Dropbox usw.) bei Ihnen Verwendung? Haben Sie sich Gedanken gemacht eigene Cloud-Lösungen zu entwickeln?

H.S.: Die Cloud Lösungen, die sie angesprochen haben werden nur dann verwendet, wenn es wirklich sein muss. Das Problem auch hier ist, dass es keine klaren gesetzlichen Vorgaben gibt. Und wenn es eine Anwendung ist, die keine Daten verwenden. Wir wollen möglichst bald eine eigene Cloud etablieren, d.h. die Idee von Clouds auch intern nutzen. Konkret bauen wir im Moment eine Dropbox-Alternative, die sicherstellt, dass die Daten dann bei uns liegen. Das ist auch ein großes rechtliches Problem. Wir wissen bei den externen Cloud-Lösungen nunmal nicht, wo die Daten liegen, daher ist es aus Sicherheitstechnischer Sicht natürlich keinesfalls eine valide Möglichkeit sensible Daten darauf zu speichern. Das ist auch ein Thema, das in der EU schon länger am Stocken ist.

I.: Im Zuge der letzten Meldungen zu Abhörpraktiken wurde bekannt, dass angeblich Hintertüren in kommerzielle Software eingebaut wurde. Wäre die Verwendung von non-Amerikanischer Software oder von Open-Source Produkten – wenn noch nicht der Fall – eine mögliche Alternative für Sie?

H.S.: Die Frage ist für welchen Bereich. Microsoft, insbesondere Windows sind zu etabliert, sodass die meisten Geschäftsprozesse nur darüber laufen. Im Serverbereich nutzen wir Linux. Ganz selektiv auch Open Source Produkte, vor allem in unserer Unternehmensweiten IT. Natürlich würden wir mehr Open Source Produkte nutzen, aber mangels Alternativen und der Gefahr, dass man keinen Support auf lange Sicht hat, ist das zurzeit nicht realisierbar.

I.: Hat Ihr Unternehmen eine Versicherung zum Schutz gegen Spionage abgeschlossen (z.B. Cyber-, Vertrauensschaden-, Computermiss-

248 brauchsversicherung)?
249 **H.S.:** Nein, nach meinem Wissensstand nicht.
250 **I.:** Nach den letzten Meldungen zu Abhörpraktiken (durch NSA etc.).
251 Haben Sie sich da allgemein bei Ihnen im Unternehmen damit be-
252 fasst? Gerade im Hinblick auf die Informationssicherheit.
253 **H.S.:** Natürlich wurde ich darauf häufig angesprochen, aber im All-
254 gemeinen war uns das schon länger bewusst, dass die Abhörprak-
255 tiken in Wahrheit ein viel größeres Ausmaß annehmen, als man es
256 wahrgenommen hat. Es liegt an der EU und anderen Institutio-
257 nen, gesetzliche Rahmenbedingungen zu schaffen, die dem Ganzen
258 etwas die Grenzen zeigen. Konkret in unserem Unternehmen aber,
259 ist das nicht so ein großes Thema, da alle Daten ausschließlich
260 intern lagern.
261 **I.:** Damit wären wir am Ende des Interviews. Herzlichen Dank!

12.6 Transcript 5

Name:	Herr R. und Herr C.
Position:	EDV-Leiter und Sicherheitsverantwortlicher
Branche:	Sicherheitstechnik
Datum:	12.12.2013 09:45 – 10:55

Interviewer: Vielen Dank, dass sie sich für das Interview Zeit genommen haben! Ich werde nun einige Fragen zu den drei verschiedenen Bereichen Risk-handling, Personal und Sicherung und Kontrolle der IT stellen. Fangen wir mit den Risiko-behandelten Fragen an.
Gibt es eine Sicherheitsverantwortliche Instanz im Unternehmen? Wenn ja, ist diese organisatorisch mit der Geschäftsführung verbunden?
H.C.: Ja, uns, also die EDV Abteilung. Wir heißen in Wirklichkeit Organisationsabteilung und die EDV ist ein Teil davon.
I.: Und Sie kommunizieren direkt zur Geschäftsleitung?
H.C.: Genau.
I.: Ok. Also hat der Informationsschutz dementsprechend einen hohen Stellenwert? D.h. geht die Geschäftsführung mit gutem Beispiel voran was die Informationssicherheit angeht?
H.R.: Aus Anwendersicht ja. Unser Generaldirektor, der damit gemeint sein könnte ist ein sehr 'braver' Endbenutzer eines EDV-Systems. Er installiert sich nichts selbst. Dafür geht er mit gutem Beispiel voran.
I.: Um Know-how Schutzmaßnahmen effektiv ergreifen zu können, bietet sich eine Risikoanalyse an. Inwieweit wurde bei Ihnen eine Risikoanalyse und Bewertung durchgeführt (ggf. gemäß ISO 27001)?
H.C.: Also die ISO 27001 haben wir bis jetzt noch nicht gemacht. Wir sind aber auch im Zuge des neuen Datenschutzgesetzes, wo es demnächst eine neue EU-Richtlinie geben wird auch in dem Bereich entsprechend sensibilisiert, weil der Datenschutzbeauftragte, so wie er in Deutschland existiert, sehr stark am Informationssicherheitsbeauftragten angelehnt ist, der dann aufgrund der ISO 27001 und ISO 27002, also mit diesen Regeln arbeitet. Diese Sachen gab es, ohne dass man die ISO explizit berücksichtigt hätte, von Haus aus in der Konzeption unserer EDV, weil auch der erste EDV-Leiter hier in der Firma entsprechend auch in dem Bereich beim früheren Konzern zum Teil tätig war. So, dass ein gewisser Sicherheitsstandard, der sich ungefähr an dieser ISO

anlehnt, implementiert war. Aber so eine richtige ISO Evaluierung und Zertifizierung gibt es in dem Bereich bei uns nicht.

I.: Und was ist mit der Risikoanalyse?

H.C.: Es gab entsprechende Analysen, aber nur punktuell, d.h. für gewisse Bereiche und nicht über die gesamte Firma. Da sind wir am überlegen, ob wir das nicht im Laufe des nächsten Jahres durchführen. Weil sich auch sehr viel an den individuellen Gegebenheiten geändert hat, d.h. es gibt verschiedenste Bereiche in der Firma, die dazu gekommen sind und gewisse Sachen haben sich umgeschichtet, d.h. die Situation entspricht nicht mehr der Ausgangssituation vor fast 20 Jahren, also nach dem Management-„buyout". Also d.h. jetzt sind die Risiken, aber auch die Chancen, die man hat, ganz andere. Und auch wenn Risiko da ist, ist der Impact ein anderer, als er vorher war, d.h. Risk-Assessment ist eine Sache, die man im Auge behalten muss. Und wir haben jetzt eine Zertifizierung für Datenschutzbeauftragte gemacht und da überlegen wir auch eine Zertifizierung für Informationssicherheitsbeauftragte zu machen.

I.: Sie hatten verschiedene Bereiche angesprochen. Können Sie auch sagen, welche Bereiche die größten Risiken aufwiesen und wurden diese in irgendeiner Form klassifiziert?

H.C.: Dadurch, dass wir auch gegenüber den Kunden in einem gewissen Bereich ein Sicherheitsunternehmen sind, d.h., dass wir Techniken für die Sicherung von Leib und Leben zur Verfügung stellen, haben wir einen gewissen Standard zu wahren gegenüber dem Kunden, damit wir nicht unglaubwürdig werden. Und in dem Zusammenhang haben wir natürlich alle diese Sicherheiten zu berücksichtigen. Also Sicherheiten, dass die Systeme, die wir haben nicht kompromittiert werden. Sicherheit, dass unsere Systeme niemandem Schaden verursachen. Die Sicherheit, dass wir selbst sicher sind vor Angriffen von außen (Arbeitsplatzsicherheit usw.). Also wenn wir über Sicherheit reden, dann gibt es unzählige unabhängige Faktoren, die den Begriff Sicherheit beinhalten und natürlich müssen wir uns in jedem von denen bewegen. Und einer davon ist natürlich, dass die Kunden die Sicherheit haben, dass unsere Gewerke für sie auch störungsfrei und gefährdungsfrei funktionieren.

I.: Bei der Risikobewertung, haben Sie da gewisse Parameter in Betracht gezogen wie Schadenshöhe und Eintrittswahrscheinlichkeit? Hatten Sie noch weitere Parameter mit einbezogen?

H.C.: Ja natürlich. Die Wiederherstellungszeit, und einige andere. Aber im Prinzip sind die Zentralpunkte vom Management aus natürlich Schadenshöhe, welches immer das erste ist was angesehen

wird. Die Reparaturzeiten sind auch etwas wichtiges, weil dann der Betrieb nicht störungsfrei funktioniert und wir sozusagen unseren Kunden gegenüber nicht den Service bieten können, der auch unserem Namen entspricht. D.h. wir würden unseren eigenen Ruf schädigen, wenn es längere Ausfälle geben würde. Das ist natürlich auch abhängig von den verschiedenen Gewerken die wir haben, verschiedene Applikationen, von denen jede natürlich einen unterschiedlichen Impact haben. D.h. es gibt da Bewertungen wie: Wie lange darf das oder jenes ausfallen. Welchen Schaden verursacht das der Firma. Und wie sicher muss das System gegenüber natürlichen Störungen (z.B. Stromausfall) sein. Wie sicher muss man es machen gegenüber Angriffen von außen. Auf solche Sachen muss man achten und schauen wie schnell man so etwas reparieren kann. Oder wie sicher muss man es machen überhaupt gegenüber einem Ausfall. Also muss es eine Hochverfügbarkeitsanwendung sein oder es reicht einfach die Reaktionszeit, bis es wieder funktioniert.

I.: Wurden von Ihnen auf Basis der Analyse und Bewertung Prioritätenlisten zu Sicherheitsmaßnahmen entwickelt?

H.C.: Prioritätslisten gab es prinzipiell schon. Sagen wir so, die gesamte Grundkonzeption der EDV-Landschaft war darauf ausgelegt, dass wenn es zu den klassischen Angriffen kommt, dass die möglichst einen geringen Impact haben. D.h., dass man Systeme nur kompromittieren kann, die low-risk haben, wo keine wichtigen Daten drin stehen oder wo die Ausfallszeiten relativ egal sind. Also sicherheitsrelevante Bereiche, wo es darum geht, dass es hochsensible Daten sind. Daten die einen gewissen Schutz bedürfen - aus Datenschutzrechtlicher Sicht, Daten drin sind die einen Markenschutz oder Technologieschutz bedürfen, weil es unser eigenes Know-How betrifft mit dem wir gegenüber anderen Mitbewerbern arbeiten. Diese Sachen sind meistens in abgesetzten Bereichen, die teilweise sogar getrennt sind, sodass diese von außen kaum erreichbar sind. Ganz andere Szenarien sind, also wenn man weggeht von der klassischen Angriffssituation, die ja normalerweise eigentlich sehr selten vorkommt, weil es dann wirklich die Institutionellen Angreifer sind, die das machen. Die klassische Spionage geht ja eher über den „Social" Aspekt, also Mitarbeiter, sodass irgendjemand sich anbiedert oder er schleust sich ein in eine facility management Firma, die da arbeitet und Zutritt zu verschiedenen Bereichen hat, wo nicht mal ein normaler Mitarbeiter Zutritt hat. Das macht dann eher die Wirtschaftsspionageangriffe aus, welche dann auch wesentlich schwieriger in den Griff zu bekommen sind.

I.: Bezüglich Know-How Schutz. Haben Sie auch Patente, die Ihr Know-How schützen?

H.R.: Das Patentprozedere ist meistens sehr mühsam.

H.C.: Insbesondere, weil ein Österreichisches Patent nichts bringt. Und ein Europäisches Patent ist zu teuer und langwierig. Wir sind hauptsächlich im Mitteltechnologiebereich unterwegs und da ändern sich die Gegebenheiten fast so schnell wie im Hochtechnologiebereich. Wenn man da ein Patentverfahren zu lange macht, dann ist meist das Produkt schon alt, wenn das Patent raus ist.

H.R.: Das einzige was wir haben ist ein Markenschutz am Namen.

H.C.: Die zweite Sache, die ich noch beim Patent sehe ist, dass man für eine Patentgewährung sehr viele Spezifikationen hergeben muss in Hände, von denen man nicht weiß ob sie auch sicher sind.

I.: Welche Maßnahmen zum Know-how Schutz konnten denn konkret von der Analyse und Bewertung abgeleitet werden?

H.C.: Teilweise. Wir haben verschiedene Maßnahmen getroffen. Durchaus noch nicht alle. Wir werden in absehbarer Zeit eine neue Bewertung machen müssen und reflektieren, ob die Maßnahmen greifen, die wir haben. Beispielsweise gibt's die Zutrittskontrolle zur Entwicklungsabteilung. Es ist EDV-technisch ein eigener Bereich. Natürlich wird auch angesehen inwieweit diese Sachen greifen. Letztendlich läuft es darauf hinaus, wie die Mitarbeiter damit dann umgehen, d.h. ob ein Mitarbeiter in einem geschützten Bereich jeden rein lässt oder nicht. Ob jemand, der Daten in einem geschützten Bereich hat und diese an irgendwen verschickt. Das liegt dann individuell an den Mitarbeitern, die man immer wieder sensibilisieren muss für diese Sachen.

I.: Inwieweit werden Unternehmenskooperationen als Risiko angesehen, insbesondere der Austausch von Zugangsdaten oder sensibler Informationen?

H.C.: Das ist sicher ein Problem. Es ist kaum ein Problem wenn irgendwelche Firmen von Extern direkt zu uns kommen. Da gibt es 2 oder 3 Partner, wo wir eigentlich die Mitarbeiter relativ genau kennen. D.h., dass der Support oder die Entwicklungsabteilung immer mit den gleichen Leuten zu tun hat. Es gibt einen Ansprechpartner den sie haben, und nur mit dem kommunizieren sie. Außerdem sind die meisten Kooperationspartner relativ kleine Firmen, sodass es auf 4-5 Leute hinausläuft die man auch kennt. Viel schwieriger ist die Situation innerhalb des Konzerns, weil wir Daten an Konzernschwestern abgeben müssen, die teilweise etwas produzieren oder weil wir im Kon-

zern das Kompetenzzentrum für diese Anlagen sind. D.h. die Daten werden zentral von uns an die Konzernschwestern verteilt und was dort passiert, da können wir nur vertrauen, dass sie genauso gutes Risk-Management haben, wie wir es auch haben. Dann sind die Daten außer Haus und nicht mehr unter unserer Kontrolle.

I.: Können Sie denn etwas zu Häufigkeit, Umfang oder Systematik von Cyber-Angriffen auf Ihr Unternehmen sagen?

H.C.: Es gibt Erfahrungen. Man kann sagen, dass es einen größeren Vorfall alle 3 Jahre gibt. Aber direkt, dass irgendjemand unsere Daten haben wollte, das ist auf die Art und Weise noch nie passiert. Es ist immer so gewesen, dass man unser System missbrauchen wollte für ganz andere Zwecke. Einmal gab es durch einen Fehler in der Testumgebung einen Einbruch in ein Testsystem, mit dem einer dann Bewertungen bei Google hochstufen wollte z.B. Bei einem anderen Fall war es – was nicht mehr passieren kann, weil es noch war, als wir mit ehemaligen von unserem ursprünglichen Konzernschwester ein gemeinsames Netzwerk gehabt haben – so, dass einige Maschinen an einer unserer Geschäftsstellen verseucht wurden und dann als Spambots verwendet wurden. Ist letztendlich weniger spionagebedeutend, da es kein gezielter Angriff gegen uns, sondern eher ein Missbrauch von Ressourcen war. Direkte Angriffe gegen uns passieren auf diese Art und Weise nicht. Da gibt es wesentlich einfachere Szenarien. Wie gesagt, die Angriffe auf die Infrastruktur machen höchstens institutionelle Angreifer. Die Konkurrenz macht das ganz anders. Die versucht Mitarbeiter abzuwerben. Das ist uns auch schon einmal passiert. Da gab es ein Gerichtsverfahren. Dann gab es Vorfälle, wo Leute die bei uns geschult wurden Anlagen zu errichten, dann aber auch bei Konkurrenten Anlagen errichtet haben und es so zu Daten-„leaks" gekommen ist. Das lässt sich leider auch nicht vermeiden. Da ist die Sensibilität der Schulenden gefragt. Wie weit bzw. in welche Schichten (z.b. nur der Anwenderschicht oder dem Kommunizieren d. technischen Unterbaus) sie den Leuten Einblicke gewähren. Das ist leider noch nicht wirklich beeinflussbar bzw. verhinderbar, da man den Leuten auch gewisse Einblicke in Technologien geben muss. Man muss nur sensibel sein, indem wie weit man es macht, damit der Mitbewerber möglichst nicht an sensible Daten kommt. Es gab auch einen dritten Vorfall in dem Bereich, der aber symptomatisch für Wirtschaftsspionage ist, nämlich Reverse Engi-

neering. D.h. ein Mitbewerber hat über einen Kunden von uns sich Anlagen besorgt. Und es gibt einen Mitbewerber der zum Teil davon lebt, dass er Reverse Engineering von unseren Anlagen macht. Weil er auch immer etwas Zeit braucht, und bis er die Technologie analysiert hat und nachmachen kann, ist er nur von geringer Bedeutung.

I.: Befindet sich dieser Mitbewerber im selben Land, also Österreich?

H.C.: Ja. Er ist aber ein kleiner Mitbewerber, der auch immer einige Jahre braucht, bis er die Prozesse nachgebaut hat und eine Nachverfolgung ist auch etwas schwierig, da es nicht leicht nachzuweisen ist, dass er es nachgebaut hat. Aber wir wissen, dass er es tut.

I.: Gibt es (oder gab es) allgemein eine Zusammenarbeit mit Sicherheitsbehörden (Polizeilich o. Nachrichtendienstlich)? Wenn ja, in welcher Form?

H.C.: Da es bis jetzt nichts Relevantes gegeben hat, außer eben bei der kleinen Firma, die Reverse Engineering betreibt. Das zahlt sich nicht wirklich aus, weil etwas zu wissen und etwas beweisen zu können zwei verschiedene Dinge sind.

H.R.: Es müssen ja zuerst beweisbare Tatsachen gegeben sein, damit überhaupt Polizeibehörden aktiv werden können. Man kann ja etwas behaupten, aber das läuft dann auf einen Zivilprozess hinaus. Die Fälle die uns betroffen haben waren einfach zu klein um so etwas zu rechtfertigen.

H.C.: Kosten-Nutzen Rechnung in dem Bereich heißt: Keine anderen Maßnahmen außer den internen Schutz zu erhöhen bzw. die Sensibilisierung der Mitarbeiter.

I.: Kommen wir nun zum Bereich Personal.
Inwieweit wird bei Ihnen eine Schulung / Sensibilisierung zur Förderung des Risikobewusstseins der Mitarbeiter bzgl. Umgang mit Informationen (insb. Email und Cloud, Chat / Skype) und Beachtung der Security-Policies durchgeführt?

H.C.: Es gibt einen Zeitpunkt wo Schulung dezidiert gemacht wird, und zwar mit jedem Mitarbeiter. Das ist bei der Einstellung. Da gibt's auch entsprechende Sicherheitsrichtlinien, die der Mitarbeiter unterschreibt, also z.B. Geheimhaltungsvereinbarungen.

H.R.: Es gibt auch eine 16-seitige IT-Richtlinie, die in der Einschulungsmappe des Mitarbeiters steht und die sein Vorgesetzter mit ihm auch durchgeht. Und wo er auch unterschreibt das verstanden und akzeptiert zu haben. Das ist relativ intensiv. Ansonsten gibt es Sensibilisierung bei Anlassfällen, wenn z.B.

ein neuer Virus im Umlauf ist, dann werden alle Mitarbeiter darüber informiert per E-Mail.

H.C.: Oder was wir auch im Zuge der neuen EU-Datenschutzrichtlinie machen werden sind periodische Workshops bzw. Schulungen, die in der Datenschutzrichtlinie vorgesehen sind, weil man sich nicht mehr darauf beziehen kann, dass der Mitarbeiter es mal gehört hat, weil er es auch mal vergisst. Solche Sachen haben eine relativ kurze Halbwärtszeit. Dann gibt es eine jährliche Schulung. Und wir sind auch dabei ein gewisses Internetportal zu erstellen, wo die Leute sich dann selbst informieren können. Es wird auf jeden Fall professionalisiert. Über das Portal wird es dann Auffrischungsseminare geben (ca. einstündig). (. . .) Chatprogramme wie Skype und auch Cloudsysteme sind bei uns grundsätzlich verboten. Aufgrund dessen, weil man Daten unkontrolliert an irgendwen verteilen kann. Dort besteht auf jeden Fall ein hoher Grad an Unsicherheit. Es gibt zwar Skype, aber nur auf speziellen Netbooks, die niemals an unser Firmennetzwerk angeschlossen werden. Die werden nur dazu genutzt um Kommunikation von Mitarbeitern, die im Ausland unterwegs sind, durchzuführen. D.h. Punkt-zu-Punkt Verbindung, isoliert von allen anderen Systemen.

I.: Inwieweit werden denn Mitarbeiter auch für die Gefahren von Geschäftsreisen sensibilisiert?

H.C.: Das ist zum Beispiel eine Sache, wo die Leute dann keine firmenrelevanten Daten auf ihren Geräten haben dürfen und, dass sie zur Kommunikation abgeschottete Systeme verwenden müssen. Z.B., wenn sie nochmal telefonieren wollen, dann über das Netbook mit Skype machen.

I.: Bieten Sie auch VPN Möglichkeiten an?

H.C.: Nein, das kommt nicht in Frage. Im Land gibt es derzeit 2 Leute, die technisch versiert sind und Zugang über VPN haben, aber ansonsten nein. Alle anderen Leute arbeiten innerhalb des Systems. Wir haben verschiedene Zweigstellen, die nur in unserem Netz sind und die

H.R.: Internetverbindung besteht dann auch nur über unsere Haupt-Firewall. Wir betreiben Österreichweit den Internetzugang nur über Wien. Wir haben Geschäftsstellenniederlassungen in anderen (. . .) Bundesländern und das Internet in diesen Geschäftsstellen geht auch über unsere Firewall. Und über die MPLS Leitungen.

I.: Haben Sie formal fixierte Sicherheitsstandards wie Clean Desk Policy oder Bestimmungen zur Nutzung / Vernichtung von Informationsbeständen?

H.C.: Bzgl. Bestimmungen, ja, die gibt's schon. Hauptsächlich bezogen auf Papier und Datenträger. Da arbeiten wir mit einem externen Dienstleister zusammen, der diese Sachen zertifiziert entsorgt. Die Leute dürfen keine Sachen in den Papierkorb werfen, die relevant sind. Dafür gibt es extra Container, die versperrt sind und wo man an die Daten nicht rankommt. Bzw. bei noch kritischeren Daten gibt es einen Reißwolf. Wir können leider nicht komplett eine Clean Desk Policy durchziehen, dadurch, dass wir auch im Projektgeschäft tätig sind. Da gibt es keine kurzfristigen Angelegenheiten, wo so etwas effektiv angewandt werden könnte. Die Mitarbeiter arbeiten tagelang gewisse Sachen aus und die Dinge liegen dann oft natürlich auf den Arbeitsplätzen. Wir sind daran interessiert, dass sie es in Container einsperren. In der Vertriebsabteilung gibt es eh meistens Ordner, die dann im Kasten eingesperrt sind. Aber wenn irgendwo in einer technischen Abteilung ein Problem ist und die teilweise die Bauteile da liegen haben, da könnte jemand, der sich technisch auskennt daraus Rückschlüsse ziehen. Ist eher dann wiederum das Problem, wie überwacht man eine Cleaning- / Facility Management Firma. Aus unserer Sicht liegen die Risiken wo anders, um an die Daten zu kommen.

I.: Findet im Rahmen des Personalauswahlverfahrens eine intensive Überprüfung der Bewerber statt (insbesondere im Bereich der IT)?

H.C.: Keine intensive. Natürlich gibt es gewisse Risiken und Probleme in anderen Ländern, in den wir vertreten sind, also z.B., dass Leute von lokalen Geschäftsstellenleitern engagiert werden und wir die möglicherweise nie zu Gesicht bekommen. D.h. wir müssen eigentlich unseren Geschäftsstellenleitern soweit vertrauen, dass sie nur Personen engagieren, die für sie vertrauenswürdig sind. Andererseits arbeiten wir in einem Bereich, wo es relativ wenig Mitbewerber gibt.

H.R.: Es ist eher ein Nischenmarkt, sodass wir teilweise auch vom Mitbewerber die Leute übernehmen und bei denen wissen wir natürlich, dass sie dort gearbeitet haben. Umgekehrt passiert das natürlich auch. (. . .)

I.: Wie wird bei Kündigung/Weggang eines Mitarbeiters verfahren?

H.C.: Kommt natürlich darauf an, auf welche Art und Weise der Mitarbeiter die Firma verlässt, also Kündigung oder Entlassung. Wenn es eine Entlassung ist, dann werden die Dinge schon gesperrt, bevor der betreffende Mitarbeiter aus der Firma ausscheidet. Bei Kündigung läuft es etwas anders. (. . .) Da arbeitet er bis zum letzten Tag und wenn er seine Sachen abgibt, dann wird das

dementsprechend gesperrt.

I.: Wurde eine Schutzbedarfsanalyse durchgeführt, die für alle regelt, welche Daten / Informationen geheim, vertraulich oder offen zugänglich sind?

H.C.: Kaum. Es gibt natürlich die Klassifizierung technischer Geheimnisse und datenschutzrechtlicher Bereiche (...). Das gilt dann entsprechend für die Bereiche Entwicklung, Support usw.

I.: Ich würde jetzt zu den technischen Sicherheitsmaßnahmen übergehen.
Inwiefern wird auf das Risiko gefährdeter Datenträger (USB-drive, HDD) geachtet und spielt die Verschlüsselung von Datenträgern und Datenverkehr (insb. E-mail) bei Ihnen eine Rolle?

H.C.: Teils, teils. Es ist so, dass Verschlüsselung bei E-Mail automatisch passiert mit dem Partner, der Verschlüsselung anbietet, also serverseitige. Das heißt die Kommunikation über das Internet wird verschlüsselt. Das ist Standard bei den Mail-Servern. Da braucht der einzelne Mitarbeiter gar nichts tun. Innerhalb des Konzerns wurde das explizit geprüft und eingerichtet, d.h. da ist die Kommunikation garantiert verschlüsselt. Mit anderen Firmen, soweit sie das unterstützen auch. Ansonsten eher nicht, weil wie gesagt, sobald man die Daten außer Haus gibt, dann kann sowieso niemand darauf pochen, dass die Daten nicht an Dritte kommen. Und die Überwachung von Internetleitungen, das können auch nur institutionelle Spionagedienste machen. Der Mitbewerber macht das anders. Die andere Sache sind die Datenträger. Wir haben eine Zeit lang damit herumexperimentiert. Letztlich ist herausgekommen, dass der Kosten-Nutzen Faktor nicht da ist (...). Wir müssen nur darauf achten, dass eben Daten nicht unkontrolliert auf irgendwelche mobilen Datenträger gelangen. Nicht sicherheitsrelevante Daten, damit haben wir kein Problem. Bei sicherheitsrelevanten Daten ist es so, dass die Mitarbeiter immer wieder sensibilisiert werden müssen das nicht zu tun. Ob man dann Datenträger verschlüsselt oder nicht, meistens ist es so, dass derjenige der den Datenträger verschlüsselt auch derjenige ist, der das Leck bei den Daten ist. D.h. er kann es auch entschlüsseln, wenn er denn will.

H.R.: Es gibt keine sicherheitsrelevanten Daten auf Datenträgern. Die Daten sind normal nur in der Entwicklungsabteilung, und nur ein ganz kleiner Personenkreis hat Zugriff auf diese, und auch nur in dem Bereich. Wir haben bis Dato den Bedarf nach diesen

Dingen nicht. Wir haben es ursprünglich bei den Technikern gemacht.

H.C.: Da haben wir TrueCrypt verwendet, aber das hat sich eher als mühsam herausgestellt, vor allem weil die Daten die da verschlüsselt wurden, nicht sicherheitsrelevant waren. (...) Und sonst hier in der Firma läuft alles über das Netzwerk, und da kursieren die Daten nicht auf Wechseldatenträgern.

I.: Wie sehen die (auch räumlichen) Zutritts- und Zugriffsberechtigungskonzepte (insb. Zugang zum Rechenzentrum) für sowohl firmeneigenes als auch firmenfremdes Personal bzgl. gefährdeten Daten und Objekten aus?

H.C.: Es gibt mehrere Sicherheitsbereiche, wo nur gewisse Personen Zutritt und Zugriff haben. (...) Da gibt es die Bereiche z. B. in den Demo-Räumen, wo nur Leute aus dem Support und dem Projekt-Management Zutritt haben. Weil dort gewisse Testumgebungen sind, die nicht so abgesichert sind, wie normale Systeme. Also nur wo man mit Begleitung Zutritt hat. Andere Bereiche, die Zutrittsberechtigungen haben, sind Entwicklung, der Support bzw. eigentlich das gesamte Gebäude. Bei allen Eingängen gibt es Zutrittskartenlaser, damit man feststellt, wer zu welcher Uhrzeit das Gebäude betreten hat. Und genauso werden eben auch spezielle Räume wie z.B. der Serverraum auch überprüft. D.h. man kann nur mit dem Chip oder mit der Karte sich Zugang verschaffen, und das wird protokolliert. Den Zugang zum Serverraum hat dabei ganz speziell nur ein ganz kleiner eingeschränkter Personenkreis.

H.R.: Das ist eigentlich nur die EDV-Abteilung plus zwei Brandschutzbeauftragte und der Geschäftsführer.

H.C.: Also kein Reinigungspersonal z.B. (...). Wenn, dann nur in Begleitung und auch da nur sehr eingeschränkt. (...)

H.R.: Wir haben auch Überwachungssysteme z.B. im Eingangsbereich und im Lager. Das Lager ist auch komplett gesichert inzwischen, weil wir Luftfracht selbst verpacken. (...) Da gibt's eigene Schulungen für alle Mitarbeiter, die da Zutritt haben. Das ist eine gesetzliche Vorschrift.

H.C.: Es gibt da eine ISO Norm dafür und eine EU-Richtlinie, die das regeln. Da muss man sich relativ strikt daran halten. Diesbezüglich werden auch Kontrollen unangekündigt durchgeführt, die diese Systeme überprüfen.

I.: Wie oft gibt es einen systematischen Passwortwechsel und gibt es diesbezüglich Regelungen (z.B. minimale Anzahl an Stellen)?

H.R.: Das ist ein großes Streitthema bei uns. Mit jedem Prüfer der bei uns jemals war - wir haben alle 3 Jahre durch unsere Konz-

ernmutter eine IT-Sicherheitsprüfung - und jedes Jahr durch die Wirtschaftsprüfung haben wir eine Prüfung die im Zuge der Wirtschaftsprüfung stattfindet. Und jedes Mal diskutieren wir über den Passwortwechsel.

H.C.: Es ist ganz einfach. Wenn man einen regelmäßigen Passwortwechsel macht, dann sind die Passwörter völlig sinnlos bzw. unsicher. Weil dann merken die Leute sich die Passwörter nicht und die stehen dann irgendwo, d.h. kleben auf dem Bildschirm oder sind komplett simpel. Daher haben wir uns entschieden, wir vergeben ein zufällig generiertes ausreichend langes Passwort mit Buchstaben, Sonderzeichen und Zahlen und das begleitet den Mitarbeiter durch unsere IT-Systeme. (...) Wenn ein Gerät abhandenkommt, wird das Passwort natürlich neu vergeben. Ansonsten darf er dieses Passwort nur in der Firma verwenden, und bei keinen anderen Services bzw. Applikationen. D.h. er darf es auch nicht auf irgendwelchen Fremdsystemen verwenden, wo das Passwort extern kompromittiert werden kann. Es gibt aber auch noch ein zweites Passwort für weniger sensible Sachen. Und dann gibt es noch andere individuelle Passwörter für Gewerke, die mit unserer internen EDV nichts zu tun haben. (...) Passwortschutz gilt natürlich auch für Laptops, die auf Geschäftsreisen mitgenommen werden.

I.: Inwieweit verfügen Sie über Schutzmechanismen wie Firewall, Anti-Virus und Anti-Spam Software? Findet bei Ihnen ein Intrusion Detection System Verwendung?

H.C.: Ja, wir haben gegen Spam hauptsächlich eine Lösung auf Basis von Spam-Assassin. Andererseits haben wir noch technische Maßnahmen beim Mail-Verkehr getroffen, sodass 70%-80% vom Spam und 99% von Viren uns gar nicht erreichen. Und der Rest wird über den Spam-Assassin entfernt bzw. über andere Spamfallen. Und eben mehrere verschiedene Virenscanner. Bzgl. Intrusion Detection System, ja das gab es für eine gewisse Zeit. Wir sind gerade dabei das wieder zu implementieren - im Zuge unserer Firewall Neuimplementierung. Es gibt mehrere mehrstufige Firewalls bei uns. In 3 Implementierungen werden auch ein paar Systeme eingeführt, z.B. Intrusion Detection, Content Analysing und andere.

I.: Also glauben Sie, gerade in diesem Bereich technischer Schutzmaßnahmen sehr gut aufgestellt zu sein?

H.C.: Auf dieser Seite sind wir schon recht passabel, aber wir werden da noch die Messlatte wesentlich höher setzen in den nächsten Wochen. Dann haben wir eigentlich kein größeres Risiko mehr, weil wie gesagt, der Aufwand für einen, der in diesem Bereich Diebstahl betreiben will, viel zu hoch ist, auch jetzt

schon. Und dies über andere Methoden wesentlich einfacher und kostengünstiger zu erreichen ist.

I.: Gehen Sie vielleicht soweit mit den Schutzmaßnahmen, dass Sie USB-Zugänge oder CD Laufwerke entfernen?

H.C.: Nein. Das ist ein komplettes Misstrauensvotum den eigenen Mitarbeitern gegenüber. Und das ist eigentlich nicht unsere Firmenpolitik. Wir lassen unseren Mitarbeitern da einen relativ großen Spielraum, soweit es vertretbar ist und sensibilisieren sie dementsprechend (. . .).

I.: Werden Ihre IT-Systeme regelmäßigen Updates unterzogen?

H.C.: Ja und nein. Es kommt drauf an, da wir verschiedene Sicherheitsstufen bei unterschiedlichen Gewerken haben. Dort wo relevante Daten sind, dort schauen wir natürlich, dass da die Sicherheit höher ist. Und es eben periodische Updates von Patches gibt. Bei den einzelnen Gewerken ist es dann unterschiedlich. Es kommt darauf an. Da kann man keine generelle Aussage darüber treffen. Es ist nicht so, dass wir alles automatisch patchen lassen. Das hat erfahrungsgemäß größeren Schaden verursacht, als Schaden von außen. Wir sind da bspw. bei einem Problem nicht zu Schaden gekommen, das es gegeben hat. Wir haben eine Software von McAfee verwendet, die vor 4-5 Jahren im Zuge eines Updates beim deutschsprachigen Windows plötzlich das Windows als Virus erkannt hat, durch eine Prüfsumme, die zufälligerweise die gleiche war, wie bei einem Virus. Und danach waren bei vielen Firmen die Systeme ausgefallen. Wir machen das nicht, dass wir das automatisch patchen. Wir testen zuerst, ob alles danach weiterhin funktioniert. (. . .) Wir haben z.B. kein Microsoft Netzwerk. Damit werden 90% der Bedrohungen zumindest nicht verteilt. D.h. RPC o.ä. wird nicht verwendet. Diese ganzen Dienste sind nicht aktiv und sie können auch nicht angesprochen werden - von anderen Rechnern aus ohne Wissen des Mitarbeiters. Wir haben also konzeptuell einige Sachen ausgeschlossen.

I.: Gibt es regelmäßige (un-)angekündigte Prüfungen auf Umsetzung und Effizienz der Schutzmaßnahmen (z.B. Penetrationstests durch interne Stellen oder externe Dienstleister), wenn ja, wie oft?

H.C.: Ja und nein, es kommt wieder drauf an. Wir haben jetzt vor kurzem einen Pen-Test gehabt, bzgl. eines Gewerkes das eben teilweise ausgelagert ist beim (. . .) Lieferanten. (. . .) Bei anderen Sachen machen wir das teilweise. Ein Kollege, der heute nicht da ist, der ist ausgebildeter Pen-Tester. Der macht in weiterer Folge regelmäßig eben solche Tests, den wir auch eben aus diesem Grund eingestellt haben.

I.: Also wird das nur intern gemacht, oder gibt es auch externe Di-

enstleister, die das erledigen?

H.C.: Externe Dienstleister machen das bei uns auch in vereinzelten Fällen. In weiterer Zukunft machen wir das aber intern, da wir einen entsprechenden Mitarbeiter haben.

I.: Wie schätzen Sie bei Ihnen die Risiken des ungewollten Know-how-Abflusses mit der zunehmenden Verwendung mobiler (und leistungsstarker) Geräte wie Tablets und Smartphones ein?

H.C.: Null, weil wir solche Geräte gar nicht erst auf unsere Systeme lassen. (. . .) Das einzige Gefahrenpotential liegt darin, dass wir über Tablets und Smartphones auf die eigenen Mails zugreifen können. Und da ist die Sensibilisierung der einzelnen Mitarbeiter gefragt, dass nur über das Hausinterne Computernetzwerk sensible Daten ausgetauscht werden. Generell haben wir dort auch nicht wirklich viele sensible Daten gespeichert.

H.R.: Die Entwicklungsabteilung arbeitet in einem getrennten Netz und der Support hat auch einen getrennten Bereich. (. . .) Für uns gibt's dadurch kaum ein Bedrohungsszenario.

I.: Inwieweit finden externe Cloud-Lösungen (GoogleDrive, Dropbox usw.) bei Ihnen Verwendung?

H.C.: Gar nicht. Sowas könnte ein Kündigungsgrund sein, wenn das verwendet wird.

H.R.: Steht dezidiert in den Richtlinien, dass es nicht zu verwenden ist. Das ist komplett verboten.

I.: Haben Sie sich Gedanken gemacht eigene Cloud-Lösungen zu entwickeln?

H.C.: Wir haben ein MPLS Netz. Das ist sozusagen abgeschottet von allen anderen Netzen, d.h. es ist ein eigenständiges System. Im Prinzip haben wir eine eigene Cloud-Lösung im Einsatz. Sobald ich einen mobilen Zugriff genehmige, stelle ich eine private Cloud ja zur Verfügung. (. . .)

H.R.: Und wir haben die mobilen Zugriffe sehr gut abgesichert. Wir haben eigene Access Points bei A1. Also mein Notebook mit der Datacard darin verbindet sich mit diesem Access Point und das ist bis zur Firewall hin bei uns getunnelt. Also besteht kein freier Internetzugriff.

H.C.: Wir spielen im Prinzip Telefonie-Provider. Das ist denke ich eine der sichersten Lösungen, die man haben kann.

I.: Im Zuge der letzten Meldungen zu Abhörpraktiken wurde bekannt, dass angeblich Hintertüren in kommerzielle Software eingebaut wurde. Wäre die Verwendung von non-Amerikanischer Software oder von Open-Source Produkten – wenn noch nicht der Fall – eine mögliche Alternative für Sie?

H.C.: Wir verwenden viele Open Source Produkte. Auf den Servern

läuft Linux und auch in der Entwicklungsabteilung, sowie bei einigen von unseren Gewerken.

H.R.: Leider nicht auf unseren Workstations. Da sind wir Microsoft-gebunden, auch aufgrund unserer eigenen Entwicklung. Die Betriebssysteme unserer Anlagen laufen zurzeit auch auf Windows. (. . .)

H.C.: Es ist halt so, dass wir Gewerke über 20 Jahre und länger betreuen müssen und vor 20 Jahren war von Linux wenig zu hören. (. . .) Deshalb haben wir fast alles unter Windows entwickelt bekommen und das müssen wir weiterbetreuen. Daher ist ein Umstieg auch nicht wirklich einfach oder sehr langfristig. Auch dadurch, dass diese Produkte sehr hohe Marktanteile haben.

I.: Hat Ihr Haus eine Versicherung zum Schutz gegen Spionage abgeschlossen (z.B. Cyber-, Vertrauensschaden-, Computermissbrauchsversicherung)?

H.C.: Explizit auf Spionage bezogen nein (. . .).

H.R.: Wir haben sie nicht, aber wir haben so viele Versicherungen, da könnte man diese auch noch wahrscheinlich einbinden. (. . .)

I.: Nochmal bettreffend der letzten Meldungen zu Abhörpraktiken: Haben Sie sich da allgemein bei Ihnen im Unternehmen damit befasst? Gerade im Hinblick auf die Informationssicherheit.

H.C.: Wir haben das schon gewusst. Wir sind in der IT derart gegen solche Praktiken, dass wir nicht sensibilisiert werden mussten. Diese Sachen sind zwar medienwirksam aufgekommen, aber uns war das schon lange bewusst. Insbesondere die Gefährdung aus England, auch schon durch ECHELON. Dass wir sozusagen gegenüber institutionellen Spionen einen sehr hohen Security Level machen werden, sodass es für die höchstens interessant ist das durch Human Engineering zu machen und nicht auf die technische Art und Weise.

I.: Damit wären wir am Ende des Interviews. Herzlichen Dank!

12.7 Transcript 6

Name:	Herr G.
Position:	Chief Information Security Officer
Branche:	Informationstechnik
Datum:	16.12.2013 10:10 – 11:10

Notiz: *Aufgrund von Zeitknappheit konnten nicht alle Fragen in Ihrem Detailgrad behandelt werden.*

Interviewer: Vielen Dank, dass sie sich für das Interview Zeit genommen haben! Ich werde nun einige Fragen zu den drei verschiedenen Bereichen Risk-handling, Personal und Sicherung und Kontrolle der IT stellen. Fangen wir mit den Risiko-behandelten Fragen an.
Gibt es eine Sicherheitsverantwortliche Instanz im Unternehmen? Wenn ja, ist diese organisatorisch mit der Geschäftsführung verbunden?

H.G.: Ja, das ist der CISO, in dem Fall ich. Es gibt aber noch mehr muss ich dazu sagen. In jeder der Corporations gibt es einen Informationssicherheitsmanager (ISM). Und dann gibt's natürlich verschiedene Rollen, die auch Sicherheitsaspekte abdecken, also Sicherheitsrollen im Unternehmen wie ein Security Agent z.B. In einzelnen Offices, wenn die Offices nicht zu groß sind und es sich um keine Niederlassung handelt, dann hat in der Regel einer in dem Office eine Sicherheitsfunktion.

I.: Um Know-how Schutzmaßnahmen effektiv ergreifen zu können, bietet sich eine Risikoanalyse an. Inwieweit wurde bei Ihnen eine Risikoanalyse und Bewertung durchgeführt (ggf. gemäß ISO 27001)?

H.G.: Wir sind ISO 27001 zertifiziert. Allerdings am Standort Wien bzw. Österreich. D.h. es gibt ein gültiges Zertifikat. (. . .) Und dann wenn man das Zertifikat hat, dann muss man zwingend ein entsprechendes Risikomanagementsystem betreiben. (. . .)

I.: Bei der Risikobewertung, haben Sie da gewisse Parameter in Betracht gezogen wie Schadenshöhe und Eintrittswahrscheinlichkeit? Hatten Sie noch weitere Parameter mit einbezogen?

H.G.: Das ist jetzt die Frage welche Methode man für das IS-Risikomanagement verwendet. Da gibt es verschiedene Ansätze. Es ist so, dass die Firma unter anderem eine Kapitalbeteiligung hat an einer anderen Firma mit Sitz in Österreich. Diese Firma entwickelt und vertreibt ein (. . .) Risikomanagementtool. Das ist eine bestimmte Methode, wo man speziell – also das ist wirk-

lich IT-lastig - aus der IT-Sicht heraus Risikomanagement betreiben kann. Dieses Tool wird auch bei uns intern verwendet. Die grundlegende Ideendefinition ist gleich, aber es fließt noch mehr hinein bei der Gesamtrisikobewertung. (. . .) Es ist eines der Tools am Markt, die es gibt und dort werden im Prinzip Abhängigkeitsketten modelliert und sie können dann auch Kataloge hinterlegen. Zum Beispiel definieren sie einen Service z.B. E-Mail-Service oder ERP System. Dann machen sie Business Impact Analysen mit den einzelnen Process-ownern, stellen die Requirements fest für den Service; Wie kritisch ist E-Mail aus der Sicht eines Bereichsleiters auf die 3 Kriterien Vertraulichkeit, Verfügbarkeit und Integrität. Wie sicher sind die Daten im Bezug auf Vertraulichkeit, d.h. müssen die extrem sicher sein usw. Dann stellen sie die Anforderungen fest, dann modellieren sie eigentlich alles was sich dahinter bewegt auf Service-Level, sprich die Anzahl der Server usw. wird modelliert. Und dann wird das Risiko gesamtaggregiert zu einem gesamten Risiko-Rating. Da kommt dann eine Qualitätsziffer raus, ähnlich wie im Finanzbereich. Das geht von CCC bis AAA. Und der Vorstand definiert ein Zielrating und sie definieren z.B. dann mit der Risikoanalyse kommen sie dann auf ein IST-Rating. Dann haben sie ein „gap" und dann fallen Maßnahmen auch aus dem Tool heraus inkl. der Abhängigkeitsanalyse. Sie können auch feststellen, welcher Faktor z.B. dann das niedrige Rating verursacht. Nehmen wir mal an, ein Server ist nicht redundant, dann ist die Ausfallsicherheit hoch. Und dann ergibt sich aus dem rechnerisch aus dem Tool ein Gesamtschadenspotential. Da fließen dann viele Dinge mit ein, nicht nur Eintrittswahrscheinlichkeit mal potentieller Schaden. Ist aber relativ komplex, das kann man jetzt nicht in 2 Sätzen erklären.

I.: Also fand auch direkt dort dann eine gewisse Klassifizierung statt?

H.G.: Ja.

I.: Können Sie auch sagen welche Bereiche die größten Risiken aufwiesen und wurden diese in irgendeiner Form klassifiziert?

H.G.: Das ist dann schon eine Frage, die heikel ist. Ich kann jetzt Ihnen antworten, aus meiner Erfahrung heraus, weil das auch ein Schwerpunkt sein wird meiner Arbeit zukünftig. Der größte Risikofaktor und oft vernachlässigt und nicht betrachtet ist und bleibt der Faktor Mensch. Und da geht man wieder Richtung Social Engineering usw. Die Nachlässigkeit und die allgemein geringe Awareness zum Thema Security ist ein riesiges Problem, dass oft völlig out-of-scope ist, d.h. es wird eigentlich nicht

wirklich als Risiko gesehen. Also man redet über hochkomplexe technische Maßnahmen mit (. . .) n-facher redundanter Auslegung der Systeme und bei den Analysen, wenn man wirklich mal Tests macht, also z.B. einen Social Engineering Test, dann stellt man fest, dass eben die Policies zwar überall irgendwo geschrieben sind, aber in der Praxis sehr schwer an den 08/15 Standard Mitarbeiter wirklich im Sinne von Awareness, dass er weiß was er tut, das ist für mich einer der kritischsten Punkte überhaupt. Zumal ja aus dem Privatbereich jeder mit IT zu tun hat und sich super auskennt und (. . .) locker im Internet umher surft. Also ich sehe da das größte Risiko eigentlich in diesen Dingen. Und das zweite ist. Ich glaube allgemein, dass ein Risikomanagementprozess, ich sag mal das Stichwort Saisonarbeit, also sprich es ist in der Regel die Kontinuität und Nachhaltigkeit bei vielen Firmen nicht gegeben. Man macht immer etwas zum audit hin. Es gibt ein Audit. Man setzt fieberhafte Aktivität ein. Dann wird alles Mögliche nachgeholt, was man vorher vielleicht versäumt hat, dann kommt das audit - das ist die berühmte Sägezahnkurve von den Aktivitäten -, dann ist das audit vorbei, dann sackt das nach dem audit um einen gewissen Prozentsatz herab um sich dann langsam wieder bis zum nächsten audit wieder herauf zuschrauben. Das Problem ist einfach diese Ungleichförmigkeit bei diesen Bemühungen in dieser Aufmerksamkeit das dieses Thema erfährt. Das halte ich eigentlich für ein Hauptproblem. Und das nächste ist auch wieder der Faktor Mensch im Sinne von Verschleißerscheinungen und Nachlässigkeit. Banal gesagt, es passiert eigentlich zu wenig als dass man das Bewusstsein schärft. Das sind so die Punkte aus meiner Sicht. Und die sind natürlich nicht konkret auf das Unternehmen bezogen, aber ich sage mal, wir sind dort auch keine Ausnahme. Das Policy Definieren und an den Mann bringen, dann gibt's Firmen, die haben viel zu viele Policies. Die kann sich kein Mensch merken. Also sprich der Transfer von einem synthetischen Policy-Framework mit zig Regulations die es da gibt, die definiert sind auf konkretes Verhalten der Mitarbeiter im Sinne von inkooperieren des Gedankens und verstehen und danach handeln. Diese Kette ist halt schwach bei den meisten, weil es ja auch lästig ist und behindert usw. Und das zweite Thema ist, Security wird natürlich gerne mal sehr schnell aufgrund von irgendwelchen Business Requirements, ich sage mal Projektrisiko, Fertigstellungstermin, Pönale Forderung, da wird die Security gerne mal sehr schnell nach hinten geschoben oder ausgehebelt. Das ist aber bei fast allen Firmen, die ich kenne so. Ja das

ist sicher nicht gut. Wenn es temporär ist, ist ok, aber mitunter entstehend auch Lösungen, die Security vom Requirement-Gedanken so implementieren, wie es eigentlich notwendig wäre oder es manchmal geplant wird.

I.: Welche Maßnahmen zum Know-how Schutz konnten denn konkret von der Analyse und Bewertung abgeleitet werden?

H.G.: Natürlich gibt es etliche Maßnahmen. Sie müssen ja nach ISO 27001 Maßnahmen durchführen. Und da muss ja ein KVB drauf liegen, d.h. sie müssen Maßnahmen umsetzen und auch die Wirksamkeit letztendlich nachweisen. (...) Idealerweise gibt es bei uns 2 Mal im Jahr eine Sitzung des Sicherheitsforums, wo unser Vorstand teilnimmt.

I.: Inwieweit werden Unternehmenskooperationen als Risiko angesehen, insbesondere der Austausch von Zugangsdaten oder sensibler Informationen?

H.G.: Ja ich denke schon. Weil, wenn es eine reine Kooperation ist und keine Übernahme, ist es natürlich immer schwierig das Thema. Ich halte es schon für risikobehaftet, weil es ja auch verschiedene Sicherheitspolitiken miteinander verbindet. Sie haben ja verschiedene Risikokulturen und auch verschiedene Sicherheitspolicies und die müssen sie dann in Einklang bringen und es ja auch sein, dass sie widersprüchlich sind und da liegt schon ein gewisses Konfliktpotential - auch im Sinne von Risiko.

I.: Können Sie denn etwas zu Häufigkeit, Umfang oder Systematik von Cyber-Angriffen auf Ihr Unternehmen sagen?

H.G.: Nein. (...) Die Frage ist auch, was ein Cyber Angriff ist. Wenn ein Port-Scan, der n-fach auftritt, auch als Angriff betrachtet wird z.B. Das sehe ich schon so. Von konkreten Angriffen bis der Intention jetzt nicht nach dem Zufallsprinzip, sondern schon mit der Intention wichtige Informationen von Unternehmen zu bekommen, ich würde mal so antworten. Ich glaube das findet sicher statt. Die awareness ist aber allgemein im Top-Management - ich sage mal - unterausgeprägt. Also jede Gefahr, die ich nicht bewusst wahrnehme ist sehr schwer zu realisieren letztendlich. Ich glaube insbesondere was, wir wissen ja spätestens seit Prism und co., also es findet häufiger statt als man glaubt und wir wissen nicht genau, welche Informationen raus gehen oder nicht.

I.: Das ist natürlich ein weiteres Problem, dass man häufig gar nicht erst sagen kann, ob man Opfer einer Attacke geworden ist, weil man es nicht registriert hat.

H.G.: Wenn sie jetzt sagen, die NSA ist in ihrer Sammelwut, d.h. sie

sammelt alle möglichen Daten und werten diese dann auch aus. Ob das dann ein Schadenspotential hat und ob es dann benutzt wird zu Industriespionage, ja, die Wahrscheinlichkeit ist nicht so gering. (...) Das Problem an der ganzen Geschichte ist auch, dass alle zusammen arbeiten und die Politik sehr holperisch versucht Populismus oder das Volk zu besänftigen, weil in Wirklichkeit liefern alle zu. Also sowohl der Heeresnachrichtendienst, als auch der BND, sie kooperieren in Wirklichkeit mit der NSA. Daher ist das schon eine Politposse, was da stattfindet.

I.: Gibt es (oder gab es) allgemein eine Zusammenarbeit mit Sicherheitsbehörden (Polizeilich o. Nachrichtendienstlich)? Wenn ja, in welcher Form?

H.G.: Ja die gibt's schon.

I.: Also findet da ein Austausch an Informationen statt?

H.G.: Ja, sowohl anlassbezogen, als auch informelle Meetings, ja.

I.: Kommen wir nun zum Bereich Personal.
Inwieweit wird bei Ihnen eine Schulung / Sensibilisierung zur Förderung des Risikobewusstseins der Mitarbeiter bzgl. Umgang mit Informationen (insb. Email und Cloud, Chat / Skype) und Beachtung der Security-Policies durchgeführt?

H.G.: Wir versuchen jetzt das Thema zu adressieren. Policies haben wir zu genüge. Ich habe jetzt als einer der ersten Maßnahmen oder Aktionen auf meinem Radar, ein Security Awareness Training gehabt. Das wird von österreichischen Hersteller angeboten. Ist so eine Art virtuelles 3D Training, wo man durch ein virtuelles Gebäude läuft und so klassischen Situationen am Arbeitsplatz und die Gefahren versucht bei den Mitarbeitern beizubringen. (...) Da werden alle Themen behandelt, wie z.B. shoulder-surfen, Bildschirm sperren, Passwortrichtlinien, Datenklassifizierung, Umgang mit externen Datenträgern usw. Alles was es so im Büro für Alltagssituationen gibt. Der Plan ist, dass man das anwendet bei uns im Unternehmen, also dass das HR übernimmt dann das tracken. D.h., dass jeder Mitarbeiter, das wäre das Ziel zumindest, ein Mal im Jahr dieses Training und den Test dazu absolviert und besteht. Da geht's genau um diese Dinge. Awareness schärfen für die Security-Themen.

I.: Inwieweit werden denn Mitarbeiter auch für die Gefahren von Geschäftsreisen sensibilisiert?

H.G.: Ja, das steht natürlich in der Policy. Jetzt können sie sich ja vorstellen, wir haben natürlich interessante Herausforderungen, weil wir z.B. mit einem anderen Land, das nach gängiger Auffassung quasi eine Diktatur ist, ein großes Projekt hat,

(. . .) und da haben wir natürlich bei Projekten mitbekommen, dass der Kunde Sicherheitsstandards fordert, damit er abhören kann. Also ich nehme mal ein Banalbeispiel. Wenn sie jetzt eine Firewall eine Officeverbindung machen, oder einen VPN Tunnel zwischen zwei Standorten, dann kann es sein, dass der Kunde ihnen sagt, er fordert ein gewisses Firmrelease, weil das nur DES verschlüsselt, weil das neueste wäre Tripple-DES und das können sie nicht mehr lesen. Also solche Sachen begegnet einem dann schon, wo man schon eigentlich wissen muss, dass da Kommunikation abgehört wird und Information nach außen dringt. Das machts natürlich noch spannender und schwieriger letztendlich. Aber wie man jetzt weiß, spätestens seit NSA, ist es nicht die Frage, ob jemand abhört, sondern die Frage ist eher, wer jetzt abhört oder wer es kann und wer es nicht kann. Wenn die NSA jetzt die bisher sicher angenommenen Sicherheitsstandards knacken, dann muss es einem klar sein, dass es keine echte geheime Information mehr gibt. Aber das heißt natürlich nicht im Umkehrschluss, das ist sehr wichtig, das steht auch häufiger in Zeitungen, (. . .) dass man nichts mehr tun sollte, sondern man sollte nach Möglichkeit es so schwer wie möglich machen. Sicherheit ist ja immer nur zeitlich begrenzt letztendlich.

I.: Bieten Sie auch VPN Möglichkeiten an?

H.G.: Ja, haben wir. Wir verkaufen es auch, aber wir bieten es auch intern an.

I.: Haben Sie formal fixierte Sicherheitsstandards wie Clean Desk Policy oder Bestimmungen zur Nutzung / Vernichtung von Informationsbeständen?

H.G.: Clean Desk Policy haben wir auch. (. . .) Die externen wie das Reinigungspersonal sind da weniger das Problem. Die haben wir gut unter Kontrolle, weil denen kann man ja im Zweifelsfall mit Auftragsentzug drohen. Es sind ja alles externe Firmen und Kontraktoren. Die müssen halt schon schauen, dass sie z.B. Räume versperren. Wir haben einen Reinigungsdienst, der wenn sie unbeaufsichtigt in Räume gehen und putzen, was de Facto der Fall ist, dann hatten wir da Security Sachen, das Türen nicht verschlossen waren hinterher. Und das hat dann schon Konsequenzen. Entweder wird das Personal dann getauscht, oder die Firma verliert den Vertrag. Bei den internen Mitarbeitern ist es etwas schwierig. (. . .) Clean Desk ist schön, aber wenn es jemand nicht tut, naja dann passiert eben auch nichts. D.h. das durchgreifen ist ein gewisses Problem. (. . .) Clean Desk wird ja auch oft falsch verstanden. Es heißt ja nicht, dass aufgeräumt werden soll, sondern, dass geheime Informationen

nicht irgendwo rumliegen dürfen. (. . .) Wir haben da auch weitere Maßnahmen. Wir haben gewisse Standards, also alle Laptops haben Festplattenverschlüsselung installiert und da schauen wir schon drauf und da kann man dann technische Maßnahmen setzen, da ist es dann einfacher ja. Bei diesen weichen Geschichten, die so eher in Richtung soft skills gehen und so, dass man z.B. fremde Mitarbeiter, die man nicht identifizieren kann, anspricht wenn sie einem im Gebäude begegnen. Dass man Kollegen anspricht, und den Mitarbeiterausweis fordern, das ist schwierig. A, da gehört eine gewisse Zivilcourage dazu und B, muss ich auch die Kultur im Unternehmen haben. Das tut man nicht. (. . .) Das Akzeptanzlevel muss auch gegeben sein. Denn was passiert mit der Sicherheit, wenn die Akzeptanz nicht gegeben ist. Die fällt von mittelmäßig hoch auf ganz niedrig. (. . .)

I.: Findet im Rahmen des Personalauswahlverfahrens eine intensive Überprüfung der Bewerber statt (insbesondere im Bereich der IT)?

H.G.: Es findet eine Überprüfung statt, aber wie intensiv sie ist, kann ich nicht wirklich sagen. Es findet aber keine dezidierte Sicherheitsüberprüfung statt im Sinne von richtigem Background Investigations. Der Prozess als solcher ist nicht wirklich sauber definiert. Was gemacht wird, so wie heute von jeder HR Abteilung ist, schaut man sich an was der Bewerber im Internet macht, bzw. die Social Networks durch. Aber das ist Sicherheit auf einem relativ niedrigem Niveau.

I.: Wie wird bei Kündigung/Weggang eines Mitarbeiters verfahren?

H.G.: Vieles ist teilautomatisiert. Der Prozess sieht vor, dass accounts so rasch wie möglich deaktiviert sind.

I.: Wurde eine Schutzbedarfsanalyse durchgeführt, die für alle regelt, welche Daten / Informationen geheim, vertraulich oder offen zugänglich sind?

H.G.: Es gibt eine Datenklassifizierung, aber man tut sich nicht leicht damit. Das ist etwas, was man Mitarbeitern extrem schwer beibringt. Zumal ich dann ja auch bei jedem Dokument bzw. Datei die angelegt wird, muss ich mir Gedanken machen, wie ich diese Daten klassifiziere. Und da gibt's noch etliches zu tun.

I.: Ich hatte ja kurz die Cloud bzw. Skype angesprochen. Gibt es Policies, die die Nutzung dieser Services im Unternehmen regeln, bzw. untersagen?

H.G.: Skype ist nicht verboten, weil wir Skype eine ganze Zeit mit Ländern mit schlechter Anbindung, es war die einzige Möglichkeit kosteneffizient zu kommunizieren. Aus der Sicherheit war eigent-

lich klar, was man von Skype zu halten hat. Also man versucht halt bei den Mitarbeitern das Bewusstsein zu schärfen, dass Skype nicht abhörsicher ist und es entsprechend (. . .) ausgewertet wird. Wir haben das aber nur bei den Anbindungen wo jetzt eine schlechte Internetanbindung ist, wird Skype benutzt. Ansonsten gibt's die internen Kommunikationssysteme (. . .) Microsoft OCS (Office Communications Server) und Lync. Aber das sind nunmal auch Microsoft Technologien, also NSA, Prism etc. Das ist natürlich auch wieder nicht abhörsicher, aber es verwendet mal gängige Verschlüsselungsalgorithmen. Das gleiche gilt für Video-conferencing. Am Ende des Tages steckt in jeder Kiste ein Amerikanischer Chip mit irgendwelchen nicht-dokumentierten Funktionen, von denen man nicht weiß. Aber ich würde mal Skype als unsicherer einschätzen, als jetzt die Tools von der Verschlüsselungsstärke aus. Gut, ist jetzt eh alles Microsoft und wird wahrscheinlich alles zusammen wachsen. Das zweite Thema Cloud. Mit der Cloud tut man sich generell schwer. Weil man es nicht wirklich kontrollieren kann. Weil es rechtliche Aspekte gibt, die man berücksichtigen muss. Bei uns ist es eigentlich laut Policy verboten. Ich sage aber mal, es wird toleriert. Es gibt immer wieder die berühmten Ausnahmen von der Regel. Die Frage ist immer zwischen dem Privatnutzungsanteil und dem betrieblich bedingten. Wir wollen nicht, dass für betriebliche Daten Cloud Services wie Dropbox und GoogleDrive benutzt werden. Aber das ist Graubereich. (. . .) Aber es ist auch etwas, was mir Bauchweh bereitet, weil man nicht so recht weiß, wie man damit umgehen soll. Also es gibt spätestens seit diesen Skandalen gewisse Unternehmungen einen eigenen Cloudbereich zu schaffen. So gibt es in Österreich etliche Firmen, die von der Austrian Cloud schwärmen oder so etwas anbieten wollen. Wie viel konkret, da fehlt mir etwas die Marktübersicht. Nachdem wir auch Service-Anbieter sind, kann ich nur sagen, auch wir überlegen etwas anzubieten, wo man als Anbieter am Markt dem Unternehmen sagen kann: Deine Daten bleiben auf jeden Fall in Österreich. Über welchen Weg sie nach Österreich kommen ist eine andere Frage. Aber sie sind zumindest hier in Österreich auf dedizierten Server und nicht auf irgendwelchen Servern weltweit, auch mit rechtlich schwierigen Sachen. D.h. aber auch im Zweifelsfall, es gilt das österreichische Recht, auch bzgl. Datenherausgabe usw., d.h. es muss dann die österreichische Staatsanwaltschaft oder wer auch immer den Zugriff autorisieren. Das ist sicherlich ein gutes Argument, wenn es

so einen Service gibt, dann spricht nichts dagegen. Aber das Problem ist, wenn ich gar nicht weiß – idealerweise ist die Cloud ja eine Virtualisierungsebene, wo vom Grundprinzip her es mich nicht zu interessieren hat, wo die Daten liegen. Es ist einfach abstrahierter Level, es ist die Cloud, und wie die Cloud sich zusammensetzt. Nur rechtlich gesehen, ist es eben so, dass es keine Rechtssicherheit in der Cloud gibt. Dazu gibt es auch viele Vorträge zu dem Thema. Also Juristen bewerten das Thema ganz extrem, insb. wenn es darum geht, wenn personenbezogene Daten abgespeichert werden, ist das aus juristischer Hinsicht ein Albtraum, weil es nicht rechtsicher ist. Der Gesetzgeber fordert etwas anderes und das ist nicht in der Cloud zu erfüllen. Also so Cloud SAP Services? Viel Spass. Wo personenbezogene Daten verarbeitet werden? (...) Ich glaube da gibt's keine Awareness, und viele Unternehmer wissen gar nicht, auf welchem Minenfeld man sich da in dieser Thematik befindet. Also es ist sicher nicht gelöst, so eine österreichische, deutsche oder europäische Lösung (...). So etwas wäre sicher zu bevorzugen. Aber über welchen Internetknoten am Ende die Daten gehen, das ist dann wieder die andere Sache. Also das eine Thema ist, wo die Daten verbleiben und von wo und wohin der Zugriff erfolgt. Und das andere Thema ist, wie kommen die Daten dort hin, also auf welchem Kommunikationsweg. Und der ist in der Regel eben beim Internet nicht unbedingt klar bestimmt. Das Internet ist nun mal anders aufgebaut, da weiß du gar nicht, auf welchem Wege die Daten verlaufen und das ist dann womöglich auch nicht abhörsicher.

I.: Ich würde jetzt zu den technischen Sicherheitsmaßnahmen übergehen.

Inwiefern wird auf das Risiko gefährdeter Datenträger (USB-drive, HDD) geachtet und spielt die Verschlüsselung von Datenträgern und Datenverkehr (insb. E-mail) bei Ihnen eine Rolle?

H.G.: Ja, wir haben gewisse Maßnahmen, aber ich muss gestehen, wir sind von der Konsequenz, so wie viele andere österreichische Unternehmen auch – das muss immer ein Kompromiss sein zwischen Usability und Security – ich wäre froh aus meiner Sicht, wenn man es durchsetzen könnte, dass man USB ports blockt. Technische Maßnahmen gibt es zu genüge. Verwaltung ist relativ aufwendig. Und man behindert natürlich den Arbeitsfluss letztendlich. Also das ist uns bisher nicht gelungen. Ich sehe da jetzt momentan auch keine Möglichkeit es umzusetzen, aufgrund der Akzeptanz der Security, also auch ein CISO kann nicht gegen das Business regieren, das geht nicht – nur aus der CISO-Sicht.

Aber das halte ich letztlich auch für ein sehr großes Problem. Es gibt verschiedene Lösungsansätze, wie man das verbessern kann. Die ultimative Lösung sehe ich nicht. DLP ist das Thema, also wie Daten aus dem Unternehmen heraus weggehen in irgendwelche Richtungen. Cloud ist da auch in dem Aspekt zu sehen. Cloud oder USB Datensticks oder was auch immer. Die werden verloren, Daten sind unverschlüsselt, Daten sind nicht klassifiziert usw. Ist ein Problem. (. . .) Bei der E-Mail wird Verschlüsselung als Service angeboten, aber das Zertifikat (z.B. S/MIME) kostet im Jahr natürlich Geld. Es ist geplant, das gerade im Management zu etablieren. Es ist aus meiner Sicht ein Muss, wir erarbeiten das auch im Hinblick auf Risikoanalysen usw., da wird's dann auch entsprechende Maßnahmen geben, die empfohlen werden. Ob sie auch umgesetzt werden, ist eine andere Sache. Es ist auf jeden Fall absolut sinnvoll, (. . .) aber da muss man evtl. auch ein bisschen Aufklärung leisten, was ist das denn genau, heißt das jetzt ich kann keine Mails mehr schicken oder kann ein andere die nicht empfangen. Was ist der Unterschied zwischen einer digitalen Signatur und einer Verschlüsselung usw. Das wird recht schnell dann auch sehr technisch komplex. Einfach von der Handhabung. Wir versuchen das natürlich auch zu schärfen. Wenn man den Mitarbeitern sagt, E-Mails schreiben ist wie Postkarten verschicken, das kann eh jeder lesen mit relativ wenigem Aufwand. Das muss dir bewusst sein, ja. . . aber es kommt nicht ganz an in den Köpfen. Wer verschlüsselt denn im Privatbereich E-Mails, ist ja auch die Frage, was steht drin. (. . .) Ich empfehle immer als relativ einfache Maßnahme 7-Zip oder so etwas, womit man auch Daten verschlüsseln kann. Da muss man dann nach Möglichkeit jemanden anrufen und nach Möglichkeit nicht das Passwort per Mail schicken. Also das sind dann Möglichkeiten, wo ich das relativ sicher machen kann. Hat dann aber wiederum Administrationsschwächen.

I.: Wie sehen die (auch räumlichen) Zutritts- und Zugriffsberechtigungskonzepte (insb. Zugang zum Rechenzentrum) für sowohl firmeneigenes als auch firmenfremdes Personal bzgl. gefährdeten Daten und Objekten aus?

H.G.: Da das Rechenzentrum wo anders liegt, kann ich nicht genau sagen, wie dort die Zutrittskonzepte aussehen. Es ist nur so, dass sie grundsätzlich nicht ohne Begleitung bei uns in den Offices herumlaufen können und bei dem Rechenzentrum sind die Kontrollen noch schärfer. (. . .) Also da schaut man schon sehr genau. Die Policy sagt ganz klar, kein Besucher ohne entsprechende Karte und auch nicht allein. Und das ist auch was, wo ich sagen

würde, das funktioniert relativ gut bei uns im Haus, aber in der Regel wird versucht das auch zu schärfen, dass man sagt, ok wenn ich jemanden nicht kenne, schauen ob er Firmenausweis hat. Ich halte 1 Mal im Monat ein Training im Rahmen des Onboardings für neue Mitarbeiter, das mache ich persönlich, da versucht man das beizubringen, was man mit den Karten machen kann, und beobachten muss. Es wird vielleicht auch zukünftig eine zusätzliche Kennzeichnung geben für dass man die Besucherkarten noch deutlicher erkennt. (. . .)

I.: Wie läuft denn das in anderen Ländern ab, wo sie Geschäftsstellen haben. Wird dort die Policy, die sie hier ausgeben, auch dort dementsprechend gelebt im Bezug auf den Konzerngedanken?

H.G.: Naja grundsätzlich gilt die Policy bei uns weltweit. Wir versuchen das auch im Rahmen von audits auch festzustellen, wie gut die Maßnahmen auch umgesetzt werden und wir werden auch dieses Tool, was wir einsetzen für das Maßnahmentracking, da sind wir momentan dabei den scope zu erweitern, d.h., der Plan ist, das auf alle Länder auszurollen. Und dann wird es dort lokal einen Sicherheitsverantwortlichen geben. Der wird das Tool befüttern müssen, sprich wenn er ein finding hat, muss er das reingeben. Und das wird dann über ein Management-Dashboard in die Unternehmenszentrale reported, d.h. ich seh dann auch den Maßnahmenstatus, generell den Risk-Status, soweit es das zulässt. Und damit ist eigentlich die Nachhaltigkeit im Prinzip schon gegeben, ja.

I.: Wie oft gibt es einen systematischen Passwortwechsel und gibt es diesbezüglich Regelungen (z.B. minimale Anzahl an Stellen)?

H.G.: Ja gibt es. Die üblichen Regelungen. Es gibt eine History, die zweistellig ist, d.h. sie können die letzten >10 Passwörter nicht verwenden. Und das Passwort hat eine gewisse Minimallänge und ist komplex zusammen zusetzen. Naja und dann die üblichen Sachen, wie nicht aufschreiben, nicht weitergeben (. . .). Es gibt schon auch eine Empfehlung den Passwortsafe zu benutzen, dieses KeePass, wo man ein Masterpasswort verwendet. Und ich denke auf dem Weg kann man die Mitarbeiter vielleicht auch eher dafür begeistern und ins Boot holen, wenn man ihnen einen Nutzen auch für den Privatgebrauch mitgibt. Und wenn sie dann sagen, das ist jetzt schon sinnvoll, dann fängt man es sich eher ein als wenn man es nur auf die beruflichen Anforderungen beschränkt. Und das gleiche gilt für den Virusschutz und das sichere surfen am Arbeitsplatz. (. . .) Der Übergang verschwimmt ja heutzutage schon fast. Ich kann fast gar nicht mehr unterscheiden zwischen dem Privatbereich und diesem Business Kontext. Und wenn man

es dann schafft auf die Gefahren, also meine Erfahrungen sind, dass jeder Mitarbeiter im Einzelnen immer anders reagiert, wenn es einen persönlich betrifft, also etwas konkret als Gefahr annehmbar ist. (. . .)

I.: Inwieweit verfügen Sie über Schutzmechanismen wie Firewall, Anti-Virus und Anti-Spam Software? Findet bei Ihnen ein Intrusion Detection System Verwendung?

H.G.: Da haben wir natürlich die ganze Palette. Wir haben natürlich viele Partner wie Symantec, CISCO usw., und nachdem wir solche Lösungen selbst anbieten, setzen wir diese natürlich auch selbst ein. (. . .) Ein Intrusion Detection System haben wir auch.

I.: Also glauben Sie, gerade in diesem Bereich technischer Schutzmaßnahmen sehr gut aufgestellt zu sein?

H.G.: Da sind wir ziemlich gut aufgestellt. Ich muss aber auch dazu sagen, es ist in der Regel nicht die technische Maßnahme das Problem, sondern das Problem ist wieder einmal die Nachhaltigkeit und das Management. Sie können jetzt dem Kunden eine Firewall verkaufen, (. . .) stellen die Firewall hin und die wird nie wieder angegriffen, erst dann wenn sie eine Änderung brauchen. Niemand checkt eine Firewall auf die Plausibilität usw. Bei größeren Unternehmen natürlich, bei kleineren nein. Wird einmal installiert und das wars. Jede Arztpraxis hat eine Firewall, aber wird die auch upgedated? Aber das ist auch das Problem, dass ich ja auch heute logging systeme habe. Aber das Problem ist dann die Auswertung. Wer wertet die aus. Wie schaffen sie es aus diese SIEM (Security information and event management) - aus lauter Bäumen sehen sie den Wald nicht mehr. Sie müssen ja die eigentlich wirklich beachtenswerten Incidents herausfiltern und den Rest können sie schmeißen. Und da entsteht eine Datenflut, die ist gigantisch und die Herausforderung ist wirklich die Korrelation von den wenigen kritischen Ereignissen und die zu reporten und zu behandeln. Da sind die meisten komplett überfordert, das muss man so sagen.

I.: Werden Ihre IT-Systeme regelmäßigen Updates unterzogen?

H.G.: Das funktioniert nicht vollautomatisch, aber wir legen die Updatezyklen fest, d.h. es muss dann erst klassisch laut ISO 27001, sie haben erst eine definierte Testumgebung, dann haben sie vielleicht noch eine Pilotgruppe oder so etwas wo sie die Security Patches rausholen und dann wird das deployed.

I.: Gibt es regelmäßige (un-)angekündigte Prüfungen auf Umsetzung und Effizienz der Schutzmaßnahmen (z.B. Penetrationstests durch interne Stellen oder externe Dienstleister), wenn ja, wie oft?

H.G.: Unangekündigt nicht wirklich. Naja, es gibt Pläne dafür, dass man diese Kultur implementiert im Unternehmen, aber das ist in Österreich sag ich mal vorsichtig auch ein heikles Thema. Wir haben vor einigen Jahren einen Social Engineering Test gemacht und den Test mit präparierten USB Sticks, und das gab schon sehr interessante Ergebnisse. Also da gab es Mitarbeiter, die das Unternehmen verklagen wollten usw. Die ganze Bandbreite an Reaktionen. Aber das war unangekündigt und das hat dementsprechend sehr hohe Wellen geschlagen. Sie müssen das quasi ankündigen, sonst kommt der Betriebsrat ins Spiel usw., sehr schwierig.

I.: Also wird das nur intern gemacht, oder gibt es auch externe Dienstleister, die das erledigen?

H.G.: Teils, teils. Idealerweise extern, aber dafür fehlt manchmal das Geld.

I.: Wie schätzen Sie bei Ihnen die Risiken des ungewollten Know-how-Abflusses mit der zunehmenden Verwendung mobiler (und leistungsstarker) Geräte wie Tablets und Smartphones ein?

H.G.: Sehr groß. Da kann ich ihnen auch sagen, wir vertreiben da eine Lösung. Wir haben MDM (Mobile Device Management). Wir haben da eine Partnerschaft mit einer anderen Firma. Technisch wieder super, auch im Sinne der organisatorischen Umsetzung und der Berücksichtigung steuerlicher, rechtlicher Aspekte usw., sie brauchen eine Betriebsvereinbarung, sie müssen im Notfall das Gerät löschen können, dann was ist mit den privaten Daten. Die werden natürlich mitgelöscht. Müssen sie überlegen, wie macht man ein Backup, wie regelt man das organisatorisch. Müssen die Mitarbeiter das selbst machen etc. Sie können da den Mitarbeiter tracken. Wir haben einen Eigenanteil bei den Firmenhandys, dann haben sie ein Miteigentumsrecht. Wir haben (. . .) Mobile-Device Vielfalt, d.h. alle Hersteller, alle möglichen Modelle, alle Betriebssysteme, Varianten usw. Derzeit sind die organisatorischen Herausforderungen die großen. Die technischen sind relativ einfach zu lösen. Die Amerikanischen Anbieter verstehen da meist gar nicht die Diskussion. Ich kenne von einer Firma, dass sie nur ein Device haben. D.h. sie haben nur Apple, und nur Applephones und Ipads. Dann würde ich auch das als guten Ansatz halten. (. . .) Aber da fehlt es auch am starken Commitment vom Management aus. Wenn da einer auf den Tisch hauen würde und sagen würde, ich möchte, dass das sicher ist und ich will nicht, dass der Mitarbeiter die Freiheit hat aus 20 Handys auszuwählen. Das ist Ineffizient, auch im Sinne vom Support. Dann würde es sehr helfen.

I.: Im Zuge der letzten Meldungen zu Abhörpraktiken wurde bekannt,

dass angeblich Hintertüren in kommerzielle Software eingebaut wurde. Wäre die Verwendung von non-Amerikanischer Software oder von Open-Source Produkten – wenn noch nicht der Fall – eine mögliche Alternative für Sie?

H.G.: Es gibt da einfach nicht viele Anbieter. Es gibt einige wenige, die sehr gute Lösungen haben. Das Problem ist, dass man – wenn es nicht gerade Open Source ist mit Propretät schafft man ja mitunter schon wieder neue Probleme. Also Open Source, wenn es vernünftige gut zu administrierende Lösungen gäbe, ja. Ansonsten glaube ich, dass das theoretische Ansätze sind, die in der Praxis nicht funktionieren, weil in jedem Handy, in jedem PC amerikanische oder chinesische Technologie steckt. Und wenn sie auf Security Vorträge fahren (. . .) wenn sie wissen, dass bei Anti-Viren Herstellern 70% kennt man, der Rest ist unknown. Wenn sie mit stuxnet und anderen Dingen sich beschäftigen, wird einem klar, dass vieles nicht dokumentiert ist und vieles geht. Erschreckend, aber es ist so. Es ist so, man kann die Haustür 3 Mal abschließen, aber es gibt nichts, was nicht unüberwindbar wäre.

I.: Hat Ihr Haus eine Versicherung zum Schutz gegen Spionage abgeschlossen (z.B. Cyber-, Vertrauensschaden-, Computermissbrauchsversicherung)?

H.G.: Ist mir nicht bekannt.

I.: Damit wären wir am Ende des Interviews. Herzlichen Dank!

12.8 Transcript 7

Name:	Herr W.
Position:	CIO (Director IT)
Branche:	Dienstleister für Versicherungswesen und Risikomanagement
Datum:	19.12.2013 09:15 – 09:50

Interviewer: Vielen Dank, dass sie sich für das Interview Zeit genommen haben! Ich werde nun einige Fragen zu den drei verschiedenen Bereichen Risk-handling, Personal und Sicherung und Kontrolle der IT stellen. Fangen wir mit den Risiko-behandelten Fragen an.
Gibt es eine Sicherheitsverantwortliche Instanz im Unternehmen? Wenn ja, ist diese organisatorisch mit der Geschäftsführung verbunden?

H.W.: Da müssen wir natürlich differenzieren. Wenn wir von Unternehmen sprechen, dann spreche ich aus der Sicht des deutschen Teils oder dem Dachteil. Bei den weltweit über 50.000 Mitarbeitern gibt es sicherlich jemanden, der für das Thema Sicherheit verantwortlich ist (. . .). Hier in Deutschland gibt es zum einen Datenschutzbeauftragten und es gibt zum anderen jemanden der die Rolle Informationssicherheit vertritt. Dementsprechend kann man die Frage bezüglich eines Sicherheitsverantwortlichen, der mit der Geschäftsführung verbunden ist klar bejahen. (. . .) Grundsätzlich trennen wir das. Es gibt jemanden außerhalb, der mich auch (in Anführungszeichen) kontrolliert - Im Sinne eines 4-Augen Prinzips. Das ist ein Datenschutzbeauftragter, der außerhalb der IT, aber unter der Geschäftsführung ist. Die IT selbst hat natürlich auch einen Securitybeauftragten, der sich um die IT-relevanten Securityaufgaben kümmert.

I.: Ok. Würden Sie denn auch sagen, dass der Informationsschutz dementsprechend einen hohen Stellenwert hat? D.h. geht die Geschäftsführung mit gutem Beispiel voran was die Informationssicherheit angeht?

H.W.: Das Management ist auf dem Weg dorthin sich dieses Themas anzunehmen. Wir hatten zuletzt eine Holdingsitzung (. . .), und da wurde das Thema Informationssicherheit vorgestellt. Zum Beispiel haben wir präsentiert, welche Maßnahmen wir getroffen haben. Es gab vor kurzem Mal einen Sabotagefall, aufgrund dessen es heute eine hohe Awareness gibt. Dieser hat dazu geführt, dass das Informationsthema Sicherheit jetzt auch Teil der Ge-

schäftsführung wird. Es geht auf jeden Fall dort hin einen hohen Stellenwert einzunehmen.

I.: Können Sie noch etwas konkreter auf diesen Sabotagefall eingehen?

H.W.: Das einzige was ich dazu sagen kann ist, dass der Fall nicht von außen gekommen ist, sondern eher eine interne Sabotage war. Bei dem Fall spielte die Unzufriedenheit mit dem Unternehmen eine Rolle. (...) Das hat letztlich dazu geführt, dass die Awareness – „wie sicher sind meine Daten" – bis hin zum Management nochmal hochgegangen ist.

I.: Um Know-how Schutzmaßnahmen effektiv ergreifen zu können, bietet sich eine Risikoanalyse an. Inwieweit wurde bei Ihnen eine Risikoanalyse und Bewertung durchgeführt (ggf. gemäß ISO 27001)?

H.W.: Wir haben gerade erst eine Risikoanalyse gemacht, und zwar eine ISO 27001 (...) auf Basis BSI-Grundschutz. (...) Die Ergebnisse werden gerade erst zusammengestellt, sodass ich sie noch nicht alle vorliegen habe und dementsprechend noch keine Aussage treffen kann.

I.: Anschließend an so eine Analyse folgt dann ja auch eine Bewertung.

H.W.: Ja genau, und daraus ergeben sich dann Maßnahmen, aber da wir uns noch im Prozess befinden, kann ich dazu noch nichts Konkretes sagen.

I.: Aber Sie haben vor sich ISO 27001 zertifizieren zu lassen?

H.W.: Ja das ist mein Ziel, das ich gern erreichen möchte. (...) Vermutlich schaffen wir es nicht ganz für das ehmen für das ich jetzt spreche, also explizit den Bereich in Deutschland bzw. diese Region. Jedoch möchte ich erst einmal in kleinen Schritten die IT zertifizieren zu lassen. Grundsätzlich kann man die IT als einzelne Komponente nicht zertifizieren lassen, weil es immer nur im Gesamtkontext gesehen und angewandt wird. Allerdings ist der Plan, zumindest die IT in diese Richtung zu bringen, dass sie zertifizierbar wird. Ich kann ja eine Checkliste abarbeiten und dann sozusagen den Nucleus immer größer gestalten, sodass auch das gesamte Unternehmen in diese Zertifizierung reinkommt.

I.: Haben Sie da gewisse Parameter in Betracht gezogen wie Schadenshöhe und Eintrittswahrscheinlichkeit? Hatten Sie noch weitere Parameter mit einbezogen?

H.W.: Aus meiner Sicht nein. Es gibt natürlich eine Art „rough estimation", also: „was bedeutet das eigentlich / wenn . . . , dann . . . ", aber die sind relativ grob gestaltet. Dadurch besitzen

sie eigentlich keine richtige Aussagefähigkeit.

I.: Auch wenn es noch keine direkte Risikobewertung gibt, können Sie trotzdem sagen welche Bereiche die größten Risiken aufweisen könnten und werden diese in irgendeiner Form klassifiziert?

H.W.: (. . .) Die größten Risiken aus meiner Sicht befinden sich im Bereich unseres eigentlichen Businesses. Das heißt, wie geht ein Berater, ein Salesman, oder ein Kundenberater mit den sensiblen Daten des Kunden um. Zum Beispiel simpel ausgedrückt: (. . .) Wenn ein Vertrag geschlossen wird, dann liegt der Vertrag offen auf dem Tisch, sodass ihn jeder einsehen kann, der in das Büro reinkommt. Dies betrifft also auch direkt die Regularien rund um „Clean Desk" (. . .). Das ist im Moment ein klares „issue", welches uns auch wirklich sehr stark prägt. Dahingehend müssen wir gerade in diesem Bereich jetzt sehr streng darauf achten, dieses Risiko zu minimieren (. . .). Daran arbeiten wir in erster Linie auch dran. (. . .) Was die Klassifizierung angeht, so müssen die Daten wie z.B. das Vertragsdatum mit Kunden- oder Personaldaten klassifiziert werden. Also dahingehend ist es vollkommen richtig davon auszugehen, dass eine Klassifizierung her muss. Die fehlt bei uns noch.

I.: Inwieweit werden Unternehmenskooperationen als Risiko angesehen, insbesondere der Austausch von Zugangsdaten oder sensibler Informationen?

H.W.: Ja, das ganze hat auch ein gewisses Risikopotential. Da wäre zum Beispiel die Vertraulichkeitserklärung zu nennen, die immer den ersten Punkt darstellt, insbesondere wenn es um Lieferanten geht. Das haben wir aber gut im Griff. Was wir noch nicht so gut im Griff haben ist, wenn wir den Datenaustausch mit unseren Dienstleistern im Sinne von Versicherern, also im Businessumfeld haben. In diesem Bereich müssen wir noch mehr aufpassen. Da ist gerade (. . .) der Erstkontakt lockerer, sodass man häufig nicht immer sofort auf Faktoren achtet wie: Wir brauchen jetzt eine Vertraulichkeitserklärung o.ä., um dieses Risiko so niedrig wie möglich zu halten. Das wird vielleicht diskutiert, aber es wird noch nicht juristisch behandelt, also dass es z.B. gleich bei dem Erstgespräch auf dem Tisch liegt. Und das ist aus meiner Sicht ein durchaus notwendiger Punkt, an dem noch gearbeitet werden muss.

I.: Also würden Sie sagen, dass es gerade in dem Bereich dementsprechend Verbesserungspotential gibt?

H.W.: Ja, genau. Das ist erkannt und wir sind dran.

I.: Können Sie denn etwas zu Häufigkeit, Umfang oder Systematik von Cyber-Angriffen auf Ihr Unternehmen sagen?

H.W.: Offen gesagt habe ich die Statistik nicht. Ich habe auch die Sichtweise nicht, zumal wir ganz stark vom Corporate geschützt sind, bevor überhaupt jemand bei uns in das Netzwerk eindringt. (...) Wir haben ein System mit drei kaskadierenden Levels. Wir in Deutschland haben einerseits Verträge mit unserem internen Dienstleister, und unser interner Dienstleister wieder mit anderen Dienstleistern wie Verizon, Telekom usw. Die erste Ebene, die durchbrochen werden muss, ist der Provider. Dann kommt die nächste Ebene, das ist dann der interne Dienstleister der uns schützt, und dann kommen erst wir. Also wir haben auch Firewalls, die wir supporten und wo wir uns drum kümmern, aber der erste Angriff kommt immer ganz außen. Im Moment habe ich keine Einsicht in die Statistik und Häufigkeit, weil ich auch die Berichte noch nicht bekomme, was auf dieser Ebene alles passiert. (...) Das was ich auf meiner Firewall sehe, befindet sich im Rahmen, d.h. das bekommen wir bewältigt. Alles was darüber hinaus geht sehe ich jedoch nicht. (...)

I.: Gibt es (oder gab es) allgemein eine Zusammenarbeit mit Sicherheitsbehörden (Polizeilich o. Nachrichtendienstlich)? Wenn ja, in welcher Form?

H.W.: Ja, die gab es. Nehmen wir mal als Beispiel diesen Fall des Sabotageaktes. Da gab es eine Zusammenarbeit, wobei ich glaube, dass dort eher weniger mit dem Nachrichtendient kommuniziert wurde, sondern eher mit der Polizei. (...) Es gab also einen regulären Informationsaustausch und Support.

I.: Was sagen Sie zu der Meldepflicht von Cyber-Angriffen?

H.W.: Es gibt eine persönliche Meinung und vielleicht eine Meinung, die ich über die Firma vertreten muss. Meine persönliche Meinung ist: Je offener und transparenter, desto besser. Das gilt für alle anderen auch. Wenn wir einer der ersten sind, die attackiert worden sind, warum sollen wir die Information nicht weitergeben, auch um Abhilfe zu schaffen. In Bezug auf das Unternehmen würde ich eine ähnliche Strategie fahren, bloß würde ich mir überlegen, an wen ich das melde. Es gibt eine zentrale (...) Meldestelle und da geht es natürlich um den Informationsfluss. Wenn das bei uns in Deutschland passiert, muss ich natürlich zuerst intern melden, je nach Region, also entweder EMEA (Europe, Middle East and Africa) oder Corporate. Wenn ich dort gemeldet habe, dann kann ich den Informationsfluss nicht mehr steuern, und ich weiß nicht wo es am Ende landet. Landet es eher in der Corporate Region und es geht eher zu der NSA, oder passiert es auf der EMEA Ebene, dann geht es nach Großbritannien. (...) Es landet dann nicht unbedingt in Deutschland, wo

es eigentlich hin müsste. Also insofern ist die Meldepflicht ein durchaus schwieriges Thema, solange ich den Informationsfluss nicht steuern kann.

I.: Kommen wir nun zum Bereich Personal.
Inwieweit wird bei Ihnen eine Schulung / Sensibilisierung zur Förderung des Risikobewusstseins der Mitarbeiter bzgl. Umgang mit Informationen (insb. Email und Cloud, Chat / Skype) und Beachtung der Security-Policies durchgeführt?

H.W.: Es gibt auf der Unternehmensebene außerhalb der IT sogenannte Compliance Schulungen, aber weniger im Sinne von Security Themen, die mehr auf die IT bezogen sind. (. . .) Außerhalb dessen gibt es wenig, zu wenig. Das ist also auch ein Outcome aus dieser Studie auf der ISO Ebene.

I.: Und wie sieht es mit Security Policies konkret aus?

H.W.: Es gibt Security Policies bei uns. Die existieren und sind auch sehr stringent. Es gibt sozusagen ein Mitarbeiterhandbuch, das hat auch jeder und da stehen auch genau diese Dinge drin. Das fängt beim Passwort an, d.h. wie viele Stellen es haben muss und wie es auszusehen hat, bis hin zum eigentlich Umgang mit Daten.

I.: Dort werden denn Mitarbeiter auch für die Gefahren von Geschäftsreisen sensibilisiert?

H.W.: Ja, so etwas wird auch erwähnt. Nur auf der anderen Seite wird die Einhaltung noch nicht kontrolliert. Es fehlt sozusagen die Kontrollstation. Das heißt, dass man punktuell auch mal reingeht und kontrolliert, inwieweit der Mitarbeiter dies und jenes geregelt hat, wie er damit umgeht und was er eigentlich macht. Das inkludiert auch Themen wie die Geschäftsreisen und behandelt Fragen inwieweit das Notebook gesichert ist und wo es liegt. Dahingehend ist die Kontrollinstanz noch nicht ausgeprägt genug.

I.: Bieten Sie auch VPN Möglichkeiten an?

H.W.: Ja, das tun wir auch.

I.: Haben Sie formal fixierte Sicherheitsstandards wie Clean Desk Policy?

H.W.: Das bauen wir gerade auf. Das ist auch ein Outcome aus der Studie (ISO 27001) und Clean Desk ist dort sehr stark gefordert. Wir sind dabei es gerade umzusetzen.

I.: Und was ist mit Bestimmungen zur Nutzung / Vernichtung von Informationsbeständen?

H.W.: Die gibt es auch, insbesondere wenn es um Papier geht.

I.: Findet im Rahmen des Personalauswahlverfahrens eine intensive Überprüfung der Bewerber statt (insbesondere im Bereich der

IT)?

H.W.: Ich weiß es nicht. Daher kann ich nicht viel dazu sagen. (...) Das was der Mitarbeiter bekommt, wenn er eingestellt wird, ist nicht IT-spezifisch, sondern eher allgemein. Dieser NDA wird erst spezieller, wenn ich mit Lieferanten spreche.

I.: Wurde eine Schutzbedarfsanalyse durchgeführt, die für alle regelt, welche Daten / Informationen geheim, vertraulich oder offen zugänglich sind?

H.W.: Da sind wir wieder bei dem Klassifizierungsthema. (...) Es gibt natürlich den Vermerk „vertraulich" oder „streng vertraulich". Das kommt aber dann in erster Linie, wenn das Unterlagen sind, die aus dem HR-Bereich kommen oder aus dem Financial-Bereich, oder der Geschäftsführung. Aber grundsätzlich wird es eher wenig geregelt, insbesondere wenn es um jegliche Korrespondenz – auch mit Kunden – (...) geht.

I.: Ich würde jetzt zu den technischen Sicherheitsmaßnahmen übergehen.

Inwiefern wird auf das Risiko gefährdeter Datenträger (USB-drive, HDD) geachtet und spielt die Verschlüsselung von Datenträgern und Datenverkehr (insb. E-mail) bei Ihnen eine Rolle?

H.W.: USB ist ein sehr sensibles Thema. Da sind wir auch mittendrin. Bislang gibt es dort keine verschlüsselten USB-devices, die wir an unsere Mitarbeiter vergeben. Die USB-devices-Schnittstelle ist offen. Wir scannen sie natürlich mit McAfee oder anderen Tools (...). Nichtsdestotrotz ist das ein Leck, das wir gerade stark im Fokus haben. Ansonsten werden natürlich auch die Systeme, die wir rausgeben, wie z.B. Laptops beachtet. Laptops werden bei uns hochgradig verschlüsselt, sodass da auf jeden Fall Sicherheit drauf ist. Bzgl. Datenverkehr ist es so, dass wenn ein Kunde zum Beispiel verschlüsselten E-Mailverkehr fordert, wir dann Cryptshare einsetzen. Das ist ein Stück „device", das genau diesen Datentransfer zwischen den beiden Parteien regelt.

I.: Wie sehen die (auch räumlichen) Zutritts- und Zugriffsberechtigungskonzepte (insb. Zugang zum Rechenzentrum) für sowohl firmeneigenes als auch firmenfremdes Personal bzgl. gefährdeten Daten und Objekten aus? Ich habe am Empfang erfahren, dass Besucher einfach so keinen Zutritt erhalten, d.h. sie brauchen eine Zutrittskarte und ggf. eine Begleitperson.

H.W.: Ja genau. Es wird darauf geachtet, dass Personen sich vorab anmelden müssen (...). In der IT ist z.B. die Tür ab 17 Uhr zu, sodass man dort auch nur rein kommt, wenn man den entsprechenden Ausweis (Zugangskarte) hat. Bei Reinigungskräften ist es so,

dass einige Zugang haben und einige nicht. Wir achten da schon darauf, aber es könnte auch sicherlich noch besser sein. Zum Beispiel, dass jeder Mitarbeiter eine „badge" trägt und man ihn dadurch direkt identifizieren (Name, Bild) kann. (. . .)Zurzeit ist es so, dass wenn ich das liegen lasse, dann auch sie theoretisch damit rein könnten. Dahingehend besteht dort noch Handlungsbedarf. (. . .) Die Zutritte werden natürlich auch alle mitgeloggt. (. . .) Beim Rechenzentrum können nur vereinzelt Leute rein. Wir planen, zu der „badge" auch noch einen PIN Code einzuführen. (. . .) Was auch noch kommen wird, ist Videoüberwachung. Das ist etwas, was wir auch aus der Bewertung ableiten und das ist gerade schon in Umsetzung.

I.: Wie oft gibt es einen systematischen Passwortwechsel und gibt es diesbezüglich Regelungen (z.B. minimale Anzahl an Stellen)?

H.W.: Ja, alle 60 Tage, (. . .) bei allen Mitarbeitern, (. . .) und inklusive Regelungen bzgl. Minimalstellen usw. Auf den Devices, den Domänen, den Applikationen und auch bei Laptops wird darauf geachtet, dass alles passwortgeschützt ist.

I.: Inwieweit verfügen Sie über Schutzmechanismen wie Firewall, Anti-Virus und Anti-Spam Software? Findet bei Ihnen ein Intrusion Detection System Verwendung?

H.W.: Ein Intrusion Detection System haben wir mittlerweile auch. Firewall und eigentlich alles, was sich um McAfee so rankt.

I.: Also glauben Sie, gerade in diesem Bereich technischer Schutzmaßnahmen sehr gut aufgestellt zu sein?

H.W.: Da sind wir gut aufgestellt. Ich würde sagen wird fangen 95% bestimmt ab. Ich weiß nicht wo die restlichen 5% landen, (. . .) aber solange ich hier bin, ist noch keine „detection" gewesen.

I.: Gehen Sie vielleicht soweit mit den Schutzmaßnahmen, dass Sie USB-Zugänge oder CD Laufwerke entfernen?

H.W.: Das ist auch wieder eine Anforderung, die im Zuge der ISO behandelt wird. Wenn ein Kunde danach fragt, ob wir zertifiziert sind, gerade in Bezug auf Informationssicherheit, dann ist damit inkludiert, dass z.B. USB-devices abgeschottet sind, also dass nicht jeder sich daran klemmen kann. (. . .) Das kommt immer mehr, gerade im Financial Service Umfeld, dass so etwas angefragt wird. Also ganz sensibel ist da einer unserer Unternehmensbereiche (. . .), der auch sehr stark mit Personaldaten arbeitet. Die machen auch Personal-Outsourcing, d.h. sie übernehmen Tätigkeiten für Kunden, und wenn diese Kunden dann zu uns kommen, fragen sie gerade nach diesen Standards.

I.: Werden Ihre IT-Systeme regelmäßigen Updates unterzogen?

H.W.: Es wird immer zuerst getestet und dann geben wir es raus. Es

wird nicht automatisiert gemacht, direkt wenn von Microsoft die Patches kommen, sondern erst einmal wird getestet. Darauf folgt ein wöchentlich durchgeführtes Patchdeployment, wo die Patches dann weitergegeben werden.

I.: Gibt es regelmäßige (un-)angekündigte Prüfungen auf Umsetzung und Effizienz der Schutzmaßnahmen (z.B. Penetrationstests durch interne Stellen oder externe Dienstleister), wenn ja, wie oft?

H.W.: Das ist genau das was ich vorhin angesprochen habe bzgl. der fehlenden Kontrollinstanz. Es gibt ein regelmäßiges Audit bei uns, welches SOX-getrieben ist. Da werden auch Security-Fragen angerissen. Aber ein stringentes kontrollieren, und auch bis zum Mitarbeiter runter, d.h. wie geht er mit den Daten um, existiert noch nicht. (. . .) Und das fehlt wahrscheinlich deswegen, weil diese Klassifizierung auf der Datenebene noch nicht da ist. In diesem Bereich ist noch erkannter Handlungsbedarf.

I.: Also gab es auch nie Penetrationstests durch interne oder externe Dienstleister?

H.W.: Doch, wir führen monatlich Penetrationstests intern durch. (. . .)

I.: Da sie ja gerade noch im Prozess der Anwendung des ISO 27001 Standards sind . Können Sie eine Schätzung abgeben, wie lange der Prozess von der Analyse bis hin zu der Ableitung von Maßnahmen dauert?

H.W.: Also bevor man eine 27000-er Zertifizierung hat, dauert das in der Regel zwischen 2 und 3 Jahren, weil ja der gesamte Unternehmensbereich angesprochen wird, bis hin zu Clean Desk und dem Umgang mit Daten. Aus IT-Sicht schafft man das bestimmt schneller. Ich denke wir sind in dem nächsten halben oder dreiviertel Jahr in der Umsetzung so weit, dass solche Themen, die wir eben diskutiert haben, wir auch abgestellt haben. (. . .) Bis wir in die regelmäßige Kontrolle bis hin zum Endmitarbeiter hinein kommen, glaube ich, dass das eher wieder zu den 2-3 Jahren gehört. Das wird also noch ein bisschen dauern. Also eine organisatorische Umsetzung, wo dann am Ende des Tages dann auch der Betriebsrat gefragt und das Personalwesen gefordert sind, dass die Ordnung im Betrieb hergestellt wird. Diese Abstimmung dauert in der Regel sehr lange.

I.: Wie schätzen Sie bei Ihnen die Risiken des ungewollten Know-how-Abflusses mit der zunehmenden Verwendung mobiler (und leistungsstarker) Geräte wie Tablets und Smartphones ein?

H.W.: Beziehe ich das erstmal nur auf meine IT, dann würde ich sagen eher gering. Da weiß jeder Mitarbeiter, dass es sensible Daten sind. Im Business (. . .) könnte ich mir auch vorstellen, dass

jemand Firmenmails an seinen privaten Account schickt, nur um das vielleicht zuhause zu lesen o.ä. (...) Wie groß das Risiko auf das Unternehmen bezogen ist, ist aus meiner Sicht nicht allzu groß. Ich glaube, dass wir das ganz gut im Griff haben. Also ich glaube nicht, dass die Mitarbeiter das auch irgendwie weiter verwenden, insbesondere Kundendaten o.ä. (...) Anders rum formuliert. Wenn das so sensibel wäre, dann hätte die Geschäftsführung eine wesentlich höhere Awareness darauf. Und weil sie relativ gering ist, scheint das noch nicht ein Thema zu sein.

I.: Also gibt es bei Ihnen auch keine Regelungen bzgl. Auswahl der Betriebssysteme der Geräte?

H.W.: Doch, das gibt es schon. Die Auswahl der Systeme gibt es, das grenzen wir ein. (...). Also im Moment halten wir uns noch an das Thema Apple und das Thema Microsoft. D.h. das ist dahingehend schon eingegrenzt. Je größer die Vielfalt nachher ist, desto schwieriger ist es dann auch das ganze zu handhaben. (...) Es heißt nicht, dass ich nicht mal was bei Android ausprobiert habe, aber im Business, gerade wenn es auch um Informationssicherheit geht, beschränken wir uns in der Anwendung nur auf iOS und Microsoft.

I.: Inwieweit finden externe Cloud-Lösungen (GoogleDrive, Dropbox usw.) bei Ihnen Verwendung?

H.W.: Weder Dropbox noch GoogleDrive werden bei uns verwendet. Ich möchte natürlich vermeiden, dass meine Daten ins Ausland gehen. Als Alternative haben wir natürlich so eine Art Dropbox, die heißt bei uns HiDrive. (...) Die Daten liegen da in Deutschland. Wir brauchen natürlich immer auch für die mobilen Devices eine Art Austauschmedium. Woran ich allerdings arbeite, ist das ganze bei uns in-zu-sourcen, also die Daten hier bei uns zu halten. Bei uns heißt das ganze DMZ (...), also, dass man von außen auch auf unsere DMZ, also die Demilitarisierte Zone aufsetzen kann und auch die Daten austauschen kann. Ich möchte die Daten bei uns intern haben (...). Ich halte grundsätzlich nicht so viel davon die Daten weg zu geben. Wenn, dann in einem begrenzten Umfeld, vertraglich geregelt und nicht bitteschön in eine Dropbox, die vielen Menschen zugänglich ist. (...) Es geht also hin zu einer eigenen privaten Cloud-Lösung, die innerhalb des Konzerns ist.

I.: Im Zuge der letzten Meldungen zu Abhörpraktiken wurde bekannt, dass angeblich Hintertüren in kommerzielle Software eingebaut wurde. Wäre die Verwendung von non-Amerikanischer Software oder von Open-Source Produkten - wenn noch nicht der Fall - eine

mögliche Alternative für Sie?

H.W.: Da wir ein amerikanischer Konzern sind, erübrigt sich die Frage eigentlich. Ich würde die Einschränkung auch nicht treffen. Wir sind mittlerweile ja auch soweit, dass amerikanische Software, schon quasi überall, auch bei den iOS Geräten (. . .) ist. Daher kann ich es auch nicht einfach ignorieren. Es mangelt auch an Alternativen. (. . .) Nehmen wir mal das Open Source Produkt Linux. Das hat ja mittlerweile Einzug gehalten und es wird ja auch von den Firmen, mit denen ich ja auch wieder eine vertragliche Regelung treffen kann, vertrieben. Also insofern hat es dort schon einen Einzug gehalten. Wenn es nun ganz Open Source ist, dann wird es bei uns keinen Einzug halten, denn das wird nicht funktionieren. Ich brauche immer den Hersteller, der mir die Software gibt und der mich auch mit updates versorgt. Und ich muss natürlich auch ein vertragliches Verhältnis mit dem Hersteller eingehen. Auch sind wir nun keine Softwareentwickler, (. . .) die vielleicht anders damit umgehen. (. . .)

I.: Nochmal bettreffend der letzten Meldungen zu Abhörpraktiken: Haben Sie sich da allgemein bei Ihnen im Unternehmen damit befasst? Gerade im Hinblick auf die Informationssicherheit.

H.W.: Die Diskussion kommt, aber sie wird nicht so intensiv geführt, wie das in den Medien dargestellt wird. (. . .)

I.: Hat Ihr Haus eine Versicherung zum Schutz gegen Spionage abgeschlossen (z.B. Cyber-, Vertrauensschaden-, Computermissbrauchsversicherung)?

H.W.: Über die Existenz einer solchen Versicherung wissen wir Bescheid, aber meines Wissens wird so etwas von uns zurzeit nicht angeboten. (. . .)

I.: Damit wären wir am Ende des Interviews. Herzlichen Dank!

CHAPTER 13

Appendix: Overview of intelligence services

Table 13.1: List of the most relevant intelligence services, which appeared in this thesis.

Country	Name	Staff	Budget	Formed
Australia[a]	Australian Secret Intelligence Service (**ASIS**)	classified	$162.5m (2007)	13.05.1952
Canada[b]	Communications Security Establishment Canada (**CSEC**)	2,000 (2012)	$350m (2012)	1946
Germany[c,d]	Bundesnachrichtendienst (**BND**)	6,050 (2009)	classified[e,f]	01.04.1956
	Bundesamt für Verfassungsschutz (**BfV**)	2,757 (2012)	€210m (2012)	07.11.1950
France[g,h]	Direction générale de la sécurité extérieure (**DGSE**)	4,620 (2007)	€543.8m (2009)	02.04.1982
New Zealand[i,j]	Government Communications Security Bureau (**GCSB**)	300 (2012)	$64m (2012)	1977
Russia[k]	Federal Security Service of the Russian Federation (**FSB**)	350,000 (2006)	classified	03.04.1995
United Kingdom[l,m]	Government Communications Headquarters (**GCHQ**)	5,675 (2010)	classified[n,o]	1919
	Secret Intelligence Service (**SIS**) = **MI6**	classified	classified	1909
	Security Service = **MI5**	3,800 (2012)	classified	1909
USA[p]	Central Intelligence Agency (**CIA**)	21,459 (2013)	$14.7bn (2013)	18.09.1947
	National Security Agency (**NSA**)	14,950 (2013)	$10.8bn (2013)	04.11.1952

[a] [7]
[b] [70]
[c] [17]
[d] [53]
[e] estimated to amount for around €400m
[f] [216]
[g] [7]
[h] [18]
[i] [128]
[j] [9]
[k] [7]
[l] [105]
[m] [31]
[n] funded by Single Intelligence Account (SIA). Total budget for the 3 agencies amounts for £2.1bn (2013)
[o] [8]
[p] [2]

Bibliography

[1] Ausgabe 09/2013 (25.02.2013). Cyber-spionage: Chinesische hacker greifen eads und thyssenkrupp an. http://www.spiegel.de/netzwelt/web/it-sicherheit-chinesische-hacker-greifen-eads-und-thyssenkrupp-an-a-885189.html, 2013. Accessed: 2013-07-14.

[2] Steven Aftergood. Intelligence budget data. http://www.fas.org/irp/budget/index.html, 2013. Accessed: 2013-10-08.

[3] ALPBACH/WB. Österreich nimmt den Kampf um die Cyber-Sicherheit auf. *Die Presse*, 2013.

[4] Marc Ambinder. What's xkeyscore? https://theweek.com/article/index/247684/whats-xkeyscore, 2013. Accessed: 2013-10-08.

[5] Jacob Appelbaum, Nikolaus Blome, Hubert Gude, Ralf Neukirch, Rene Pfister, Laura Poitras, Marcel Rosenbach, Jörg Schindler, Gregor P. Schmitz, and Holger Stark. Der unheimliche freund. *Der Spiegel - Ausgabe 44/2013*, 44:21–26, 2013.

[6] No author. Gesetz zur beschränkung des brief-, post- und fernmeldegeheimnisses (artikel 10-gesetz - g 10). http://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html, 2001. Accessed: 2013-11-22.

[7] No author. The 10 best intelligence agencies in the world. http://www.smashinglists.com/10-best-intelligence-agencies-in-the-world/, 2010. Accessed: 2013-10-08.

[8] No author. Funding and financial controls. https://www.sis.gov.uk/about-us/legislation-and-accountability/funding-and-financial-controls.html, 2011. Accessed: 2013-10-08.

[9] No author. History of the gcsb. http://www.gcsb.govt.nz/about-us/history.html, 2011. Accessed: 2013-10-08.

[10] No author. Gamma international. http://surveillance.rsf.org/en/gamma-international/, 2012. Accessed: 2013-08-12.

[11] No author. Android pushes past 80leap 156.0 http://www.idc.com/getdoc.jsp?containerId=prUS24442013, 2013. Accessed: 2013-11-15.

[12] No author. Belgacom attack: Britain's gchq hacked belgian telecoms firm. http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html, 2013. Accessed: 2013-10-20.

[13] No author. Überwachung: Bnd leitet massenhaft metadaten an die nsa weiter. http://www.spiegel.de/netzwelt/netzpolitik/bnd-leitet-laut-spiegel-massenhaft-metadaten-an-die-nsa-weiter-a-914682.html, 2013. Accessed: 2013-08-04.

[14] No author. Überwachung: Nsa späht internationalen zahlungsverkehr aus. http://www.spiegel.de/netzwelt/netzpolitik/nsa-spaeht-internationalen-zahlungsverkehr-aus-a-922283.html, 2013. Accessed: 2013-10-20.

[15] No author. Bnd selbst im besitz von prism-technik. http://www.mdr.de/fakt/bnd-und-prism100.html, 2013. Accessed: 2013-10-08.

[16] No author. China blamed after asio blueprints stolen in major cyber attack on canberra hq. http://www.abc.net.au/news/2013-05-27/asio-blueprints-stolen-in-major-hacking-operation/4715960, 2013. Accessed: 2013-09-23.

[17] No author. Confidential committee. http://www.bnd.bund.de/EN/Scope_of_Work/Supervision_and_Control/Confidential_Committee/Confidential_Committee_node.html, 2013. Accessed: 2013-10-08.

[18] No author. D. le renseignement de securitÉ. http://www.senat.fr/rap/a08-102-4/a08-102-42.html, 2013. Accessed: 2013-10-08.

[19] No author. Dates when prism collection began for each provider. http://static.guim.co.uk/sys-images/Guardian/Pix/audio/video/2013/6/6/1370553948414/Prism-001.jpg, 2013. Accessed: 2013-11-22.

[20] No author. Financial times lexicon. http://lexicon.ft.com/Term?term=cyber, 2013. Accessed: 2013-08-03.

[21] No author. Google transparenzbericht - verbreitung von malware nach autonomem system. http://www.google.com/transparencyreport/safebrowsing/malware/, 2013. Accessed: 2013-10-21.

[22] No author. Information on iso/iec 27001:2013. http://www.iso27001security.com/html/27001.html, 2013. Accessed: 2013-10-15.

[23] No author. Interview mit edward snowden: Nsa liefert bnd werkzeuge für lauschangriff. http://www.spiegel.de/politik/ausland/interview-mit-edward-snowden-im-spiegel-nsa-und-bnd-arbeiten-zusammen-a-909800.html, 2013. Accessed: 2013-07-07.

[24] No author. Mapa mostra volume de rastreamento do governo americano. http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/, 2013. Accessed: 2013-10-08.

[25] No author. Neue nsa-dokumente: Us-geheimdienst hörte zentrale der vereinten nationen ab. http://www.spiegel.de/politik/ausland/nsa-hoerte-zentrale-der-vereinte-nationen-in-new-york-ab-a-918421.html, 2013. Accessed: 2013-10-20.

[26] No author. Nsa files - decoded. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded, 2013. Accessed: 2013-11-02.

[27] No author. Nsa slides explain the prism data-collection program. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/, 2013. Accessed: 2013-10-08.

[28] No author. Procedures used by nsa to minimize data collection from us persons: Exhibit b – full document. http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document, 2013. Accessed: 2013-10-19.

[29] No author. Serie wirtschaftsspionage. http://www.auwi-bayern.de/awp/inhalte/weitereNavigation/Serie-Wirtschaftsspionage/index.html, 2013. Accessed: 2013-10-01.

[30] No author. Spähangriff auf belgacom: Britischer geheimdienst hackte belgische telefongesellschaft. http://www.spiegel.de/netzwelt/web/belgacom-geheimdienst-gchq-hackte-belgische-telefongesellschaft-a-923224.html, 2013. Accessed: 2013-10-20.

[31] No author. Staff and management. https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management.html, 2013. Accessed: 2013-10-08.

[32] No author. Us-geheimdienst: Nsa führt deutschland als spionageziel. http://www.spiegel.de/politik/ausland/nsa-fuehrt-deutschland-als-spionageziel-a-915871.html, 2013. Accessed: 2013-10-18.

[33] No author. Verizon forced to hand over telephone data – full court ruling. http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order, 2013. Accessed: 2013-10-08.

[34] No author. Was ist ein kmu? http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_de.htm, 2013. Accessed: 2013-12-20.

[35] No author. Wenn malware mobil wird. http://www.sophos.com/de-de/security-news-trends/security-trends/malware-goes-mobile/why-ios-is-safer-than-android.aspx, 2013. Accessed: 2013-11-15.

[36] No author. Xkeyscore presentation from 2008 – read in full. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2013. Accessed: 2013-10-08.

[37] James Ball and Spencer Ackerman. Nsa loophole allows warrantless search for us citizens' emails and phone calls. http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls, 2013. Accessed: 2013-10-19.

[38] Byrnes Barrett, Silverman. The ssh protocol. http://www.snailbook.com/protocols.html, 2013. Accessed: 2013-11-15.

[39] Behrends, Johannes. Cyber-versicherungen haben eine große zukunft. Insurance Business Report - Versicherungswirtschaft - Sonderdruck 02/2013, 2013. Accessed: 2013-12-20.

[40] Detlef Borchers. Nsa-Überwachungsskandal: Arbeitet der bnd mit prism-software? http://www.heise.de/newsticker/meldung/NSA-Ueberwachungsskandal-Arbeitet-der-BND-mit-PRISM-Software-1919184.html, 2013. Accessed: 2013-10-08.

[41] Brainloop AG. Studie: Industriespionage 2012. http://corporate-trust.de/pdf/CT-Studie-2012_FINAL.pdf, 2012. Accessed: 2013-08-28.

[42] Nick Browning, Markus Krisetya, Larry Lairson, and Alan Mauldin. Submarine cable map 2013. http://submarine-cable-map-2013.telegeography.com/, 2013. Accessed: 2013-09-21.

[43] BSI. Iso 27001-zertifizierung auf der basis von it-grundschutz. http://blog.iso27001standard.com/2013/09/09/is-iso-27001-among-the-top-iso-standards/, 2013. Accessed: 2013-10-15.

[44] Daniel Chechik. Look what i found: Moar pony! http://blog.spiderlabs.com/2013/12/look-what-i-found-moar-pony.html?utm_source=dlvr.it&utm_medium=twitter, 2013. Accessed: 2013-12-04.

[45] Per Christensson. Rootkit. http://www.techterms.com/definition/rootkit, 2010. Accessed: 2013-10-08.

[46] Citizen Lab. Planet blue coat mapping global censorship and surveillance tools. https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/, 2013. Accessed: 2013-10-03.

[47] James R. Clapper. Statement by director of national intelligence james r. clapper on allegations of economic espionage. http://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence, 2013. Accessed: 2013-10-22.

[48] Richard A. Clarke and Robert K. Knake. *World Wide War*. Hoffmann und Campe, 1. edition, 2011.

[49] M. Andrew Colarik. *Cyber Terrorism: Political and Economical Implications*. Idea Group Publishing, 1. edition, 2006.

[50] Lucian Constantin. One in five data breaches are the result of cyberespionage, verizon says. http://news.idg.no/cw/art.cfm?id=0AF23856-CBA1-9BB9-091C4CC035F4D209, 2013. Accessed: 2013-11-22.

[51] cpo. Verfassungsschutz fordert besseren schutz vor wirtschaftsspionage. http://www.heise.de/newsticker/meldung/Verfassungsschutz-fordert-besseren-Schutz-vor-Wirtschaftsspionage-1228903.html, 2011. Accessed: 2013-07-05.

[52] Bundesministerium der Justiz und für Verbraucherschutz. § 42a informationspflicht bei unrechtmäßiger kenntniserlangung von daten. http://www.gesetze-im-internet.de/bdsg_1990/__42a.html, 2011. Accessed: 2013-09-12.

[53] Bundesministerium des Innern. Verfassungsschutzbericht 2012. http://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte/vsbericht-2012, 2012. Accessed: 2013-10-08.

[54] Florian Diekmann. Reaktion auf cyber-attacken: Usa drohen bei hacker-angriffen mit handelskrieg. http://www.spiegel.de/wirtschaft/soziales/usa-drohen-china-wegen-cyber-angriffen-mit-sanktionen-und-handelskrieg-a-884412.html, 2013. Accessed: 2013-07-04.

[55] Philip Dorling. Australian spies in global deal to tap undersea cables. http://www.theage.com.au/technology/technology-news/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html, 2013. Accessed: 2013-10-08.

[56] Philip Dorling. Australian spy agency helped bhp negotiate trade deals. http://www.smh.com.au/national/australian-spy-agency-helped-bhp-negotiate-trade-deals-20131106-2x1sw.html, 2013. Accessed: 2013-11-08.

[57] Philip Dorling. Snowden reveals australia's links to us spy web. http://www.theage.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html, 2013. Accessed: 2013-10-08.

[58] dpa. „keine nsa-wirtschaftsspionage in deutschland". http://www.handelsblatt.com/politik/deutschland/verfassungsschutz-chef-maassen-keine-nsa-wirtschaftsspionage-in-deutschland/8700868.html, 2013. Accessed: 2013-08-29.

[59] Emma Draper. Privacy international commences legal action against british government for failure to control exports of surveillance technologies. https://www.privacyinternational.org/press-releases/privacy-international-commences-legal-action-against-british-government-for-failure, 2012. Accessed: 2013-08-12.

[60] DuckDuckGo. Dont track us. http://donttrack.us/?kad=en_GB, 2013. Accessed: 2013-10-05.

[61] Symantec employee. W32.duqu: The precursor to the next stuxnet. http://www.symantec.com/connect/de/w32_duqu_precursor_next_stuxnet, 2011. Accessed: 2013-09-24.

[62] Symantec employee. Flamer: Highly sophisticated and discreet threat targets the middle east. http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east, 2012. Accessed: 2013-09-24.

[63] ENISA. Eu cyber cooperation - the digital frontline. http://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2012/eu-cyber-cooperation-the-digital-frontline/at_download/fullReport, 2012. Accessed: 2013-10-02.

[64] European Court of Human Rights. European convention on human rights. www.echr.coe.int/Documents/Convention_ENG.pdf, 2000. Accessed: 2013-07-29.

[65] European Defence Agency. Cyber defence factsheet. http://www.eda.europa.eu/docs/default-source/eda-factsheets/cyber-defence-factsheet, 2013. Accessed: 2013-07-29.

[66] European Union. Charter of fundamental rights of the european union. www.europarl.europa.eu/charter/pdf/text_en.pdf, 2000. Accessed: 2013-07-29.

[67] Inc. FireEye. Fireeye advanced threat report – 2h 2012. http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2h2012.pdf, 2013. Accessed: 2013-07-16.

[68] Max Fisher. Eric schmidt, in new book: China could contribute to fracturing the internet into pieces. http://www.washingtonpost.com/blogs/worldviews/wp/2013/02/03/eric-schmidt-in-new-book-china-could-contribute-to-fracturing-the-internet-into-pieces/, 2013. Accessed: 2013-09-03.

[69] European Union Agency for Network and Information Security. Enisa threat landscape, mid-year 2013. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013/at_download/fullReport, 2013. Accessed: 2013-11-04.

[70] Colin Freeze and Stephanie Nolen. Charges that canada spied on brazil unveil csec's inner workings. http://www.theglobeandmail.com/news/world/brazil-spying-report-spotlights-canadas-electronic-eavesdroppers/article14720003/, 2013. Accessed: 2013-10-08.

[71] Friederike Freiburg, Reuters, and Valerie Wagner. Spähskandal: Auch frankreichs geheimdienst zapft massenhaft daten ab. http://www.spiegel.de/politik/deutschland/auch-frankreichs-geheimdienst-zapft-massenhaft-daten-ab-a-909501.html, 2013. Accessed: 2013-10-19.

[72] Craig Freudenrich. How fiber optics work. http://computer.howstuffworks.com/fiber-optic4.htm, 2013. Accessed: 2013-10-11.

[73] Brian Fung. A hypnotic visualization of everything gmail knows about you and your friends. http://www.nationaljournal.com/tech/a-hypnotic-visualization-of-everything-gmail-knows-about-you-and-your-friends-20130705, 2013. Accessed: 2013-10-19.

[74] Christian Funk and Denis Maslennikov. It threat evolution: Q2 2013. http://www.securelist.com/en/analysis/204792299/IT_Threat_Evolution_Q2_2013, 2013. Accessed: 2013-09-26.

[75] fX. Eu sagt cyberkriminalität den kampf an – entwurf fast fertig. http://www.basicthinking.de/blog/2013/01/18/eu-sagt-cyberkriminalitat-den-kampf-an-entwurf-fast-fertig/, 2013. Accessed: 2013-09-12.

[76] Pravin Ganore. Submarine cable and the internet. http://blog.esds.co.in/submarine-cable-and-the-internet/, 2013. Accessed: 2013-09-21.

[77] Florian Gathmann, dpa, and Reuters. Deutsche prism-erkenntnisse: Friedrich muss angaben zu anschlagsplänen relativieren. http://www.spiegel.de/politik/deutschland/innenminister-friedrich-geraet-in-die-defensive-a-911232.html, 2013. Accessed: 2013-10-29.

[78] Matthias Gebauer. Cyberspionage: Bnd gründet neue abteilung zur abwehr von hackerangriffen. http://www.spiegel.de/netzwelt/netzpolitik/bnd-gruendet-neue-abteilung-zur-abwehr-von-hackerangriffen-a-890616.html, 2013. Accessed: 2013-09-12.

[79] Barton Gellman. Nsa broke privacy rules thousands of times per year, audit finds. http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html, 2013. Accessed: 2013-10-19.

[80] Barton Gellman and Todd Lindeman. Inner workings of a top-secret spy program. http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/, 2013. Accessed: 2013-10-08.

[81] Barton Gellman and Greg Miller. U.s. spy network's successes, failures and objectives detailed in 'black budget' summary. http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html, 2013. Accessed: 2013-10-21.

[82] Barton Gellman and Ellen Nakashima. U.s. spy agencies mounted 231 offensive cyber-operations in 2011, documents show. http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration, 2013. Accessed: 2013-09-24.

[83] Barton Gellman and Ellen Nakashima. U.s. spy agencies mounted 231 offensive cyber-operations in 2011, documents show. http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html, 2013. Accessed: 2013-09-01.

[84] Barton Gellman and Laura Poitras. U.s., british intelligence mining data from nine u.s. internet companies in broad secret program. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html, 2013. Accessed: 2013-10-20.

[85] Jan Goldman. *Words of Intelligence: A Dictionary*. The Scarecrow Press, Inc., 1. edition, 2006.

[86] Whitson Gordon. Wolfram alpha's facebook report analyzes every dark corner of your facebook activity. http://lifehacker.com/5939392/wolfram-alphas-facebook-report-analyzes-ever-dark-corner-of-your-facebook-activity, 2012. Accessed: 2013-10-19.

[87] Siobhan Gorman and Jennifer Valentino-DeVries. New details show broader nsa surveillance reach. http://online.wsj.com/news/articles/SB10001424127887324108204579022874091732470, 2013. Accessed: 2013-10-20.

[88] Alexander Gostev. The flame: Questions and answers. http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers, 2012. Accessed: 2013-09-24.

[89] D.B. Grady. Inside the secret world of america's top eavesdropping spies. http://theweek.com/article/index/226723/inside-the-secret-world-of-americas-super-sophisticated-eavesdropping-spies, 2012. Accessed: 2013-10-08.

[90] Glenn Greenwald. Nsa collecting phone records of millions of verizon customers daily. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, 2013. Accessed: 2013-10-08.

[91] Glenn Greenwald. Xkeyscore: Nsa tool collects 'nearly everything a user does on the internet'. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, 2013. Accessed: 2013-10-08.

[92] Glenn Greenwald and Ewen MacAskill. Boundless informant: the nsa's secret tool to track global surveillance data. http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining, 2013. Accessed: 2013-10-08.

[93] Glenn Greenwald and Ewen MacAskill. Nsa prism program taps in to user data of apple, google and others. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, 2013. Accessed: 2013-10-08.

[94] Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe. Microsoft handed the nsa access to encrypted messages. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data, 2013. Accessed: 2013-10-08.

[95] Christian Götz. Intrusion detection systeme im vergleich. http://www.securitymanager.de/magazin/intrusion_detection_systeme_im_vergleich.html, 2004. Accessed: 2013-10-21.

[96] Thomas Gutschker, Maria K. Wagner, and Markus Wehner. Amerika darf deutsche abhören. http://www.faz.net/aktuell/politik/inland/geheimdienst-affaere-amerika-darf-deutsche-abhoeren-12273496.html, 2013. Accessed: 2013-07-07.

[97] Handelsblatt. Die unterschätzte Gefahr. *Handelsblatt*, 2013.

[98] Claus Hecking. Spähangriff auf belgacom: Telefonanbieter der europäischen union gehackt. http://www.spiegel.de/netzwelt/web/spaehangriff-auf-eu-telefonanbieter-belgacom-a-922555.html, 2013. Accessed: 2013-10-20.

[99] Michail Hengstenberg. Nsa-affäre: 'champagner!'. http://www.spiegel.de/netzwelt/netzpolitik/nsa-kann-auch-iphone-blackberry-und-android-telefone-auslesen-a-920963.html, 2013. Accessed: 2013-10-20.

[100] Gamma Group Homepage. https://www.gammagroup.com/. Accessed: 2013-11-22.

[101] Nick Hopkins and Julian Borger. Exclusive: Nsa pays £100m in secret funding for gchq. http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden, 2013. Accessed: 2013-10-22.

[102] Judith Horchert. Hackertreffen in köln: Sie haben uns doch gewarnt. http://www.spiegel.de/netzwelt/netzpolitik/sigint-2013-sie-haben-uns-doch-gewarnt-a-909705.html, 2013. Accessed: 2013-10-29.

[103] Hutchins, M. Eric and Cloppert, J. Michael and Amin, M. Rohan. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. https://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Security/Meetings/ISOAG/2012/Sept_ISOAG_NetworkDefense.pdf, 2010. Accessed: 2013-09-17.

[104] Mikko Hypponen. Finfisher range of attack tools. http://www.f-secure.com/weblog/archives/00002601.html, 2013. Accessed: 2013-09-02.

[105] Intelligence and Security Committee. Annual report 2010–2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211561/isc-annualreport1011.pdf, 2011. Accessed: 2013-10-08.

[106] J. Lech Janczewski and M. Andrew Colarik. *Cyber Warfare and Cyber Terrorism*. Information Science Reference, 1. edition, 2008.

[107] Cory Janssen. Honeypot. http://www.techopedia.com/definition/10278/honeypot, 2013. Accessed: 2013-11-22.

[108] Cory Janssen. Two-factor authentication. http://www.techopedia.com/definition/13699/twofactor-authentication, 2013. Accessed: 2013-11-22.

[109] Myriam Joire. Researchers create hollow fiber optic cable, almost reach the speed of light. http://www.engadget.com/2013/03/26/researchers-create-hollow-fiber-optic-cable-almost-reach-the-sp/, 2013. Accessed: 2013-10-11.

[110] Kaspersky Lab. The nettraveler (aka 'travnet'). http://www.securelist.com/en/downloads/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf, 2013. Accessed: 2013-09-18.

[111] Kaspersky Lab. Red october: Diplomatic cyber attacks investigation. http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation, 2013. Accessed: 2013-09-02.

[112] Kaspersky Lab. Winnti - more than just a game. http://www.securelist.com/en/downloads/vlpdfs/winnti-more-than-just-a-game-130410.pdf, 2013. Accessed: 2013-09-21.

[113] Meghan Keneally. Yahoo ceo marissa mayer reveals she feared committing treason over nsa scandal and mark zuckerberg thinks the government blew it with the surveillance. http://www.dailymail.co.uk/news/article-2419441/Yahoo-CEO-Marissa-Mayer-feared-sent-jail-treason-NSA-scandal.html, 2013. Accessed: 2013-10-08.

[114] Gerry Kennedy. Universal access to text using speech recognition. http://www.spectronicsinoz.com/article/universal-access-to-text-using-speech-recognition, 2009. Accessed: 2013-07-01.

[115] Joe Kloc. Forget prism: Fairview is the nsa's project to 'own the internet'. http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/, 2013. Accessed: 2013-10-20.

[116] Dejan Kosutic. Is iso 27001 among the top iso standards? http://blog.iso27001standard.com/2013/09/09/is-iso-27001-among-the-top-iso-standards/, 2013. Accessed: 2013-10-15.

[117] Stefan Krempl. Innenministerium macht ernst mit meldepflicht nach cyberangriffen. http://www.heise.de/security/meldung/Innenministerium-macht-Ernst-mit-Meldepflicht-nach-Cyberangriffen-1818361.html, 2013. Accessed: 2013-09-12.

[118] Philipp Krohn. Gute fahrer sollen weniger prämie zahlen. http://www.faz.net/aktuell/finanzen/meine-finanzen/versichern-und-schuetzen/autoversicherung-gute-fahrer-sollen-weniger-praemie-zahlen-12655209.html, 2013. Accessed: 2013-11-10.

[119] Kroll, Lars. Herausforderung Unternehmenssicherheit. Private Contact, 2013. Accessed: 2013-12-20.

[120] Constanze Kurz. Die menschenrechte sollen es richten. http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/aus-dem-maschinenraum-die-menschenrechte-sollen-es-richten-12602024.html, 2013. Accessed: 2013-10-19.

[121] Lana Lam. Edward snowden: Us government has been hacking hong kong and china for years. http://www.scmp.com/news/hong-kong/article/1259508/edward-snowden-us-government-has-been-hacking-hong-kong-and-china, 2013. Accessed: 2013-10-19.

[122] Lana Lam and Stephen Chen. Exclusive: Snowden reveals more us cyberspying details. http://www.scmp.com/news/hong-kong/article/1266777/exclusive-snowden-safe-hong-kong-more-us-cyberspying-details-revealed, 2013. Accessed: 2013-10-19.

[123] Jaron Lanier. Digital passivity. http://www.nytimes.com/2013/11/28/opinion/digital-passivity.html?_r=0, 2013. Accessed: 2013-11-28.

[124] Carol D. Leonnig. Court: Ability to police u.s. spying program limited. http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html, 2013. Accessed: 2013-10-19.

[125] K. Lee Lerner and Brenda Wilmoth Lerner. *ENCYCLOPEDIA of Espionage, Intelligence, and Security: Volume 1*. The Gale Group, Inc., 1. edition, 2004.

[126] K. Lee Lerner and Brenda Wilmoth Lerner. *ENCYCLOPEDIA of Espionage, Intelligence, and Security: Volume 3*. The Gale Group, Inc., 1. edition, 2004.

[127] Konrad Lischka. Cyber-angriffe auf us-konzerne: Im netz der china-hacker. http://www.spiegel.de/netzwelt/netzpolitik/hacker-aus-china-so-arbeiten-die-cyberkrieger-a-884245.html, 2013. Accessed: 2013-08-04.

[128] Keith Locke. Keith locke: Dotcom case shows the cost of spying is spooky. http://www.nzherald.co.nz/kim-dotcom-case/news/article.cfm?c_id=1503274&objectid=10854676, 2012. Accessed: 2013-10-08.

[129] Philippe Lopez. China unveils yi long uav. http://en.ria.ru/military_news/20121114/177450890.html, 2012. Accessed: 2013-08-02.

[130] Ewen MacAskill and Julian Borger. New nsa leaks show how us is bugging its european allies. http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies, 2013. Accessed: 2013-10-19.

[131] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. Gchq taps fibre-optic cables for secret access to world's communications. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, 2013. Accessed: 2013-10-08.

[132] Ewen MacAskill, Nick Davies, Nick Hopkins, Julian Borger, and James Ball. Gchq intercepted foreign politicians' communications at g20 summits. http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits, 2013. Accessed: 2013-10-20.

[133] Mandiant. Mandiant apt1 report. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, 2013. Accessed: 2013-10-14.

[134] John Markoff. Vast spy system loots computers in 103 countries. http://www.nytimes.com/2009/03/29/technology/29spy.html?adxnnl=1&adxnnlx=1382105694-ajhFZX0gDheAZ1OCtAn6Yg, 2009. Accessed: 2013-09-25.

[135] Morgan Marquis-Boire and Bill Barczak. From bahrain with love: Finfisher's spy kit exposed? https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/, 2012. Accessed: 2013-08-12.

[136] Morgan Marquis-Boire and Bill Barczak. The smartphone who loved me: Finfisher goes mobile? https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/, 2012. Accessed: 2013-08-12.

[137] Declan McCullagh. Skype: We can't comply with police wiretap requests. http://news.cnet.com/8301-13578_3-9963028-38.html, 2008. Accessed: 2013-10-08.

[138] Declan McCullagh. U.n. calls for 'anti-terror' internet surveillance. http://news.cnet.com/8301-13578_3-57537559-38/u.n-calls-for-anti-terror-internet-surveillance/, 2012. Accessed: 2013-07-05.

[139] Annett Meiritz and Philipp Wittrock. Spähaffäre: Deutsche geheimdienste außer kontrolle. http://www.spiegel.de/politik/deutschland/prism-aufklaerung-wie-deutsche-geheimdienste-kontrolliert-werden-a-911222.html, 2013. Accessed: 2013-10-20.

[140] Andre Meister. Bundesnachrichtendienst überwacht drei millionen telekommunikationsverkehre im jahr, einmal täglich auch etwas relevantes. https://netzpolitik.org/2013/bundesnachrichtendienst-uberwacht-jede-sekunde-eine-telekommunikation-einmal-taglich-auch-etwas-relevantes/, 2013. Accessed: 2013-11-22.

[141] Andre Meister. Geheimes dokument: Bundeskriminalamt kauft international bekannten staatstrojaner finfisher/finspy von gamma. https://netzpolitik.org/2013/geheimes-dokument-bundeskriminalamt-kauft-international-bekannten-staatstrojaner-finfisherfinspy-von-gamma, 2013. Accessed: 2013-08-12.

[142] mho. Huawei und zte wehren sich gegen spionageverdacht. http://www.heise.de/newsticker/meldung/Huawei-und-ZTE-wehren-sich-gegen-Spionageverdacht-1708114.html, 2012. Accessed: 2013-07-04.

[143] mos/ddp. Trojaner aus china bedrohen deutsche stromnetze. http://www.welt.de/wirtschaft/webwelt/article4162853/Trojaner-aus-China-bedrohen-deutsche-Stromnetze.html, 2009. Accessed: 2013-07-14.

[144] Ellen Nakashima. In a world of cybertheft, u.s. names china, russia as main culprits. http://www.washingtonpost.com/world/national-security/us-cyber-espionage-report-names-china-and-russia-as-main-culprits/2011/11/02/gIQAF5fRiM_story.html, 2011. Accessed: 2013-07-14.

[145] Ellen Nakashima. Chinese hackers who breached google gained access to sensitive data, u.s. officials say. http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html, 2013. Accessed: 2013-08-02.

[146] Ellen Nakashima. Confidential report lists u.s. weapons system designs compromised by chinese cyberspies. http://www.washingtonpost.com/world/national-

security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html, 2013. Accessed: 2013-07-16.

[147] Ellen Nakashima. U.s. said to be target of massive cyber-espionage campaign. http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story_1.html, 2013. Accessed: 2013-07-14.

[148] Ellen Nakashima, Greg Miller, and Julie Tate. U.s., israel developed flame computer virus to slow iranian nuclear efforts, officials say. http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html, 2012. Accessed: 2013-09-24.

[149] Matt Nash. Virus cracks banking secrecy. https://now.mmedia.me/lb/en/reportsfeatures/virus_cracks_banking_secrecy, 2012. Accessed: 2013-09-24.

[150] Margaret C. National Defense Research Institute Harrell and Melissa A. Bradley. Data collection methods - semi-structured interviews and focus groups. http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR718.pdf, 2013. Accessed: 2013-12-20.

[151] United Nations. The use of internet for terrorist purposes. http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 2012. Accessed: 2013-07-05.

[152] New York Times. Tracking ghostnet: Investigating a cyber espionage network. http://www.f-secure.com/weblog/archives/ghostnet.pdf, 2009. Accessed: 2013-10-05.

[153] Kevin J. O'Brien. Europe weighs requiring firms to disclose data breaches. http://www.nytimes.com/2013/01/17/technology/17iht-data17.html, 2013. Accessed: 2013-10-29.

[154] US House of Representatives. House intelligence committee launches investigation into national security threats posed by chinese telecom companies working in the u.s. http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/111711ChineseTelecom.pdf, 2011. Accessed: 2013-07-04.

[155] Office of the High Commissioner for Human Rights. International covenant on civil and political rights. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, 1966. Accessed: 2013-06-28.

[156] Office of the National Counterintelligence Executive. Report to congress on foreign economic collection and industrial espionage. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf, 2011. Accessed: 2013-11-07.

[157] Thomas Oppermann. Bericht zu den maßnahmen nach dem terrorismusbekämpfungsgesetz für das jahr 2011. http://dip.bundestag.de/btd/17/127/1712774.pdf, 2013. Accessed: 2013-11-22.

[158] Pierluigi Paganini. Cyber-espionage: The greatest transfer of wealth in history. http://resources.infosecinstitute.com/cyber-espionage-the-greatest-transfer-of-wealth-in-history/, 2013. Accessed: 2013-09-09.

[159] Pierluigi Paganini. Cyberespionage, another watering hole attack against us website. http://securityaffairs.co/wordpress/11405/intelligence/cyberespionage-another-watering-hole-attack-against-us-website.html, 2013. Accessed: 2013-09-09.

[160] Frank Patalong. Daten-Überwachungszentrum in utah: Festung der cyberspione. http://www.spiegel.de/netzwelt/netzpolitik/bluffdale-das-datensammel-zentrum-der-nsa-a-904355.html, 2013. Accessed: 2013-10-22.

[161] Nicole Perlroth. Google adds malware statistics to transparency report. http://bits.blogs.nytimes.com/2013/06/25/google-adds-malware-statistics-to-transparency-report/, 2013. Accessed: 2013-10-21.

[162] Jared Peters. Qualcomm's snapdragon 800 comes with built-in support for always-on voice recognition. http://www.talkandroid.com/170747-qualcomms-snapdragon-800-comes-with-built-in-support-for-always-on-voice-recognition/, 2013. Accessed: 2013-11-10.

[163] Laura Poitras, Marcel Rosenbach, and Holger Stark. Geheimdokumente: Nsa überwacht 500 millionen verbindungen in deutschland. http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-500-millionen-verbindungen-in-deutschland-a-908517.html, 2013. Accessed: 2013-10-08.

[164] Kevin Poulsen. New snowden leak reports 'groundbreaking' nsa crypto-cracking. http://www.wired.com/threatlevel/2013/08/black-budget/, 2013. Accessed: 2013-10-21.

[165] John Reed. Meet the flame virus's mean little sibling. http://killerapps.foreignpolicy.com/posts/2012/10/15/meet_the_flame_viruss_mean_little_sibling, 2012. Accessed: 2013-09-24.

[166] John Reed. Meet red october, the newest cyber espionage operation. http://killerapps.foreignpolicy.com/posts/2013/01/14/meet_red_october_the_newest_cyber_espionage_operation, 2013. Accessed: 2013-09-26.

[167] Ole Reissmann. It-sicherheitsbericht: Vorhang auf für den cyber-minister. http://www.spiegel.de/netzwelt/web/it-sicherheitsbericht-vorhang-auf-fuer-den-cyber-minister-a-768544.html, 2011. Accessed: 2013-10-21.

[168] Ole Reissmann. Spionage: Usa und israel sollen hinter flame-virus stecken. http://www.spiegel.de/netzwelt/netzpolitik/flame-usa-und-israel-sollen-hinter-spionage-virus-stecken-a-839878.html, 2012. Accessed: 2013-09-24.

[169] Ole Reissmann, AFP, and dpa. Klagen gegen Überwachung: Europäischer gerichtshof prüft vorratsdaten-richtlinie. http://www.spiegel.de/netzwelt/netzpolitik/europaeischer-gerichtshof-prueft-vorratsdaten-richtlinie-a-910270.html, 2013. Accessed: 2013-10-19.

[170] Ole Reissmann and Christian Stöcker. Überwachung: Studie stellt sinn von vorratsdaten in frage. http://www.spiegel.de/netzwelt/netzpolitik/ueberwachung-studie-stellt-sinn-von-vorratsdaten-in-frage-a-811675.html, 2012. Accessed: 2013-10-29.

[171] Press release. Parlament verabschiedet härtere eu-weite strafen für 'cyberkriminelle'. http://www.europarl.europa.eu/news/de/news-room/content/20130701IPR14763/html/Parlament-verabschiedet-härtere-EU-weite-Strafen-für-Cyberkriminelle, 2013. Accessed: 2013-09-16.

[172] Global Research and Analysis Team (GReAT). Gauss: Abnormal distribution. http://www.securelist.com/en/analysis/204792238/Gauss_Abnormal_Distribution, 2012. Accessed: 2013-09-24.

[173] Global Research and Analysis Team (GReAT). miniflame aka spe: 'elvis and his friends'. http://www.securelist.com/en/blog/763/analysis/204792247/miniFlame_aka_SPE_Elvis_and_his_friends, 2012. Accessed: 2013-09-24.

[174] Global Research and Analysis Team (GReAT). 'nettraveler is running!' - red star apt attacks compromise high-profile victims. http://www.securelist.com/en/blog/8105/NetTraveler_is_Running_Red_Star_APT_Attacks_Compromise_High_Profile_Victims, 2013. Accessed: 2013-09-29.

[175] Global Research and Analysis Team (GReAT). Red october - java exploit delivery vector analysis. http://www.securelist.com/en/blog/208194086/, 2013. Accessed: 2013-09-26.

[176] Global Research and Analysis Team (GReAT). The 'red october' campaign - an advanced cyber espionage network targeting diplomatic and government agencies. http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies, 2013. Accessed: 2013-09-26.

[177] Global Research and Analysis Team (GReAT). Winnti. more than just a game. http://www.securelist.com/en/analysis/204792287/Winnti_More_than_just_a_game, 2013. Accessed: 2013-09-26.

[178] Shane Richmond and Christopher Williams. Millions of internet users hit by massive sony playstation data theft. http://www.telegraph.co.uk/technology/sony/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html, 2011. Accessed: 2013-09-12.

[179] Michael Riley. How the u.s. government hacks the world. http://www.businessweek.com/articles/2013-05-23/how-the-u-dot-s-dot-government-hacks-the-world, 2013. Accessed: 2013-08-13.

[180] Andreas Rinke. Eu-kommission: Meldepflicht für hackerangriffe trifft zehntausende unternehmen. http://www.spiegel.de/netzwelt/netzpolitik/eu-kommission-44-000-firmen-trifft-meldepflicht-fuer-hackerangriffe-a-881145.html, 2013. Accessed: 2013-09-26.

[181] Julie J. C. H. Ryan, D. Sc, and The George. The use, misuse, and abuse of statistics in information security research", presented to american society of engineering. In *Management National Conference (ASEM 2003)*, 2003.

[182] Ted Samson. Companies think they're prepared for apt cyber attacks, but they aren't. http://www.infoworld.com/t/security/companies-think-theyre-prepared-apt-cyberattacks-they-arent-212796, 2013. Accessed: 2013-10-21.

[183] David E. Sanger. Obama order sped up wave of cyberattacks against iran. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0, 2012. Accessed: 2013-09-24.

[184] David Sasaki. 25 years later: The good and bad of the web. http://davidsasaki.name/2013/12/25-years-later-the-good-and-bad-of-the-web/, 2013. Accessed: 2013-12-20.

[185] Schmid, Gerhard. Report on the existence of a global system for the interception of private and commercial communications (echelon interception system) (2001/2098(ini)). http://info.publicintelligence.net/ECHELONreport.pdf, 2001. Accessed: 2013-11-01.

[186] Bruce Schneier. What exactly are the nsa's 'groundbreaking cryptanalytic capabilities'? http://www.wired.com/opinion/2013/09/black-budget-what-exactly-are-the-nsas-cryptanalytic-capabilities/, 2013. Accessed: 2013-10-19.

[187] Defense Security Service. Administration strategy on mitigating the theft of u.s. trade secrets. http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf, 2013. Accessed: 2013-07-13.

[188] Vernon Silver. Mjm as personified evil says spyware saves lives not kills them. http://www.bloomberg.com/news/2012-11-08/mjm-as-personified-evil-says-spyware-saves-lives-not-kills-them.html, 2012. Accessed: 2013-08-12.

[189] Matt Sledge. Cia's gus hunt on big data: We 'try to collect everything and hang on to it forever'. http://www.huffingtonpost.com/2013/03/20/cia-gus-hunt-big-data_n_2917842.html, 2013. Accessed: 2013-08-01.

[190] Andrei Soldatov and Irina Borogan. In ex-soviet states, russian spy tech still watches you. http://www.wired.com/dangerroom/2012/12/russias-hand/all/, 2012. Accessed: 2013-07-06.

[191] Christian Stöcker. Us-spionage: Nsa späht banktransfers und brasilianischen Ölkonzern aus. http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-swift-banktransfers-und-oelkonzern-petrobras-a-921128.html, 2013. Accessed: 2013-10-20.

[192] Christoph Sydow. Schnüffelsoftware xkeyscore: Deutsche geheimdienste setzen us-spähprogramm ein. http://www.spiegel.de/politik/deutschland/bnd-und-bfv-setzen-nsa-spaehprogramm-xkeyscore-ein-a-912196.html, 2013. Accessed: 2013-10-08.

[193] Symantec. W32 stuxnet dossier. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2011. Accessed: 2013-10-16.

[194] TeleGeography. Submarine cable map. http://www.submarinecablemap.com/, 2013. Accessed: 2013-10-06.

[195] Craig Timberg. The nsa slide you haven't seen. http://articles.washingtonpost.com/2013-07-10/business/40480665_1_nsa-slide-prism, 2013. Accessed: 2013-10-08.

[196] Craig Timberg and Ellen Nakashima. Agreements with private companies protect u.s. access to cables' data for surveillance. http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html, 2013. Accessed: 2013-08-05.

[197] Alexander Tsolkas and Friedrich Wimmer. *Wirtschaftsspionage und Intelligence Gathering*. Springer Verlag, 1. edition, 2013.

[198] Ugander, Johan amd Karrer, Brian and Backstrom, Lars and Marlow, Cameron. The anatomy of the facebook social graph. http://arxiv.org/pdf/1111.4503v1.pdf, 2011. Accessed: 2013-10-29.

[199] uid1307457. 1.0 trojan horses. http://www.dslreports.com/faq/trojans/1.0_Trojan_horses, 2009. Accessed: 2013-10-08.

[200] uid1307457. what is a dropper trojan? http://www.dslreports.com/faq/trojans/1.0_Trojan_horses, 2009. Accessed: 2013-10-08.

[201] Udo Ulfkotte. *Verschlusssache BND*. Koehler & Amelang, 3. edition, 1997.

[202] Joris Van Hoboken, Axel Arnbak, and Nico Van Eijk. Cloud computing in higher education and research institutions and the usa patriot act. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534, 2013. Accessed: 2013-11-29.

[203] vbr. Huawei sagt Übernahme von us-unternehmen ab. http://www.heise.de/newsticker/meldung/Huawei-sagt-Uebernahme-von-US-Unternehmen-ab-1193971.html, 2011. Accessed: 2013-07-04.

[204] Verizon. Data breach investigations report 2013. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf, 2013. Accessed: 2013-11-09.

[205] John Villasenor. The flame cyber espionage attack: Five questions we should ask. http://www.forbes.com/sites/johnvillasenor/2012/06/04/the-flame-cyber-espionage-attack-five-questions-we-should-ask/2/, 2012. Accessed: 2013-09-29.

[206] Peter Walker. Boston bombing identification attempts on social media end in farce. http://www.theguardian.com/world/2013/apr/19/boston-bombing-suspects-reddit-social-media, 2013. Accessed: 2013-10-29.

[207] Simon Walters. Hammond's £500m new cyber army: As he reveals top-secret whitehall bunker for the first time, defence secretary says future wars will be fought with viruses. http://www.dailymail.co.uk/news/article-2436946/Hammonds-500m-new-cyber-army-As-reveals-secret-Whitehall-bunker-time-Defence-Secretary-says-future-wars-fought-viruses.html, 2013. Accessed: 2013-10-05.

[208] Joby Warrick. Jordan emerges as key cia counterterrorism ally. http://articles.washingtonpost.com/2010-01-04/news/36847422_1_jordanian-intelligence-service-base-chapman-general-intelligence-department, 2010. Accessed: 2013-10-08.

[209] Zack Whittaker. Microsoft admits patriot act can access eu-based cloud data. http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225, 2011. Accessed: 2013-11-29.

[210] Wilhoit, Kyle. Who's really attacking your ics equipment? http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf, 2013. Accessed: 2013-11-08.

[211] Andreas Wilkens. Verfassungsschutz registriert zunehmende wirtschaftsspionage übers internet. http://www.heise.de/ct/meldung/Verfassungsschutz-registriert-zunehmende-Wirtschaftsspionage-uebers-Internet-219591.html, 2009. Accessed: 2013-07-05.

[212] Clay Wilson. Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress. http://www.history.navy.mil/library/online/computerattack.htm, 2005. Accessed: 2013-11-09.

[213] Edward Wong. Hacking u.s. secrets, china pushes for drones. http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?pagewanted=2&_r=2&hp, 2013. Accessed: 2013-09-23.

[214] Paul Wright. Meet prism's little brother: Socmint. http://www.wired.co.uk/news/archive/2013-06/26/socmint, 2013. Accessed: 2013-10-18.

[215] ZDNet.de. Zdnet.de - digitale wirtschaftsspionage: ein totgeschwiegenes problem. http://www.youtube.com/watch?v=4r8IxxLMsJc, 2012. Accessed: 2013-07-28.

[216] Reuters ZEIT ONLINE, dpa. Gerhard schindler soll neuer bnd-chef werden. http://www.zeit.de/politik/deutschland/2011-10/bnd-schindler-geheimdienstchef, 2011. Accessed: 2013-10-08.

[217] Kim Zetter. 5 fun facts from the latest nsa leak. http://www.wired.com/threatlevel/2013/06/five-fun-facts-on-the-nsa-leak/, 2013. Accessed: 2013-10-19.