HORIZON 2020

Digital Security: Cybersecurity, Privacy and Trust
H2020-DS-2015-1

DS-04-2015 Information driven Cyber Security Management
Grant n° 700176

Secure Information Sharing Sensor Delivery event Network[†]

Deliverable D2.8: Final legal requirements

Abstract: The following document examines the techniques used by SISSDEN in terms of their criminal law and data protection law admissibility. The document also looks at whether and how technologies developed by SISSDEN can be protected with the help of an intellectual property rights management. The document is and updated and expanded version of the earlier deliverable D2.2 “Preliminary legal requirements”.

Contractual Date of Delivery	31 October 2018
Actual Date of Delivery	31 December 2018
Deliverable Security Class	Public
Editor	Ninja Marnau (USAAR)
Contributors	USAAR, NASK, CYBE
Internal Reviewers	Arturo Campos (CYBE), Angelo Consoli (EXYS)
Quality Assurance	Adam Kozakiewicz (NASK)

[†] The research leading to these results has received funding from the European Union Horizon 2020 Programme (H2020-DS-2015-1) under grant agreement n° 700176.

The *SISSDEN* consortium consists of:

Naukowa i Akademicka Sieć Komputerowa	Coordinator	Poland
Montimage EURL	Principal Contractor	France
CyberDefcon Limited	Principal Contractor	United Kingdom
Universitaet des Saarlandes	Principal Contractor	Germany
Deutsche Telekom AG	Principal Contractor	Germany
Eclexys SAGL	Principal Contractor	Switzerland
Poste Italiane – Società per Azioni	Principal Contractor	Italy
Stichting the Shadowserver Foundation Europe	Principal Contractor	Netherlands

Table of Contents

TABLE OF CONTENTS ... **3**

1 INTRODUCTION ... **6**

2 SCOPE OF THIS DOCUMENT ... **7**

3 CONSIDERED TECHNIQUES ... **8**

3.1 HONEYPOTS ... 8
3.1.1 Spampot ... *8*
3.1.1.1 Sample Data ... 8
3.1.2 DDoS honeypots ... *9*
3.1.2.1 Source Address Spoofing ... 9
3.1.2.2 Amplifiers ... 9
3.1.2.3 Sample Data ... 9
3.1.3 Darknets ... *10*
3.1.3.1 Sample Data ... 10
3.2 NETWORK TRAFFIC MONITORING ... 10
3.2.1 Netflow ... *10*
3.2.2 PCAP of honeypot and darknet traffic ... *11*
3.2.3 Intrusion Detection ... *11*
3.2.3.1 Suricata IDS ... 11
3.2.3.2 Montimage Monitoring Tool (MMT) ... 12
3.3 MALWARE ANALYSIS ... 14
3.3.1 Sandboxes ... *14*
3.3.1.1 Sample Data ... 14
3.4 PORTSCANS / ACTIVE NETWORK PROBES (CURRENTLY NOT PLANNED) ... 14
3.5 DATA SHARING PLATFORM ... 15
3.5.1 Sharing data within the project ... *15*
3.5.2 Sharing data with ISPs/CERTs ... *15*
3.5.3 Sharing data with the public ... *15*
3.5.4 Sharing data with law enforcement agencies ... *15*

4 CRIMINAL LAW ... **16**

4.1 GERMAN CRIMINAL LAW ... 16
4.1.1 DDoS Attack Monitoring ... *16*
4.1.1.1 Possible criminal liability for DDoS attacks ... 16
4.1.2 Criminal liability for honeypot deployment ... *24*
4.1.2.1 Perpetration and incitement ... 24
4.1.2.2 Accessory in computer sabotage, Section 303b I Nr. 2, 27 of the Criminal Code ... 24
4.1.2.3 Aid for further offenses ... 27
4.1.2.4 Negligence of the accomplice ... 27
4.1.2.5 Use of honeypots with limited data rate ... 28
4.1.2.6 Risk considerations ... 28
4.1.3 Sandboxes ... *28*
4.1.4 Port scans / Active Network Probes ... *28*
4.2 POLISH CRIMINAL LAW ... 29
4.2.1 Article 268 § 2 – making difficult to obtain knowledge of the information when the information is a record on an electronic information carrier and article 268 a – destroying of computer data ... *29*
4.2.2 Article 269 a - interfering with the functioning of a computer system ... *31*
4.2.3 Article 269 b – manufacturing of computer programs ... *31*
4.2.4 Article 269 c – legal defense of actions to detect errors in the security of information systems ... *32*
4.3 DUTCH CRIMINAL LAW ... 33
4.3.1 Computer Trespassing (DoS attacks), Section 138b of the Criminal Code ... *33*
4.3.2 Unlawful Interception, Section 139c of the Criminal Code ... *34*
4.3.3 Computer Sabotage, Section 161sexies and 161septies of the Criminal Code ... *34*
4.3.4 Data Manipulation, Section 350b of the Criminal Code ... *35*

5 PRIVACY AND DATA PROTECTION LAW ... **37**

5.1 PROCESSING OF PERSONAL DATA ... 37
5.1.1 According to Directive 95/46/EC ... 37
5.1.1.1 Applicability of Directive 95/46/EC ... 37
5.1.1.2 Principles relating to data quality ... 39
5.1.1.3 Criteria for making data processing legitimate ... 39
5.1.1.4 Rights of the data subject ... 40
5.1.1.5 Confidentiality and security of processing ... 42
5.1.1.6 Notification to the supervisory authority ... 43
5.1.2 According to Regulation (EU) 2016/679 (GDPR) ... 43
5.1.2.1 Applicability of Regulation (EU) 2016/679 ... 44
5.1.2.2 Principles relating to data quality ... 48
5.1.2.3 Criteria for making data processing legitimate ... 49
5.1.2.4 Rights of the data subject ... 51
5.1.2.5 Controller's obligations ... 54
5.2 DATA SHARING PLATFORM ... 58
5.2.1 Data sharing within the project ... 58
5.2.1.1 According to Directive 95/46/EC ... 58
5.2.1.2 According to Regulation (EU) 2016/679 (GDPR) ... 58
5.2.2 Data sharing with ISPs and CERTs ... 58
5.2.2.1 According to Directive 95/46/EC ... 58
5.2.2.2 According to Regulation (EU) 2016/679 (GDPR) ... 59
5.2.3 Data sharing with the public ... 59
5.2.3.1 According to Directive 95/46/EC ... 59
5.2.3.2 According to Regulation (EU) 2016/679 (GDPR) ... 59
5.2.4 Reference Data Set for trusted recipients ... 60
5.2.5 Sharing data with law enforcement agencies ... 60
5.2.5.1 According to Directive 95/46/EC ... 60
5.2.5.2 According to Directive (EU) 2016/680 ... 60
5.2.5.3 According to Regulation (EU) 2016/679 (GDPR) ... 60
5.2.5.4 Application of national law ... 60
5.3 DATA TRANSFER TO THIRD NON-EU STATES ... 60
5.3.1 EU-U.S. Privacy Shield ... 61
5.3.2 EU Standard Contractual Clauses ... 62
5.3.2.1 Objectives ... 62
5.3.2.2 Regulated content ... 63
5.3.2.3 C2C clauses 2001/497/EC and 2004/915/EC ... 64
5.3.2.4 C2P clauses 2010/87/EU ... 65
5.3.2.5 Validity and DPA oversight ... 66
5.3.3 Binding Corporate Rules (BCR) ... 67

6 INTELLECTUAL PROPERTY RIGHTS MANAGEMENT ... 69

6.1 INTRODUCTION TO IPR MANAGEMENT ... 69
6.1.1 Patents ... 70
6.1.2 Trademarks ... 70
6.1.3 Industrial design ... 70
6.1.4 Trade secrets ... 70
6.1.5 Copyrights & related rights ... 71
6.1.6 Protection of layout-designs or topographies of integrated circuits ... 71
6.1.6.1 Definition of integrated circuit and layout-design ... 71
6.2 SISSDEN ASSETS - A PROVISIONAL IPR AUDIT ... 72
6.2.1.1 Guidelines for a SISSDEN IPR audit ... 72
6.2.1.2 The IPR Audit ... 73
6.2.1.3 Developing a provisional register of partners' IPR assets ... 73
6.3 RISKS TO SISSDEN ASSETS ... 74
6.4 ASSET PROTECTION ... 75
6.4.1 Patent & IP searches relating to SISSDEN ... 75
6.4.2 Utility models ... 75
6.4.3 Trademarks ... 75
6.4.4 Others ... 75
6.4.5 Licensing of IP assets ... 76
6.5 TOWARDS A BUSINESS STRATEGY ... 77
6.6 GLOSSARY & ACRONYMS ... 78

7 CONCLUSIONS AND RECOMMENDATIONS – SUMMARY ... 80

7.1 CRIMINAL LAW 80
7.1.1 German criminal law 80
7.1.2 Polish criminal law 80
7.1.3 Dutch criminal law 81
7.2 PRIVACY AND DATA PROTECTION LAW 81
7.2.1 Processing of personal data 81
7.2.1.1 Directive 95/46/EC 81
7.2.1.2 GDPR 82
7.2.2 Data sharing platform 82
7.2.3 Data transfer to third non-EU states 83
7.3 INTELLECTUAL PROPERTY RIGHTS MANAGEMENT 83
8 BIBLIOGRAPHY 85

1 Introduction

The SISSDEN project aims to collect information about malware infections and other network threat activities. To this end, SISSDEN will deploy an extensive sensor network, collecting and processing this threat information. Therefore, it is necessary to ensure legal compliance of our envisioned sensor network architecture and data processing as well as assess means to safeguard the consortium's intellectual property. In this deliverable we will provide an initial assessment of the criminal and data protection law implications as well as IPR management regarding the SISSDEN network.

2 Scope of this document

From a methodological point of view, this document first summarizes the techniques used by SISSDEN to subsequently subject them to a legal assessment. This approach was chosen in order to ensure that all essential characteristics of the technical infrastructure were adequately depicted. The abstraction is intended to ensure that small technical changes do not cause any changes in the legal assessment, while changes that differ greatly from our initial assumptions can be easily detected as they may require a new legal assessment. Although the data protection policies aim to be neutral to the underlying technology, a thorough understanding of the techniques deployed in SISSDEN will help to provide actionable legal guidelines.

At the level of data protection, the deliverable D2.2 examined mainly the Directive 95/46/EC (Data Protection Directive). However, the Directive was replaced by the Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) on 25 May 2018. For this reason, the GDPR had also been taken into account as part of SISSDEN's legal consideration. This was done as part of this deliverable. This document does not include a legal consideration of the Directive 2002/58 / EC (E-privacy Directive), as it applies only to publicly available electronic communications services (access providers) pursuant to Article 3 1) of Directive 2002/58 / EC.

At the level of criminal law, there are no EU-wide regulations that apply to this project. However, within the scope of SISSDEN, it is not feasible to assess the national criminal law of all member states or even globally. Hence, we will focus on the national law of member states chosen by the SISSDEN consortium as an initial example. The assessment will cover German and Dutch national law in Deliverable D2.8, given that these countries will play a fundamental role in deploying the SISSDEN architecture.

Furthermore, this document will discuss intellectual property laws. IPR laws are well-established through a system of patents, copyright and trademarks, formed to enable recognition of, or financial benefit, from an invention or creation. Successful IPR management can be complex and time-consuming. SISSDEN must ensure that assets created by the project are fully protected through the appropriate means. Assets brought to the project by partners also require careful rights administration. As a first step, an IP Audit will assess the current situation and aid in the planning of future IP protection as the project progresses through its various stages.

In relation to IPR, this document broadly describes the legal processes that the SISSDEN project must adhere to and the protections available to: a) minimize the risk of legal infringement of the IP of others, b) reduce the need to initiate legal action against others in order to preserve the rights of SISSDEN and its partners and, c) outlines why IP is a valuable business asset. Due to the complexity of the law on IP protection, SISSDEN partners should decide if this is a task that can be effectively performed in-house or if the services of key specialists in this area should be employed.

3 Considered Techniques

This section gives an overview of the techniques that are relevant within the scope of SISSDEN and provides descriptions for each technique that can also be understood by non-technical readers.

3.1 Honeypots

SISSDEN will deploy a variety of different types of honeypots. These are intended to accept malicious traffic and malware aimed at exploiting the vulnerable system the honeypot emulates. The network of honeypots is described in detail in deliverable D3.3 Initial technical architecture. It will initially include: glastopf, conpot, cowrie, honeytrap, elasticpot and dionaea. Although each of these honeypots vary in the services that they emulate, they operate similarly from a legal point of view. They all passively collect the network traffic which attempts to access the emulated vulnerable service.

We will therefore focus our legal assessment on two types of honeypots that, first, exemplify the general legal assessment regarding their deployment and, second, have specific additional properties regarding criminal law and data protection law.

3.1.1 Spampot

Spampot is a closed source software from SHAD. The aim of the software is to collect spam (unsolicited bulk emails) in order to gain insights into current spam campaigns. Within this framework, both the distribution ways and malicious attachments of spam are analyzed. Spampot simulates therefore a misconfigured device, which can be used to relay spam via SMTP, HTTP and SOCKS proxy abuse. Attackers often first test the functionality of the misconfigured device with few messages. Therefore spampot allows the attacker to send a small amount of test mails. However, as soon as the attacker wants to send larger amounts of messages, these are delivered to a local mail server and stored there. Within the project, spambot will be used as a SHAD managed VM.

3.1.1.1 Sample Data

An acquired data set can contain the following data:

Nature of the data	Example
Timestamp	Thu 30 Jun 12:21:39 CEST 2017
Src/Dst IP	192.168.0.106
Src/Dst Port	110, 995, 143, 993, 25, 2525, 465
Service specific data	Subject: spam mail Message-ID: <server11.01@example.net> Date: Wed, 29 Jun 2017 11:31:00 +0200 From: Sender <sender@example.net> To: Recipient <recipient@example.net> MIME-Version: 1.0 Content-Type: text/plain; charset=us-ascii

	Content-Transfer-Encoding: 7bit
Spam message bodies in Unix mbox format	Hello World!

3.1.2 DDoS honeypots

Reflective Distributed Denial of Service (DDoS) attacks follow a common pattern: The attacker searches for so-called amplifiers on the Internet and abuses them to flood the victim's system with packets so the service is no longer reachable.

3.1.2.1 Source Address Spoofing

A big part of the DDoS attacks exploit the design of the stateless UDP protocol. The attacker abuses a property of the UDP transport protocol. UDP is itself connectionless, the packets are single datagrams with no reference to other packets. This means that each packet has to carry enough information for the receiving system to send an answer. In particular, each packet holds the IP address of the source system. Due to the fact that the receiving system cannot verify this address, it has to trust the sender to provide its correct IP address. However, it is also easily possible to provide a bogus source address so that the response will be sent to a third system instead of the original source. This third system has no means of identifying the original source other than trying to cooperate with the intermediate (second) system, since the packet it receives does not carry any information about the original source.

3.1.2.2 Amplifiers

First and foremost, an amplifier is a service which utilizes the UDP protocol to answer requests. Furthermore, it exhibits one important characteristic: the answer to a request is larger than the request itself (in terms of the amount of data) by the so-called amplification factor. This means that if a system sends requests to the amplifier at a rate of *X*, it will receive responses at a rate of (amplification factor) times *X*.

A DDoS attack now combines these two techniques. The attacker finds a suitable hosting provider where he/she can send crafted requests to (multiple) amplifiers using UDP packets and fakes the source IP address to be that of the victim's system. Each amplifier thus sends replies to the victim's system, clogging its Internet connection with useless data. Genuine packets from other clients cannot reach the victim's system and consequently the service is unreachable.

The honeypots used as part of the SISSDEN project are implemented as special cases of the aforementioned amplifiers. They offer the same basic functionality to an attacker as regular amplifiers, but employ rate limiting: once they receive a certain number of packets containing the same (genuine or spoofed) source address within a fixed time frame (e.g., 10 packets within one minute), the source (victim) address is put on a blacklist and the honeypot stops sending amplified replies to the victim for a certain duration (e.g., one day). By limiting the amount of network traffic that an attacker can generate using a honeypot, the operators try to make sure that if the honeypot is discovered by scanners and later abused for a DDoS attack, its contribution to the overall traffic is minimal and that the honeypot is not ultimately responsible for the unreachability of the DDoS victim.

3.1.2.3 Sample Data

An acquired data set can contain the following data:

Nature of the data	Example
IP address of the victim	192.168.0.106
Protocol (ISO Layer 7)	DNS/NTP/SSDP/…
Timestamp of the attack	Thu 30 Jun 12:21:39 CEST 2016
Full packet	IP header, UDP header, payload (depending on the protocol)

3.1.3 Darknets

SISSDEN considers to additionally monitor connection attempts on darknets. A darknet is a routed but unused IP address space that records all network traffic that arrives at any of the IP addresses that are part of the darknet. Darknets are purely passive and do not actively send out traffic. That is, they do not attempt emulation of any services nor do they respond to connection attempts in any way. Connection attempts to an IP serving as a Darknet will be logged through the supporting data capture mechanisms. Since this monitoring will only passively collect incoming traffic we do not see any relevance for a criminal law assessment. Data protection law regarding darknets will be investigated below.

3.1.3.1 Sample Data

Data captured through the use of darknets includes:

Nature of the data	Example
Packet timestamp	Thu 30 Jun 12:21:39 CEST 2016
Source and destination IP address	192.168.0.106
Source and destination UDP/TCP port numbers	119, 137, 161, …
TCP/UDP/ICMP and other protocol header information	Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0xc7ce Identifier (BE): 1040 (0x0410) Identifier (LE): 4100 (0x1004) Sequence number (BE): 11297 (0x2c21) Sequence number (LE): 8492 (0x212c)
Any packet payload other than header (typically for UDP/ICMP)	

3.2 Network Traffic Monitoring

3.2.1 Netflow

To summarize and aggregate network communication all connections to the honeypots could be centrally monitored by a Netflow probe and collector. The goal of the data aggregation is to provide statistical data of certain communication streams. On the software

side the project planned to use fprobe[1] for the Netflow probe, nfdump[2] for the collection and nfsen[3] as graphical web based front end, with the captures stored in the Cisco Netflow v5 format. However, during development this functionality has been dropped, since equivalent data is collected and stored by Moloch as part of the monitoring activity described in the next section.

3.2.2 PCAP of honeypot and darknet traffic

All connections to the honeypots are monitored using a Moloch instance. Moloch is an open source, large scale, full packet capturing, indexing, and database system.[4] In addition to aggregating data via Netflow, all connections to the honeypots are monitored using a Moloch instance. Moloch captures, stores and exports all packets in standard PCAP format and thus provides a web interface for browsing, searching, and exporting PCAP files. Unlike Netflow, data aggregation does not occur. Consequently, the storage of the traffic as PCAP could include personal data of Honeypot or Darknet traffic.

The two darknets operated in the project capture, store and process raw traffic data. NASK does not store raw PCAP and only the results of the processing, while CYBE stores raw PCAPs and the processing and analysis results of the darknet captured traffic.

3.2.3 Intrusion Detection

All connections to honeypots/darknets will be centrally monitored by instances of Suricata IDS and Montimage Monitoring Tool (MMT).

3.2.3.1 Suricata IDS

Suricata is an open source event-based monitoring solution that allows analysing network traffic according to a set of security properties. The main objective of these properties is to formally specify security goals and/or attack behaviour related to the application or protocol that is being monitored. For this purpose, Suricata will also generate real-time alerts over the Honeypot traffic.

3.2.3.1.1 Sample data

A Suricata alert can contain the following data:

Nature of the data	Example
Timestamp	2009-11-24T21:27:09.534255
Event type	alert
Source IP	192.168.2.7
Source Port	1041
Destination IP	192.168.250.50

[1] http://fprobe.sourceforge.net/

[2] http://nfdump.sourceforge.net/

[3] http://nfsen.sourceforge.net/

[4] https://github.com/aol/moloch

Destination Port	80
Protocol	TCP
Alert	"action": "allowed", "gid": 1, "signature_id" :2001999, "rev": 9, "signature": "ET MALWARE BTGrab.com Spyware Downloading Ads", "category": "A Network Trojan was detected", "severity": 1

3.2.3.2 Montimage Monitoring Tool (MMT)

In addition to the monitoring of the connections to the honeypots with Suricata, the connections to the honeypots and darknets will be also monitored by a Montimage Monitoring Tool (MMT). MMT is an event-based monitoring solution that allows a network traffic analysis according to a set of security properties (MMT_Security properties). By setting up these properties, security goals and / or attack behavior can be formally specified. In contrast to Suricata, MMT does not work exclusively on the basis of pattern matching, but can also specify expected or unexpected behavior and correlate information from different sources. Within the project, MMT is used to display statistics and other information of the observed traffic. A MMT alert contains all the metadata and analysis data used by the different events that lead to the satisfaction of the property.

3.2.3.2.1 Sample data

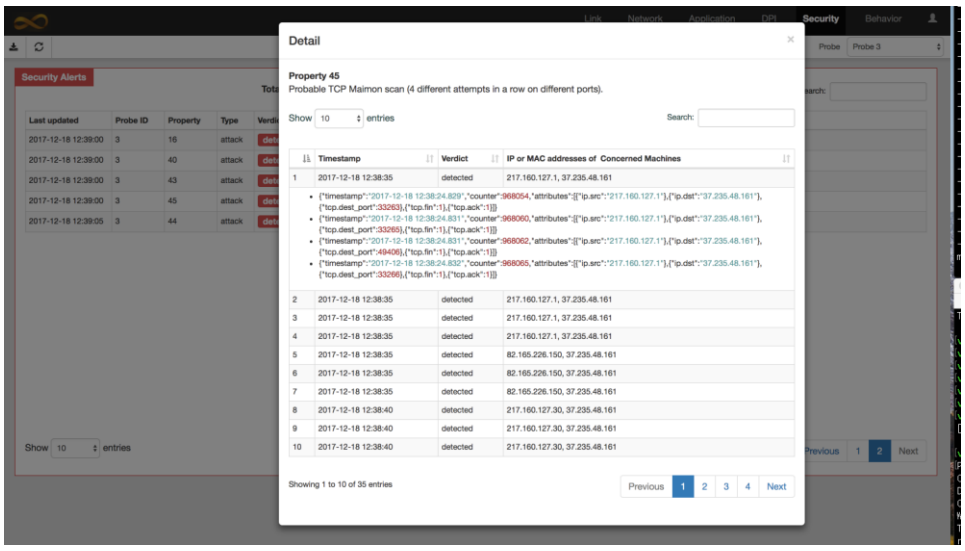
An MMT alert contains the following information:

Example alert in CSV format with history in JSON format	10, 123, "eth1", 1452523000.331799, 4, "detected", "attack", "Two successive TCP SYN requests but with different destination addresses.", {"event_12":{"timestamp":1452523000.158154,"description":"SYN request","attributes":[{"ip.src":"192.168.0.20"},{"ip.dst":"67.196.156.65"},{"tcp.flags":"2"}]},"event_13":{"timestamp":1452523000.329879,"description":"SYN request","attributes":[{"ip.src":"192.168.0.20"},{"ip.dst":"66.235.120.127"},{"tcp.flags":"2"}]}}

Description of format

Field number	Name	Description
1	format_id	Identifier of the format of the encapsulated application report
2	probe	Identifier of the probe generating the report
3	timestamp	Timestamp (seconds.micros) corresponding to the time when the output row was reported
4	property_id	Number: identifying the property
5	verdict	Word: respected or not respected or detected or not detected giving respectively the status of a security rule and and attack ["detected", "not_detected", "respected", "not_respected", "unknown"]
6	type	Word: type of property detected ["attack", "security", "test", "evasion"]
7	cause	String: description of the property
8	history	JSON object: containing a list of events that lead to the verdict. It includes timestamp, either IP or MAC addresses, and the values corresponding to the events of the property that occurred
9	verdict_count	Number of verdicts

Visualisation of alert



3.3 Malware analysis

3.3.1 Sandboxes

Analysing the behaviour of malware is a complex task. It is near impossible to determine the exact underlying algorithm of a malware sample as modern attacks often react to the conditions on the victim's system and sometimes come in a trimmed-down version which only receives the actual instructions later on from the attacker directly.

Because of this and the increasing complexity of malware, analysis tools often employ dynamic analysis, which means that the sample is executed and its behaviour observed during runtime. Among the tracked features are disk accesses, system APIs called by the malware, a screenshot of its visual appearance, and its network activity.

The technique used within the SISSDEN project focuses on analysing network activity of malware samples, as this activity is key to form a botnet. The samples are run on virtual machines (sandboxes) and any communication with other machines on the Internet is monitored and captured by the host. When samples are executed all content, including the full requests as well as the responses of the contacted hosts is recorded for further processing. By doing so, the operators of the sandbox gain a detailed insight on the communication behaviour of the malware sample.

To counter the possibility that the malware forces the sandbox to perform attacks against other computers, protection and mitigation measures are included within the sandbox. For example, spam emails are captured and not sent and large network traffic volumes are throttled by applying rate limiting, similar to the DDoS honeypots mentioned above. While these measures do not guarantee full prevention of all possible attacks, it effectively reduces the impact of the most common ones.

3.3.1.1 Sample Data

An acquired data set can contain the following data:

Nature of the data	Example
Full program file	Locky.exe
Network communication as PCAP-file	IP header, UDP/TCP header, payload (depending on the malware)
Screenshot of the System	Image from Desktop with changed background after executing a CryptoLocker
System behaviour	List of API calls called by the malware, disk accesses, etc.

3.4 Portscans / Active Network Probes (currently not planned)

While the current architecture in SISSDEN is clearly focused on passive data collection and does not foresee performing active network scans, we still discuss scans here, if only for comparison.

For example, network scans might be used to scan the Internet for hosts that are vulnerable to amplification attacks. Such active network probes are composed of port scans and fingerprinting algorithms. Port scans are used to find vulnerable protocols like DNS, SNMP, SSDP, CharGen, QOTG, NTP and NetBIOS. For this reason setup an Internet-wide scanner would be needed to identify amplifiers for the mentioned protocols. To inform the administrators of the scanned hosts and give them the opportunity to exercise their right to opt-out from the scans, there would be a reverse DNS record pointing at a web server containing suitable information. To ease the remediation process, information about each host might be collected by processing the traffic and extracting fingerprints. Fingerprints would need to be protocol-specific and assist to learn the underlying hardware, the system architecture and the operating system of a potentially vulnerable system.

3.5 Data sharing platform

The SISSDEN project requires that partners share data among themselves and with third parties. A detailed legal assessment for all subsequent sharing use cases is included in Sections 5.2 and 5.3.

3.5.1 Sharing data within the project

The project partners will have access to the raw data of the honeypots, sandboxes and active network probes. The raw data could include personal data (in a legal meaning). Therefore the project partners might need a legal reason for sharing personal data and it is possible that the data must be secured in a special way (cf. Sections 5.2 and 5.3).

3.5.2 Sharing data with ISPs/CERTs

SISSDEN aims to inform ISPs and CERTs about ongoing attacks and vulnerable systems that fall under their responsibility, which involves sharing data with ISPs/CERTs. This shared data can contain personal data, so that the project partners might need a legal clearance for this data transfer.

3.5.3 Sharing data with the public

The project partners want to inform the public and other researchers about ongoing attacks and malware trends, as well as enable advanced security research with a curated data feed. This can be, for example, the publication of the domain names used in amplification attacks and their ranking. To avoid the disclosure of personal data, such data feeds may need to be pseudonymized or even anonymized. Additionally, SISSDEN will also want to share reference datasets for research purposes which are not anonymized.

3.5.4 Sharing data with law enforcement agencies

It is imaginable that the project partners uncover a larger case of cybercrime activity and want to inform a law enforcement agency. For this case it would be useful to know on which legal basis this data exchange stands and which data can be given to the agency and which must not. National data retention requirements need also to be considered.

4 Criminal law

4.1 German criminal law

4.1.1 DDoS Attack Monitoring

In general, those who operate honeypots are not primarily a target of criminal prosecution. In fact, law accepts honeypots in order to monitor the network.[5] However, honeypots can be used to commit DDoS-Attacks, which are punishable by law.[6]

In other words, honeypots and DDoS-Attacks can be seen from different (legal) points of view. The problems associated with the use of honeypots is that these emulated systems offer the same functionality as "normal" amplifiers and therefore initially participate in the attack. This is why, first of all, it must be said which criminal offenses come into question when performing a DDoS-Attack (see 4.1.1). Subsequently the accomplice liability of the honeypot operator must be investigated (see 4.1.2).

4.1.1.1 Possible criminal liability for DDoS attacks

The increasing use of networked devices has also lead to an increased potential for DDoS attacks. Computers and computer networks are not only the instrument to perform attacks. Instead, they can also be target of different forms of digital attacks. With this in mind the German legislator extended the Criminal Code in the 1980s by introducing specific digital crime offenses such as Section 202a Criminal Code (data espionage), Section 303a Criminal Code (data tampering) or Section 303b of the Criminal Code (computer sabotage). These new criminal offenses, whose main goal is to fight digital crime, were continuously adapted and expanded during the following years.

4.1.1.1.1 Computer sabotage, Section 303b of the Criminal Code

Section 303b of the Criminal Code contains three variants of digital criminal offenses. With regard to DDoS attacks, the extension made in 2007 of Section 303b of the Criminal Code is of particular interest. Due to this new provision, Section 303b I Nr. 1 of the Criminal Code is to be applied (explicitly) to Denial-of-Service attacks.[7]

Section 303b[8]

Computer sabotage

(1) Whosoever interferes with data processing operations which are of substantial importance to another by

1. committing an offence under Section 303a(1); or

2. entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or

[5] Schweda, Bundestag verabschiedet IT-Sicherheitsgesetz, ZD-Aktuell 2015, 04737.

[6] BT-Drs. 16/3656, p. 13.

[7] BT-Drs. 16/3656, S. 13; Weidemann, in: BeckOK StGB, 32. Edition, 01.09.2016, Section 303b, Recital 10; Laue, Strafrecht und Internet – Teil 1, jurisPR-StrafR 13/2009 Annotation 2.

[8] Translation of the German Criminal Code by Prof. Dr. Michael Bohlander https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2482.

3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,

shall be liable to imprisonment not exceeding three years or a fine.

(2) If the data processing operation is of substantial importance for another's business, enterprise or a public authority, the penalty shall be imprisonment not exceeding five years or a fine.

(3) The attempt shall be punishable.

(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender

1. causes major financial loss,

2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or

3. through the offence jeopardises the population's supply with vital goods or services or the national security of the Federal Republic of Germany.

(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.

4.1.1.1.1.1 Requirements of Section 303 b I Nr. 2 of the Criminal Code

On the basis of Section 303 b I Nr. 1 of the Criminal Code, anyone who interferes with data processing (Section 202a II of the Criminal Code) either by modifying or entering data, with the intention of causing disadvantages to others, will be punished. This only applies to data processing which is of substantial importance to some party.

The first aspect to be considered is the "transmitting data". Transmission means any transmission of data from one computer to another within an existing network or telecommunication system.[9] This criterion makes it clear that the scenarios must be examined exhaustively from a technical point of view. Only then is a methodical and complete legal investigation possible.

During a DDoS attack, the server is overloaded in its response capacity due to a large number of received requests. As a consequence its recording and processing capacity is stressed out. Access to the server by legitimate users is thus blocked or at least impeded. Therefore the "sending of requests" (from the aggressor to the victim) is to be understood as a data transmission.

In most cases the intention to cause someone a disadvantage is also given. Disadvantage means the damage to legitimate interest, which do not have to be of an economic nature per se.[10] Material damages or damages to the public image of the victim are possible.[11] The

[9] Weidemann, in: BeckOK StGB, 32. Edition, 01.09.2016, Section 303b, Recital 12; Fischer, Kommentar StGB, 64. Aufl. 2017, Section 202a, Recital 6.

[10] Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b, Recital 12a.

[11] Ratkic, Denial-of-Service-Attacken im österreichischen und deutschen Strafrecht, Graz, 2014, 2.1.1.

main goal of these attacks is usually the damage, which the operator of the attacked system suffers from, if the attacker is successful.

A drastic deterioration of the system access or a (temporary) total breakdown of the web presence of a company, which promotes goods, offers services, informs, advises customers or provides some kind of customer service, would lead to considerable image damages and financial losses. It is exactly this motivation, which the perpetrator of the attack has (in most of the cases); hence he fulfils the subjective criterion of the case.

All varieties of Section 303b of the Criminal Code require a data processing of significant importance to someone, which is significantly disturbed. The term of "data processing" is to be interpreted broadly and covers not only the individual data processing, but also the further handling of data and its utilization.[12] As a consequence, the totality of computational processes is covered.[13] Websites are also included by this term: the user sends requests to the server; the server then processes them and replies back to the user. For this reason the criterion "Data processing" in terms of Section 303b I of the Criminal Code is fulfilled.[14]

Furthermore the "processing of data" must be of substantial importance to another person. Trivial cases are therefore excluded from Section 303b I.[15] Whether a case is trivial has to be decided individually and cannot be determined with a general rule. However, a significant meaning is assumed when the respective task of the person or his organization is wholly or at least predominantly dependent on the operability of the data processing.[16] This is typically assumed to be true in practical cases. The attacker's goal is usually the disruption of data processing that serve an important purpose for the victim.[17] This type of data processing typically falls under the criterion of "substantial".[18]

The processing of data does not stop being important because the task it fulfils can be accomplished in some other way.[19] In practice, such assurances, as well as ensuring functionality of the system during an ongoing attack, are very challenging. Measures must be taken ahead of time to be able to react appropriately towards an attack. In particular, restarting the system or resetting the Internet connection are not helpful.

As a consequence of the offence, the processing of data must suffer from a significant disturbance. A disturbance is given if the smooth processing of data is more than insignificantly impaired.[20] Any non-trivial impairment of the functionality is sufficient.[21] When it comes to a DoS attack, the service (e.g. website) is blocked, usually because of a

[12] BT-Drs. 10/5058, p. 35.

[13] Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b, Recital 4.

[14] Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b StGB, Recital 4ff.

[15] BT-Drs. 16/3656, p. 13.

[16] Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b, Recital 6.

[17] OLG Frankfurt, Beschluss v. 22.5.2006 – 1 Ss 319/05 = MMR 2006, 547.

[18] Heger, in: Lackner/Kühl, StGB, 28. Aufl. 2014, Section 303b, Recital 2.

[19] Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b StGB, Recital 8.

[20] Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b StGB, Recital 9.

[21] Wieck-Noodt, in: Münchener Kommentar zum StGB, 2. Aufl. 2014, Section 303b, Recital 19.

massive data transmission.[22] The system is flooded with information; hence it is overloaded and collapses. This flooding is also punishable according to Section 303b of the Criminal Code.

In order to not penalize every low or moderate impact, which an attack can cause, the malfunction of the data processing itself must be of significant importance.[23] This relevance threshold can already be reached if a single other possible data processing operation cannot be carried out because of the attack.[24] This importance can thus be assumed in case of a DoS attack, which blocks other intended transmissions.

4.1.1.1.1.2 Requirements of Section 303 b I Nr. 1 of the Criminal Code

Section 303b I Nr. 1 is an extension (in German legal terms: qualification) of Section 303a of the Criminal Code.[25] Section 303b I Nr. 1 of the Criminal Code requires that the offender significantly disturbs data processing, which is of substantial importance for another, by committing the criminal offence of Section 303a I of the Criminal Code. Therefore, the prerequisites of Section 303a of the Criminal Code have to be fulfilled.

Section 303a

Data tampering

(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment not exceeding two years or a fine.

(2) The attempt shall be punishable.

The "suppression" of data means that access to the data by authorized parties is prevented for more than an insignificant period of time, and that for this reason, they cannot be used (though their physical integrity is preserved).[26]

One has to distinguish between the data of the service (for example, the website) and the users' inputs. As a result of DoS attacks, which overload the Internet connection, the service is blocked. This means that only authorized persons with physical access to the server can access the data. "Small" websites of private persons can be stored on the PC, which would then act as a server. But in most cases — especially when it comes to major website operators — the servers are located in a data centre, which they cannot access if the Internet connection is overloaded. Under these circumstances the service provider, who is the authorized entity, cannot access the data submitted by the users. The result is thus the suppression of that data.

It is disputed if the criterion of "suppression" is also fulfilled when the data is just temporarily inaccessible. The prevailing opinion in the literature assumes that it is.[27] On the

[22] Laue, Strafrecht und Internet – Teil 1, jurisPR-StrafR 13/2009 Annotation 2.

[23] Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. Aufl. 2012, p. 180.

[24] Stree/Hecker, in: Schönke/Schröder, StGB, 29. Aufl. 2014, Section 303b, Recital 9.

[25] BT-Drs. 10/5058, p. 36.

[26] Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303a StGB, Recital 10.

[27] Schönke/Schröder/Stree/Hecker StGB Section 303a Recital 6; Weidemann, in: BeckOK, Section 303a, Recital 10.2; Gercke, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, Section 303a Recital 5.

other hand, the OLG Frankfurt differs from them because of the principle of legal certainty (Art 103 II GG).[28] According to the court, there must be other limiting evaluation criteria besides the time aspect: the extensiveness and intensity of the interference.

In any case, an attack that lasts for a long time constitutes a crime according to Section 303a I Nr 1 of the Criminal Code.

Furthermore Section 303a of the Criminal Code requires the right of disposal of the authorized party to be affected.[29] The accessibility of the website for third parties is not a crucial aspect for the data suppression. The decisive issue is the inability of the service provider to reach the data.[30] As said before, when it comes to large (website) operators, this is generally the case.

Next we will analyse the criterion of "rendering unusable". This variant is relevant if the usability of the data is affected in such a manner that it can no longer fulfil its purpose.[31] An example mentioned in German legal literature is a software that stops functioning after a certain number of execution unless a new license key is entered.[32] If a DoS attack leads to a server overload and inaccessibility of the data provided by that server, this implies that the usage of the data (regarding to its intended purpose) is restricted. If the damage is of little impact, however, the criterion of being "rendered unusable" is not fulfilled.[33]

The goal of a DDoS attack is to cause a malfunction of the target system by sending a large data volume. As a result, the perpetrator meets both criteria (suppressing data and rendering them unusable). Thus he commits an act that is punishable according to Section 303a of the Criminal Code. This result is not surprising. The legislator was aware that both criteria are not mutually exclusive.[34] The intention was to close gaps in criminal liability. It is assumed that the remaining criterion of Section 303b I of the Criminal Code (namely, data processing of substantial importance) is fulfilled.

4.1.1.1.1.3 Requirements of Section 303 b I Nr 3 of the Criminal Code

Concerning Section 303 b I Nr 3 of the Criminal Code, the DoS attack does not meet all criteria. For Section 303 b I Nr 3 of the Criminal Code it is necessary that the perpetrator destroys, damages, renders unusable, removes or changes the data processing system. The currently prevailing view sees this criminal offence committed when the attack causes a direct damage to the hardware.[35] However, this is not commonly the case for DoS attacks.

4.1.1.1.1.4 Requirements of Section 303 b II of the Criminal Code

The perpetrator commits the qualification of Section 303 b II of the Criminal Code when the data processing is done by another person's company, another person's enterprise or by an

[28] Anmerkung OLG Frankfurt/M, Beschluss v. 22.5.2006 – 1 Ss 319/05, MMR 2006, 546.

[29] Weidemann, in: BeckOK StGB, 32. Edition, 01.09.2016, Section 303a, Recital 5.

[30] Hilgendorf/Valerius, Computer und Internetstrafrecht, Recital 197.

[31] BT-Drs. 10/5058, p. 35.

[32] Würmeling, Einsatz von Programmsperren – Zivil- und strafrechtliche Aspekte, CR 1994, 592.

[33] Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303a Recital 11.

[34] BT-Drs. 10/5058, p. 35; Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303a StGB, Recital 8.

[35] Weidemann, in: BeckOK StGB, 32. Edition, 01.09. 2016, Section 303b, Recital 13; Fischer, Kommentar StGB, 64. Aufl. 2017, Section 303b StGB, Recital 13.

authority. This makes it clear that this paragraph contemplates two different types of victim groups. Paragraph one is dedicated to private persons and paragraph two is dedicated to other's companies, enterprises and authorities. In the second case, the law increases the sentence.

4.1.1.1.2 Data Espionage, Section 202 a of the Criminal Code

Section 202a

Data espionage

(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.

(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

Furthermore the perpetrator could be facing the penalty of Sections 202a, 202b and 202c of the Criminal Code. According to Section 202a I of the Criminal Code, it is a punishable offense to obtain access (for oneself or another person) to protected data without authorization by circumventing security measures.

However, DoS attackers do not penetrate the system. They just overload them and render them unreachable. By this action, the offender does not gain access to the data. This is why he is not liable to prosecution under the charge of Section 202a of the Criminal Code.

4.1.1.1.3 Data interception, Section 202 b of the Criminal Code

Section 202b

Data Interception

Whosoever unlawfully intercepts data (section 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment not exceeding two years or a fine, unless the offence incurs a more severe penalty under other provisions.

Section 202 b of the Criminal Code incorporates a subsidiarity clause. This paragraph is not applied when the perpetrator's action faces other, higher penalties. Especially Section 202a of the Criminal Code replaces Section 202b.[36]

As determined above, the criteria of Section 202a of the Criminal Code are not met by a DoS attacker. Section 202 b of the Criminal Code might therefore be applicable.

Section 202b addresses anyone who, without being authorized to do so, intercepts another person's data from a non-public data transfer or from electromagnetic emissions of a data

[36] BT-Drs. 16/3565, p. 11.

processing system, by using technical tools. Eavesdropping (e.g. on phone calls) is also covered by Section 202 b of the Criminal Code. [37]

However, the perpetrator of a DoS attack neither gets access to the data nor "eavesdrops". As a consequence, the criteria of Section 202 b of the Criminal Code are not fulfilled.

Because the perpetrator does not attempt to commit Section 202a of the Criminal Code or Section 202b, an investigation of a (possible) penalty under Section 202c does not have any relevance.

Section 202c

Acts preparatory to data espionage and phishing

(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible

1. passwords or other security codes enabling access to data (section 202a(2)), or

2. software for the purpose of the commission of such an offence, shall be liable to imprisonment not exceeding one year or a fine.

(2) Section 149(2) and (3) shall apply mutatis mutandis.

4.1.1.1.4 Trespassing, Section 123 of the Criminal Code

Section 123

Trespassing

(1) Whosoever unlawfully enters into the dwelling, business premises or other enclosed property of another, or into closed premises designated for public service or transportation, or whosoever remains therein without authorisation and does not leave when requested to do so by the authorised person, shall be liable to imprisonment not exceeding one year or a fine.

(2) The offence may only be prosecuted upon request.

DoS attacks could be considered as an offense to the property (trespassing). If an attacker obtains digital access to a website, he enters a private area and commits a "digital trespass". Section 123 is a "classic" criminal sanction of the Criminal Code. This paragraph penalizes those who enter a residence or other enclosed property without authorization. According to the prevailing opinion in the literature this paragraph requires a physical transgression into a private area. Even unauthorized access to a web site does not meet this criterion, let alone the prevention of access by others. As a result, DoS attacks do not fall under Section 123 of the Criminal Code.

[37] BT-Drs. 16/3656, p. 11.

4.1.1.1.5 Blackmail, Section 253 of the Criminal Code

Section 253

Blackmail

(1) Whosoever unlawfully with force or threat of serious harm causes a person to commit, suffer or omit an act and thereby causes damage to the assets of that person or of another in order to enrich himself or a third person unlawfully shall be liable to imprisonment not exceeding five years or a fine.

(2) The act shall be unlawful if the use of force or the threat of harm is deemed inappropriate to the purpose of achieving the desired outcome.

(3) The attempt shall be punishable.

(4) In especially serious cases the penalty shall be imprisonment of not less than one year. An especially serious case typically occurs if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of blackmail.

The perpetrator can use the fact that the website is unavailable (as a consequence of sending a large data volume) as a means of pressure, in order to force the victim to make a payment. This would be considered as blackmail in the sense of Section 253 of the Criminal Code.

4.1.1.1.6 Other offenses

Damage to property according to Section 303 of the Criminal Code should also be considered. This could be the case, for example, if the attacker is pursuing the goal of overloading the Internet or network connection of a nuclear power plant, so that he can interfere with the control and thereby damage the reactor.

Section 303

Criminal damage

(1) Whosoever unlawfully damages or destroys an object belonging to another shall be liable to imprisonment not exceeding two years or a fine.

(2) Whosoever unlawfully alters the appearance of an object belonging to another substantially and permanently shall incur the same penalty.

(3) The attempt shall be punishable.

It is also conceivable that the perpetrator deliberately attacks a hospital in order to disrupt internal digital systems. Damage to life supporting systems, for example, could cause patients to suffer from physical injury or even lead to their death. Here, Section 223 of the Criminal Code would apply for bodily harm and Section 212 of the Criminal Code for homicide.

The attacker, however, does not always intend to harm his victim or to commit homicide. Would it be the case that someone ends up being injured or killed, the perpetrator would

commit negligence in a personal injury (Section 229 of the Criminal Code) or negligent homicide (Section 222 of the Criminal Code).

Conclusion: The main perpetrator of a DDoS attack commits a criminal offence according to the German Criminal Code, Section 303b.

4.1.2 Criminal liability for honeypot deployment

From an objective point of view, the honeypot operator could be seen as someone who participates in DDoS attacks. In Germany there are two forms of participation during a criminal offense: either the person is the principal of the committed crime (Section 25 of the Criminal Code) or he is an accessory (Sections 26, 27 of the Criminal Code).

4.1.2.1 Perpetration and incitement

The honeypot neither performs this type of attack by his own nor incites others to do so. Therefore, the operator is neither a principal nor an indirect perpetrator of the crime according to Section 25 I of the Criminal Code.

Inciting a crime according to Section 26 of the Criminal Code requires a communication element between the author and the indirect perpetrator. It is necessary that the instigator influences the indirect offender to commit the crime. This communication element does not take place when it comes to a DDoS attack. A criminal responsibility as an instigator to a crime under Section 26 of the Criminal Code is therefore out of the question.

4.1.2.2 Accessory in computer sabotage, Section 303b I Nr. 2, 27 of the Criminal Code

However, the operator could be seen as an accessory or accomplice during the computer sabotage (Section 303b I Nr. 2, 27 of the Criminal Code). For this to be the case, the honeypot's operator would need to have the intention to assist the (principle) perpetrator during the crime. The DoS attack itself is an illegal act under Section 303b I Nr 2 of the German Criminal Code (see above).

Section 27

Accessory

(1) Any person who intentionally assists another in the intentional commission of an unlawful act shall be convicted and sentenced as an accessory.

(2) The sentence for the accessory shall be based on the penalty for a principal. It shall be mitigated pursuant to section 49(1).

4.1.2.2.1 Assistance to the crime

The perpetrator must have committed the crime through the honeypot. "Assistance to the crime" means every action that facilitates or leads to the execution of the crime. The assistance can be both: physical and psychological.

Seen from an objective point of view, honeypots are meant by the attacker to become part of the DoS attack. Honeypots transfer data to the victim which may cause the server to shut down. It is doubtful whether each participating bot in a DDoS attack is cause for the success. Many requests may even arrive after the shut down and therefore not be causal. Assistance according to the meaning of Section 27 of the Criminal Code does not have to be causal in the sense of the "condition sine qua non" formula for the success. It is sufficient if the risk

for the success is facilitated. In this case, the honeypots contribute to overloading the system. Thus, honeypots support the offense, according to Section 303b I Nr 2.

4.1.2.2.2 Criminal Intent

For the subjective part, in order to be considered as an assistant to the crime, the operator must have a so-called "doubled accessory intent". This means that he must both accept the intentional (main) offense, and intend to facilitate it.

4.1.2.2.2.1 Intent towards the crime

In this case, the main offense is the computer sabotage (Section 303b I Nr. 2 of the Criminal Code). The accomplice's intention has to refer to this offense. The accomplice does not need to know the exact circumstances of the case. It is sufficient if the accomplice has an approximate idea of the crime.

It is sufficient for the intention of the accomplice if he tacitly accepts the main crime (so-called eventual intent).

The honeypots are installed with the intention to be found by potential attackers. The situation is different if the operator is confident that the attack will not take place. It would then be considered only as a negligent act, which would not be punished.

In case of a DDoS attack, there could be doubt if the accomplice (operator) actually tacitly accepts the crime or not. The fact of operating a honeypot does not mean (in principle) that the operator agrees with the DDoS attack. However, this also does not mean that the possibility of complicity is to be excluded. It is generally accepted that the accomplice does not necessarily have to have a particular interest in the crime. Even if the accomplice disapproves of the crime itself, he can still be punished as an accomplice.

However, the operator of the honeypot has to have at least a vague concept of the specific crime. It is not sufficient, if the operator tacitly accepts all potential IT-related criminal offences.[38] But for the planned SISSDEN honeypots the later seems to be the case. They are meant to passively await connections and collect all sorts of malware that may be used for criminal offenses, including e.g. DDoS attacks, ransomware, trojans, data espionage, data theft, data sabotage, or even bitcoin mining. The whole point of honeypots in the SISSDEN scenario is that the researchers don't have a clear picture of the current threat landscape and therefore gather information via those honeypots. The intent therefore is not sufficiently appropriated with regard to the specific DDOS attacks exploiting the honeypots.

Conclusion: The operators of honeypots lack the necessary knowledge and intent to act as an accessory for data sabotage, unless intentionally neglecting security measures (Section 303b I Nr. 2, 27 of the German Criminal Code).

4.1.2.2.2.2 The intent regarding the aid action

It is necessary to analyse if there is really the intention to aid the offender. The main offender does not necessarily need to recognize the support. For the operator to be punished as an accomplice, the offender does not have to know that he has fallen into the honeypot trap. The vulnerable system of the honeypot may facilitate the attack. The operator of the honeypot is aware of that.

[38] See BGH, Beschluss vom 28. 2. 2012 – 3 StR 435/11.

However, the deployment of honeypots by CERTs or researchers would be considered as "occupationally typical" and therefore "neutral" behaviour. Courts and scholars agree that, if the aid action itself is considered occupationally typical, there are additional requirements regarding the intent on the aid action. They require positive knowledge of the crime or even malicious intent.[39] Since the honeypot operators in our SISSDEN case do not know specifics of the criminal offences trying to exploit the honeypots – these may even happen months or years after the initial deployment – they have neither knowledge or malicious intent.

4.1.2.2.3 Illegitimacy

Additionally, the operator of the honeypot could be legally justified.

There is no "emergency aid" (Section 32 of the Criminal Code) situation to justify the support. Configuring a honeypot is not a suitable means to avert DDoS attacks.

The consent of the victim could also be seen as a justification. This presupposes knowledge of the "victim". This is not the case, basically due to the anonymity of the Internet. The situation is different when the attacked company has its own IT security department and establishes a honeypot for analysis purposes.

Because attacks do not stop taking place due to honeypots and the threatening situation is in general not recognizable for the victim, the idea of a "presumed consent" of the victim does not help, either.

Section 34 of the Criminal Code, which provides a justification in case of imminent danger, also does not apply because the operation of a honeypot does not aver the concrete danger to the victim.

The act (operating a honeypot) could be justified, however, under the aspect of fundamental rights (freedom of scientific research).

In other aspects of (criminal) law we can find justifications, which are also derived from the freedom of scientific research. Section184 b V of the Criminal Code is an example. According to this paragraph, those who distribute child pornography will not be punished, if the act serves exclusively the lawful fulfilment of official or professional obligations. This exemption intends to exclude, among other reasons, scientists from a punishment, when their intention is to perform scientific research. Even though this recognized justification is derived from the fundamental right of freedom of scientific research, it cannot be used as a general rule: It relates to one specific section of the Criminal Code only.

A justification might, however, be derived directly from the freedom of scientific research, as laid down in Article 5 III Alt. 2 of the German constitution.

However, deriving a direct justification from fundamental rights is highly controversial. The German Federal Constitutional Court is of the opinion that there is an interdependency between fundamental rights and criminal law, so a justification is not generally excluded. This leads to the question whether it is possible or not to derive a justification from this specific fundamental right.

In criminal law, there is a system of recognized justifications, but this does not mean that other justifications are excluded. Therefore, **a justification from Art 5 III 2 of the German constitution is conceivable.**

[39] See for more details Joecks, Münchener Kommentar zum StGB, 3. Auflage 2017, Section 27 Rn 49-78.

There is, however, much uncertainty when it comes to the question whether fundamental rights can be used or not directly as a justification in a criminal case. Opinions in the jurisprudence are divided. The prevailing doctrine however denies the possibility of directly applying fundamental rights as a justification. This means that the effects of fundamental rights must be considered when applying the "simple" existing justifications. For example, Art 8 of the German constitution grants the fundamental right to demonstrate. When interpreting Section 240 II of the Criminal Code, one has to decide whether a coercion is reprehensible; here, the value of Art 8 of the German constitution must be considered. In the context of Section 193 of the Criminal Code, fundamental rights, such as freedom of expression (Art. 5 of the

Because of methodological reasons, the idea of the freedom of science as a general justification must be rejected. The problem of honeypots is that the individual case plays a decisive role in the end. The operator (scientist) does not know the victim of the DDoS attacks, thus he cannot perform a risk assessment.

Moreover, the system of justifications conceived in the Criminal Code is sufficient to consider fundamental rights, so there is no room for additional justifications by directly applying the freedom of scientific research.

The requirements for a "wrong assumption of being justified" are also not given. The operator of the honeypot is not mistaken about the existence of a recognized justification.

Conclusion: Based on these considerations: Although the honeypot operator is not justified by research purposes, deploying and operating honeypots does not constitute sufficient intent for an accessory of computer sabotage (Section 303b I Nr. 2, 27 of the German Criminal Code).

4.1.2.3 Aid for further offenses

As initially outlined, DDoS attacks can also cover other offenses such as extortion (Section 253 of the Penal Court) or damage to property (Section 303 of the Penal Court). Therefore, the question if the operator helps the perpetrator to do these "other" offenses rises again.

An aid to extortion under the aspect Sections 253, 27 of the Criminal Code cannot be considered due to a lack of subjective facts.

To be punished, the operator would need to have double intention: concerning the aid provided and concerning the main offense. The aid must therefore know that the main offense is extortion. However, the operator of the honeypot will usually not know the peculiarities of the individual case.

This also means that neither the aid to commit damage to property (Sections 303 I 27 of the Criminal Code), nor injury to others (Sections 223 I, 27 of the Criminal Code) nor homicide (Sections 212 I, 27 of the Criminal Code) come into question.

The aid to a negligent personal injury according to Section 229 of the Criminal Code or to a negligent homicide according to Section 222 of the Penal Court is not possible from a dogmatic point of view, according to Section 27 I of the Penal Court.

4.1.2.4 Negligence of the accomplice

Before investigating negligence crimes it must be said that the differentiation between principal and accomplice/accessory outlined is only related to intentional offenses. When hospitals are victims of DDoS attacks, and (for example) life sustaining systems fail as a

result, people could be injured or end up dead. This brings then into question if the honeypot operator commits a negligent injury according to Section 229 of the Criminal Code or even a negligent homicide according to Section 222 of the Criminal Code. This would be the case if the operator could realistically expect that health or life is being threatened by the attack.

4.1.2.5 Use of honeypots with limited data rate

In the criminal investigation it was assumed that honeypots are used without a limited data rate. However, limiting the rate of data could have an impact on the previous criminal analysis.

In the case of a limitation the potential threat to the victim is considerably reduced. Limiting the data rate exercises reasonable care thus ruling out negligence.

Conclusion: Deploying and operating honeypots may constitute the risk for a negligent offense, if individuals are hurt in the attack.

4.1.2.6 Risk considerations

The present investigation concludes that the operation of honeypots is may be associated with criminal risks.

It should be clear that there is no assured jurisprudence regarding the legal issues related to honeypots. In particular, there is still a lack of relevant court rulings. Ultimately the courts will be the ones who decide on the liability to prosecution of the honeypot operator.

The intensity of the attack or its impact on the victim are decisive criteria for the criminality of the operator. Section 303 b of the Criminal Code requires that a data processing is significantly disturbed. It depends on the respective system of the victim whether it is enough (and what kind of intensity is required) to disturb his system.

Recommendation: To minimize the risk of negligent offenses, it is important to rate limit outbound traffic of the honeypot to the minimum necessary for analysing the attack.

4.1.3 Sandboxes

Regarding the operation of sandboxes to execute malware samples, the assessment of criminal law holds similar results. The operator does not have sufficient knowledge or intent regarding the specific offence the malware performs and thus cannot be considered accessory. To avoid negligence, it is equally important as for honeypots to limit the outgoing communication to the absolute minimum and to closely monitor and intervene, if harmful network activity is detected.

Recommendation: To minimize the risk of negligent offenses, it is important to restrict network access of the malware in the sandbox and the outbound data rate to the minimum necessary for analysing the malware behaviour. In addition, reasonably expectable harmful actions that are typically performed by malware should be contained, such as sending email spam.

4.1.4 Port scans / Active Network Probes

TCP or UDP port scans for research purposes could be punishable as data espionage, Section 202a I of the German Criminal Code. According to Section 202a it is a punishable offense to obtain access to protected data without authorization by circumventing security measures. The operator of the port scan or active network probe gains data regarding the services

without authorisation of the services owner. However, the most relevant criterion regarding the assessment of potential data espionage via port scans is the circumvention of security measures. As port scans can by definition only get data from open ports – whether they are open intentionally or unintentionally – there are no security measures in place which would be circumvented. The potential fact that the owner of the system is unaware or opposed to the port scan is not considered a security measure.

Conclusion: Port scans and network probes are not considered criminal offenses according to German criminal law.

Recommendation: If a port scan accidentally overloads the scanned system, the same argumentation as for DDoS attacks above is applicable. Thus, it is recommended to monitor port scans and exercise reasonable care to limit the (unlikely) risk of overloading systems with the port scan requests.

4.2 Polish criminal law

In general, the Polish criminal regulations are in line with both German and Dutch criminal law. Polish regulation of computer-related offences is shown in the Chapter XXXIII of Polish Criminal Code – Offences against the protection of information and in majority is in force since 2004 when Poland implemented the Council of Europe's Cybercrime Convention, signed on 23 November 2001.

For the purpose of SISSDEN's analysis the following provisions of Polish Criminal Code should be taken into account: article 268 § 2 - making difficult to obtain knowledge of the information when the information is a record on an electronic information carrier, article 268 a – destroying of computer data, article 269 a - interfering with the functioning of a computer system, article 269 b – manufacturing of computer programs and 269 c – legal defense of actions to detect errors in the security of information systems.

What is particularly important in Polish regulations is that the prosecution of the most of the offences mentioned above occurs on a motion of the injured person. That means that without a prior motion of the particular person (individual or a company) who suffers from the offence the prosecution cannot commence. When, however, the motion is placed the prosecution is in progress and the motion cannot be withdrawn without the consent of the prosecutor or the court.

4.2.1 Article 268 § 2 – making difficult to obtain knowledge of the information when the information is a record on an electronic information carrier and article 268 a – destroying of computer data

> ***Article 268.*** *§ 1. Whoever, not being authorized to do so, destroys, damages, deletes or alters a record of essential information or otherwise prevents or makes it significantly difficult for an authorized person to obtain knowledge of that information,*
>
> *shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.*
>
> *§ 2. If the act specified in § 1 concerns the record on an electronic information carrier, the perpetrator shall be subject to the penalty of deprivation of liberty for up to 3 years.*

§ 3. Whoever, by committing an act specified in § 1 or 2, causes a significant loss of property

shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 4. The prosecution of the offence specified in § 1-3 shall occur on a motion of the injured person.

Art. 268a. *§ 1. Whoever, without being authorized to do so, destroys, damages, removes, changes or makes an access to data difficult or in a significant way disrupts or prevents from the automatic process, gathering or transmission of such data,*

shall be subject to the penalty of deprivation of liberty for up to 3 years.

§ 2. Whoever, by committing an act specified in § 1, causes a significant loss of property

shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 3. The prosecution of the offence specified in § 1 or 2 shall occur on a motion of the injured person.

In Polish jurisprudence both article 268 § 2 and § 3 and article 268a are considered to criminalize a DoS or DDoS attack.

Both offences are of common character what means that they can be committed by anyone who not being authorized to do so acts in a way described in these articles.

Authorization mentioned in both provisions can be derived from a provision of law or from a decision of the disposer of the carrier or data.

Also, both offences can only be committed intentionally – with direct intention or possible intention. In Polish law, a prohibited act is committed intentionally, if the perpetrator intends to commit it, that is, he wants to commit (direct intention) it or by anticipating the possibility of committing it, he agrees (possible intention).

When it comes to article 268, what is particularly interesting is that Polish legislator has foreseen higher penalty if the criminal act concerns the record on an electronic information carrier.

A graded type of both prohibited acts is connected with causing of significant loss of property.

As it was mentioned above, both offences can only be prosecuted when a respective motion of the injured person is placed.

Finally, it must be stressed that both offences are only committed when the consequence of the respective act is stated by the court – regarding article 268 § 2 the consequence must be destroying, damaging, deletion or alteration a record of essential information or otherwise preventing or making it significantly difficult for an authorized person to obtain knowledge

of that information; regarding article 268a the consequence must be destroying, damaging, removing, changing or making an access to data difficult or in a significant way disrupting or preventing from the automatic process, gathering or transmission of such data.

With regard to SISSDEN research, we have already established that any participation in a DoS or DDoS attack is not intentional. Therefore, article 268 § 2 and § 3 and article 268a of Polish Criminal Code are not applicable in the case of SISSDEN data or SISSDEN systems being misused by an attacker to carry out a DoS attack.

4.2.2 Article 269 a - interfering with the functioning of a computer system

> ***Art. 269a.*** *Whoever, without being authorized to do so, by transmission, destruction, removing, damaging or changing information data, in significant manner disrupts the work of a computer system, teleinformatic system or a teleinformatic network,*
>
> *shall be subject to the penalty of deprivation of liberty for a term of between 3 months up to 5 years.*

The subject of protection in this provision is a safe working of computer or information system or teleinformatic network and in consequence – the availability and integrity of the data being processed in these systems or networks.

According to the most of the legal writings this provision can be applied to any act which is an attack on the safety of a system or a network, including DoS and DDoS.

This offence can only be committed intentionally – with direct intention or possible intention. In Polish law, a prohibited act is committed intentionally, if the perpetrator intends to commit it, that is, he wants to commit (direct intention) it or by anticipating the possibility of committing it, he agrees (possible intention).

This offence is only committed when the consequence of respective act is stated by the court – the consequence should be significant disruption of the work of a computer system, teleinformatic system or a teleinformatic network by transmission, destroying, removing, damaging or changing information data.

With regard to SISSDEN research, we have already established that any participation in a DoS or DDoS attack is not intentional. Therefore, article 269a of Polish Criminal Code is not applicable in the case of SISSDEN data or SISSDEN systems being misused by an attacker to carry out a DoS attack.

4.2.3 Article 269 b – manufacturing of computer programs

> ***Art. 269b.*** *§ 1. Whoever, produces, acquires, sells off or makes available to other persons devices or computer software adapted to perform a crime mentioned in art. 165 § 1 pt 4, art. 267 § 2, art. 268a § 1 or § 2 in connection with § 1, art. 269 § 2 or art. 269a, and computer passwords, access codes or other data that allow for the access to information stored in an information system, computer system or teleinformatic network,*
>
> *shall be subject to the penalty of deprivation of liberty for up to 3 years.*

§ 1a. No offense is committed if the offender acts solely for the purpose of security of an information system, computer system or teleinformatic network or for the purpose of developing of the method of that security.

§ 2. In case of a conviction for an offense referred to in § 1, the court rules the forfeiture of items, and may decide their forfeiture if they were not the property of the perpetrator.

This provision was added to Polish Criminal Code in 2004 with the exception of § 1a which was added in 2017.

The offence criminalized in this provision is some form of preparation of committing the offences described in articles 165 § 1 pt 4, article 267 § 2, articles 268a § 1 or § 2 in connection with § 1, articles 269 § 2 or art. 269a.

This offence can only be committed intentionally – with direct intention or possible intention. In Polish law, a prohibited act is committed intentionally, if the perpetrator intends to commit it, that is, he wants to commit (direct intention) it or by anticipating the possibility of committing it, he agrees (possible intention).

By the revision of this provision done in March of 2017 the Polish legislator intended to exclude the criminal liability of the offender if his actions described herein are undertaken only for the purpose of security of an information system, computer system or teleinformatic network or for the purpose of developing of the method of that security.

Bearing in mind that the SISSDEN project aims to collect information about malware infections and other network threat activities it is justified to declare that the actions in the project shall not be found the offence criminalized in article 269b of Polish Criminal Code.

4.2.4 Article 269 c – legal defense of actions to detect errors in the security of information systems

Art. 269c. Whoever acts solely for the purpose of security of an information system, computer system or teleinformatic network or for the purpose of developing of the method of that security shall not be subject to the penalty for the offence specified in article 267 § 2 or article 269a if he immediately notifies the disposer of that system or network about the threats disclosed and his acting did not infringe any public or private interest and did not cause a loss of property.

This provision was added to Polish Criminal Code in March of 2017 for the purpose of protection of people testing the systems and networks. It is intended to protect not only the people testing the systems and networks on the request of the disposer of the system or network but everyone who acts solely for the purpose of security of an information system, computer system or teleinformatic network or for the purpose of developing of the method of that security provided however that the offender immediately notifies the disposer of that system or network about the threads disclosed and his acting did not infringe any public or private interest and did not cause a loss of property.

Conclusion:

All the criminal provisions of Polish criminal law require intentional behavior of the offender therefore they are not applicable to the SISSDEN research. Parallel to the

considerations for German and Dutch Criminal law, the central question is, whether SISSDEN deploying vulnerable systems or sharing network traffic data with third parties could negligently enable attackers to misuse these data and systems to carry out attacks. Without judicial precedent with regard to IT security research it is difficult to predict, whether a court would consider researchers publishing network traffic data or deploying honeypot systems as negligent behavior or to be causal for a following attack by a third party.

Unlike German and Dutch criminal law however, Polish law provides a number of cases excluding the criminal liability when the offender acts for the purpose of security of an information system, computer system or teleinformatic network or for the purpose of developing of the method of that security. Therefore, the risk of possible infringement of criminal law in Poland with SISSDEN systems is possibly lower.

4.3 Dutch criminal law

Similarly to most EU Member States, the Netherlands have issued an extensive cybercrime legislation including criminal law.

The first bill to specifically address IT-related crimes was the Computer Crime Act (Wet computercriminaliteit) in 1993, which was included into the Dutch Criminal Code (Wetboek van Strafrecht. In 2006 the Dutch Criminal Code had a major revision to implement the Council of Europe's Cybercrime Convention, which the Netherlands signed on 23 November 2001.

Most relevant for the SISSDEN research practices are the criminal offences of computer trespassing (DoS attacks) (Section 138b), unlawful interception (Section 139c), and computer sabotage (Section 161sexies). To a lesser extent data manipulation (Section 350a) might have to be considered.

In contrast to other EU Member States when interpreting Dutch Criminal Law we have to consider prosecutorial discretion (opportuniteitsbeginsel). "This means that the Public Prosecutor decides whether or not it is expedient to prosecute someone for an offence. A consequence of this principle for substantive law is that criminal provisions may be formulated broadly, covering acts that may not in themselves be very worthy of criminal prosecution; for example, changing without authorisation a single bit in a computer already constitutes damage to data (Article 350a DCC), but will usually not be prosecuted."[40]

4.3.1 Computer Trespassing (DoS attacks), Section 138b of the Criminal Code

Section 138b

Any person who intentionally and unlawfully hinders the access to or use of a computerised device or system by offering or sending data to it shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category.

This provision includes the requirement of "intentionally" hindering. With regard to SISSDEN research, we have already established that any participation in a DoS or DDoS attack is not

[40] Bert-Jaap Koops, 'Cybercrime Legislation in the Netherlands', Electronic Journal of Comparative Law, vol. 14.3 (December 2010), p. 2.

intentional. Therefore, Section 138b is not applicable in the case of SISSDEN data or SISSDEN systems being misused by an attacker to carry out a DoS attack.

4.3.2 Unlawful Interception, Section 139c of the Criminal Code

Section 139c

1.

Any person who intentionally and unlawfully intercepts or records by means of a technical device data which is not intended for him and is processed or transferred by means of telecommunication or by means of a computerised device or system, shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category.

2.

Subsection (1) shall not apply to intercepting or recording:

[...]

2°. by or on the instructions of the person entitled to use the telecommunication connection, except in cases of obvious misuse;

3°. for the purpose of a good operation of a public telecommunication network, for the purpose of criminal proceedings, or for the purpose of implementation of the Intelligence and Security Services Act 2002.

SISSDEN collects network traffic data only within the own networks of its consortium partners or as the endpoint of a communication (Website, Honeypot, Email, System). Therefore, the communication is intended for the SISSDEN partner, who is intercepting the data. Additionally, SISSDEN partners among each other may be privileged to intercept and record data from other partners under paragraph 2 no. 2, if they are instructed by the entitled partner. This may be a relevant exception from the criminal offense in cases where one SISSDEN partner acts on behalf and under the instruction of another internal or external SISSDEN partner.

4.3.3 Computer Sabotage, Section 161sexies and 161septies of the Criminal Code

"System interference is penalised in various provisions, depending on the character of the system and of the interference. If the computer and networks are for the common good, intentional interference is punishable if the system is impeded or if the interference causes general danger (gemeen gevaar) to goods, services, or people (Article 161sexies DCC). Negligent system interference in similar cases is also criminalised (Article 161septies DCC)."[41]

Section 161sexies

1.

[41] Bert-Jaap Koops, 'Cybercrime Legislation in the Netherlands', Electronic Journal of Comparative Law, vol. 14.3 (December 2010), p. 6.

Any person who intentionally destroys, damages or renders unusable any computerised device or system infrastructure facility or any telecommunication infrastructure facility, causes the defective functioning or operation of such facility, or frustrates a safety measure taken in respect of such facility, shall be liable [...].

2.

Any person who:

a. manufactures, sells, obtains, imports, distributes or otherwise makes available or has in his possession a technical device that has been primarily adapted or designed for the commission of such serious offence, [...] with the intention of using it in the commission of a serious offence, as referred to in subsection (1), shall be liable [...].

Section 161septies

Any person who, through negligence, causes any computerised device or system infrastructure facility or any telecommunication infrastructure facility to be destroyed, damaged or rendered unusable, which results in the defective functioning or operation of such facility, or causes a safety measure taken in respect of such facility to be frustrated, shall be liable [...].

4.3.4 Data Manipulation, Section 350b of the Criminal Code

Section 350b

1.

Any person who, through negligence, causes data stored, processed or transferred by means of a computerised device or system to be altered, erased, rendered unusable or disabled, or causes other data to be added thereto, shall, if this causes serious damage to that data, be liable to a term of imprisonment or of detention not exceeding one month or a fine of the second category.

2.

Any person who, through negligence, causes data intended to cause damage to a computerised device or system to be unlawfully made available or disseminated, shall be liable to a term of imprisonment or detention not exceeding one month or a fine of the second category.

Negligent behaviour under paragraph 1 only constitutes a criminal offense, if serious damage is caused. “Serious damage” includes an information system not being available for several hours due to an attack.[42]

Conclusion:

The criminal provisions requiring intentional behaviour are not applicable to the SISSDEN research. Parallel to the considerations for German Criminal law, the central question is, whether SISSDEN deploying vulnerable systems or sharing network traffic data with third parties could negligently enable attackers to misuse these data and systems to carry out attacks. Without judicial precedent with regard to IT security research it is difficult to predict, whether a court would consider researchers publishing network traffic data or deploying honeypot systems as negligent behaviour or to be causal for a following attack by a third party.

Recommendation:

Considering the risk, it is to be advised that SISSDEN systems have to be closely monitored and data must only be shared after a vetting process to rule out negligent behaviour. Considering the Dutch characteristic of prosecutorial discretion, the criminal offenses are phrased broadly. It is therefore crucial to document the IT security research purpose of SISSDEN’s systems and data sharing platform as well as document the monitoring and technical and organisation security measures the SISSDEN researchers put in place to prevent misuse.

[42] Hoge Raad (Dutch Supreme Court) 19 January 1999, NJ 1999, 25.

5 Privacy and data protection law

5.1 Processing of personal data

5.1.1 According to Directive 95/46/EC[43]

It is questionable whether the saving of data, gained through honeypots, sandboxes or even port scans (see above), is a relevant process in terms of data privacy, for example collection of personal data according to Article 2 (b) Directive 95/46/EC, and whether this is legally permissible.

5.1.1.1 Applicability of Directive 95/46/EC

First of all the Directive 95/46/EC must be applicable in a substantive and territorial way.

5.1.1.1.1 Substantive applicability

Article 3 (1) of the Directive 95/46/EC applies for the processing of personal data in a wholly or partly automatic way.

5.1.1.1.1.1 Personal data

Pursuant to Article 2 (a) of the Directive, personal data are all information concerning a particular or identifiable natural person. The natural person is then referred as data subject. A person can be considered determinable if he can be identified directly or indirectly. This applies if there is an identification number or if specific elements allow conclusions to be made on the physical, psychological, economic, cultural or social identity. For the DDoS attack monitoring and port-scans, it is in particular the IP address of the victim, which could represent personal data. For IP addresses, the ECJ ruled in its judgment of 19 October 2016 that both static and dynamic IP addresses represent personal data.[44] For dynamic IP addresses this only applies if the responsible authority has legal means which allow it to determine the data subject by means of the additional information about the Internet access provider.[45] Whether this is the case depends on the legal possibilities within the respective Member State[46] and therefore cannot be assessed globally. For the SISSDEN project, it seems reasonable to assume that IP addresses, regardless of national law, are to be viewed as personal data. In the case of malware analysis, it is not impossible that a malware tries to download personal data, such as email addresses, in order to carry out further attacks. Furthermore, the responses of port-scans may include personal data, in addition to IP addresses, e.g. in the response to "monlist" (NTP) or in SSDP packets.

Conclusion: Within the framework of SISSDEN personal data is present.

5.1.1.1.1.2 Processing of personal data

In addition to the existence of personal data, their processing according to Article 3 (1) of the Directive is also a prerequisite. The concept of processing is broadly defined in Article 2 (b) and encompasses not only the recording and transmission of personal data but also the collection of such data. The form of data processing must be fully or partially automated

[43] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

[44] ECJ, Judgment from 19.10.2016, Case C‑582/14, ECLI:EU:C:2016:779, para. 49.

[45] Ibid.

[46] ECJ, Judgment from 19.10.2016, Case C‑582/14, ECLI:EU:C:2016:779, para. 47.

happen. In the case of the DDoS honeypots, SISSDEN stores the packet sent by the attacker to the honeypot. This packet contains the IP address of the victim. The IP address of the victim is a personal data (see above) regardless of whether it is relative or absolute. Thus, this technique provides for the collection of personal data. For the sandboxing of malware, it is initially unclear from the perspective of SISSDEN whether or not the malware downloads personal data, such as e-mail addresses, to the sandbox. If this is the case, there is a processing of personal data, otherwise the use of sandboxes is not a data protection relevant process.

Portscans are not used by SISSDEN and their use would introduce additional personal data. If a vulnerable port is detected on a system, the system's IP address and response packets would be stored. In the case of NTP, the response packets contain the IP addresses of the last 100 clients. In the case of SSDP the device names on the local network are included. For DNS, SNMP, CharGen, QOTD, and NetBIOS, the response packet contains undefined data. As already stated, IP addresses represent personal data. This also applies to NTP. SSDP response packets can also include personal data, for example when a device bears the name of a natural person. The content of the response packages is not relevant in the case of SSDP and NTP. After a measurement of the size of the response packets (number of bytes), the content can therefore be deleted. Nevertheless, collection of personal data in case of SSDP and NTP would occur from a legal point of view. A subsequent deletion therefore does not eliminate the previous collection. The other IP addresses (honeypots) are stored, used for analysis purposes, and transmitted to ISPs and CERTs (see below). This is also done in an automatic way.

Conclusion: The prerequisite "processing of personal data" is regularly fulfilled.

5.1.1.1.1.3 Exemptions from the applicability

Article 3 (2) of the Directive contains several exemptions which are not covered by the processing of personal data. On the one hand, the Directive is not intended to apply to data processing in the context of an activity which is not covered by the law of the European Union. This means, for example, public security, defense or the security of the state. Furthermore, the Directive is not intended to apply to the processing of personal data if it is carried out by a natural person solely for private or family purposes. For SISSDEN, none of these exemptions are relevant.

5.1.1.1.1.4 Controller

Although it is not a written prerequisite for the applicability of Directive 95/46/EC, there must be a responsible body for data processing. The responsible body is defined in Article 2 (d) of the Directive and referred to as a "controller". Controller is any natural or legal person, authority or entity that alone or together with others decides on the purposes and means of the processing of personal data. Initially, SISSDEN is not an independent organization but a research project. However, this does not preclude a joint controllership for processing if the project partners jointly decide on the purposes and means of the processing of personal data.[47] The data protection obligations from the Directive then apply to all project partners.[48] The key question when assessing whether a joint controllership is whether one

[47] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, adopted on 16 February 2010, 00264/10/EN, WP 169, P. 18.

[48] Ibid.

party alone decides on the purposes and means or whether this decision is taken jointly.[49] Within the framework of the joint control, the participation must not be equally shared and may take different forms.[50] The central element of the joint controllership is that responsibility for compliance with data protection regulations and possible violations of these provisions is clearly assigned.[51] For SISSDEN, all project partners determine the purpose and the means by which the processing of personal data takes place. To a large extent, these are already defined in the work of the research project. For this reason, SISSDEN can therefore be regarded as a joint controller.

Conclusion: SISSDEN is joint controller.

Recommendation: All project partners of SISSDEN already declared themselves responsible for compliance with data protection regulations. One project partner should act as a first point of contact for data protection requests and be mentioned in this function on the website.

5.1.1.1.2 Territorial applicability

Directives are binding for all Member States of the European Union.[52] All Member States have transformed the provisions in a Directive into national law.[53]

Conclusion: The Directive 95/46/EC is applicable in a substantive and territorial way.

5.1.1.2 Principles relating to data quality

Under the title "Principles Relating to data quality" the European legislator has established a number of principles for the processing of personal data in Article 6 of the Data Protection Directive. In principle, according to subparagraph (a), personal data must be processed fairly and lawfully. According to subparagraph (b), this must be done for clear and legal purposes. Further data processing for historical, statistical or scientific purposes is not to be regarded as generally incompatible with previous purposes. For SISSDEN, this means that data collected on a different legal basis can nevertheless be used for the research work, when there is an appropriate safeguard. Subparagraph (c) and (d) specify that only necessary data may be collected (data minimization) and that the data must be accurate. Latter means that incomplete or incorrect data must be deleted or corrected. After subparagraph (e), personal data may be collected or further processed only to the fulfilment of purpose. If this is done, data may only be processed in an anonymous form. For historical, statistical or scientific purposes, the Member States are required to adopt a regulation. For this reason, no global statements can be made here.

5.1.1.3 Criteria for making data processing legitimate

A justification is necessary for the legal processing of personal data. The European law prohibits the processing of personal data unless a permission is given. Article 7 of the Directive provides possible permissions in descending form from consent to a legitimate interest. The legal grounds mentioned in subparagraphs (a) to (e) are not considered within the framework of the project. The project partners can neither recover the consent of the

[49] Ibid.

[50] Ibid., P. 19.

[51] Ibid., P. 22.

[52] Art. 288 Treaty on the Functioning of the Union (TFEU).

[53] Ibid.

affected person nor are they in agreement with this. Another legal obligation to collection of personal data is also not visible. Similarly, the justification in subparagraph (d) for processing in the event that the interests of the data subject are of vital concern are, regularly, not present. Subparagraph (e) allows the processing of data in the case of the performance of a task which is in the public interest or is carried out in the exercise of public authority. In both cases a formal act of entrusting is mandatory which is not available in the case of SISSDEN.

A justification for the processing must therefore be based on the reasons given in subparagraph (f). Article 7 (f) requires a balance between the interest of the controller and the privacy interest of the data subject.[54] For the benefit of the data subject, it must be taken into account that any data processing is associated with dangers. The heart of the SISSDEN project is a global sensor network, which is operated by the project consortium. This provides insights about ongoing attacks within the Internet. The network is supplemented by a malware analysis and other external data sources. This allows SISSDEN to inform not only the victim but also other organizations such as CERTs, ISPs, hosting providers and law enforcement agencies about ongoing attacks. This is particularly the case for the citizen, but also for small and medium-sized enterprises, which alone do not have the capacity to counter such attacks. For this reason, SISSDEN provides an important contribution to the prevention of cybercrime and creates the possibility of effectively preventing security breaches. In addition, the data collected by SISSDEN is a major contribution to research on cybersecurity and thus also serves the development of new defense strategies. It should also be borne in mind that no specific categories of personal data (Article 8) will be processed. Rather, the data processed by SISSDEN is classified as less sensitive because conclusions on the data subject are not immediately possible for everyone (even for SISSDEN). In order to achieve the purposes pursued with SISSDEN, it is necessary to store the IP addresses in a non-anonymized form. Only in this way is it possible to carry out a permanent analysis and evaluation of cybercrime. In the field of malware sandboxes it is unclear whether SISSDEN receives any personal data through possible downloads of a malware. It is also unclear which category of personal data it might be. However, this makes the operation of sandboxes from a data protection perspective not illegal. Rather, if a malware downloads personal data to the sandbox, SISSDEN must perform a case-by-case analysis. Within the framework of this individual case analysis, it is necessary to examine whether data subjects or authorities have to be informed, or whether the deletion of the data is sufficient. In view of the interests pursued by SISSDEN and the interest of the individual in the protection of his personal data, this solution appears to be justified. In principle the interests of SISSDEN in data processing seems to predominate, however bearing in mind that the design of the justifications provided for in Article 5 is a task of the Member States.

Conclusion: SISSDEN may process the data obtained by honeypots. The personal data in the case of NTP and SSDP response payloads must be deleted after measuring the size of the response payload.

5.1.1.4 Rights of the data subject

The data subject is entitled to the right of notification, the right of access and the right of objection.

[54] Brühann in: Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Art. 7, Rn. 20.

5.1.1.4.1 Data subject's right of information

Articles 10 and 11 of the Directive provide an obligation for the controller to inform the data subject about the processing. Article 10 is applicable only if the data are collected directly from the data subject. This requires at least an active involvement of the data subject.[55] The data subject must know and consent the collection of data for the purpose of processing.[56] In the case of SISSDEN, however, the data are collected without the data subject being aware of it. For this reason, there is no obligation to provide information under Article 10 of the Directive. However, information might be provided in accordance with Article 11 of the Directive. An information according to Article 11 has to take place about the identity of the controller, the purposes of processing and other information such as the categories of data concerned, the recipients or categories of recipients (in the case of disclosure by transmission) and the data subjects rights of information and rectification. Article 11 does not specify a time for the information. However, the information should be given at the earliest possible time.[57] The Directive provides derogations from the information obligation in Article 11 (2). Paragraph 1 should not be applied if the information of the data subject is impossible or involves a disproportionate effort. This applies in particular to data processing in the context of scientific research. A distinction between impossibility and disproportionate effort can be difficult, but is not absolutely necessary because of identical legal sequences.[58] A lot of effort for the information of the data subject justifies alone no exception.[59] The decisive factor is, rather, an individual case-balancing between the amount of the effort and the interest of the data subject on an information.[60] In the case of SISSDEN, a notification of the data subject is normally only possible with the aid of the IP address. This means that the project partners would have to find out which person is behind the corresponding IP address and then inform them in a different way. Such a search is not possible for SISSDEN, since the IP address without further additional knowledge does not allow to identify the data subject without a doubt. However, SISSDEN does not have any legal basis for gaining additional knowledge, for example by requesting an ISP. Furthermore, current research results show that a contact via the WHOIS information in the case of the Alexa[61] Top 10,000 websites has only a success rate of 16.2%.[62] In the case of the Alexa Top 1 million, the success rate already drops to 6.3%.[63] For this reason, and with regard to the high-ranking interests pursued with SISSDEN, an information on the data subject is not required. Furthermore, an information can be dispensed if a law allows the storage or transfer of personal data. This can be relevant to SISSDEN in case of data transfer to law enforcement agencies (see below).

[55] Ibid., Art. 10, Rn. 7.

[56] Ibid.

[57] Ibid., Art. 11, Rn. 5.

[58] Ibid., Rn. 8.

[59] Ibid.

[60] Ibid.

[61] Alexa Internet, Inc. is an analytics company that offers a global traffic rank of all websites, https://www.alexa.com.

[62] STOCK, B., PELLEGRINO, G., ROSSOW, C., JOHNS, M., AND BACKES, M. Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification. In USENIX Security Symposium (2016).

[63] Ibid.

5.1.1.4.2 Data subject's right of access

The right of access includes, in Article 12 (a), essentially the right of the data subject to get information on the data processing without constraint at reasonable intervals and without excessive delay or expense. According to subparagraph (b), the data subject is entitled to rectification, erasure or blocking of data if the data are not processed in accordance with the Directive. In the case of rectification, erasure or blocking of data, the controller must, in accordance with subparagraph (c), also communicate the changes to third parties to whom the data have been transmitted, if this is not impossible or disproportionate. According to Article 13 (1), the Member States may restrict the right of information in the listed cases, e.g. national security. Although the national law of the Member State applies here, it can be assumed that there is no exception to Article 13 (1) for SISSDEN. Article 13 (2) provides that Member States may adopt exceptions to Article 12, in particular for scientific research where there is obviously no risk to the private sphere of the data subject. A more detailed design is the task of the Member States, which in exceptional cases must provide legal safeguards.

5.1.1.4.3 Data subject's right to object

Article 14 provides a general right of opposition (Article 14 (a)) as well as a right of opposition in the case of direct advertising (Article 14 (b)). The latter seems not relevant to SISSDEN. Within the framework of Article 14 (a), the data subject is at least entitled to a right of objection in the cases referred to in Article 7 (e) and (f). This has an increased relevance for SISSDEN because data processing will be regularly justified by Article 7 (f) (see above). The right to object exists if the data subject provides a legitimate reason which arises from a particular situation of the data subject. By taking into account important individual interests, the data subject should be given the opportunity to influence the overall assessment according to Article 7 (f).[64] This is especially valid in case of active data collection methods (not employed in SISSDEN) – this person may, for example, have a legitimate interest in being excluded from portscans or network probes. In the case of an effective objection, data processing is prohibited and the controller can no longer refer to the data.[65] In order to give the data subject the possibility of an opt-out, SISSDEN will provide a contact opportunity on the website of the project.

Conclusion: For SISSDEN there is no obligation to inform the data subject about the processing. The data subject, however, has a right of access and a right to object with legitimate reasons.

Recommendation: SISSDEN has to provide a contact opportunity on the website of the project to allow the data subject to opt-out from data acquisition and processing.

5.1.1.5 Confidentiality and security of processing

Any data processing must be confidential and secure in accordance with Articles 16 and 17 of the Directive. Article 16 stipulates that persons who are under the responsibility of controller or the data processor may only process personal data on the instructions of the controller. The persons referred to in Article 16 are, for example, workers, freelancers, self-employed subcontractors and their workers, who carry out certain activities on the instructions of the controller.[66] All these persons are bound to confidentiality, which must be

[64] Ibid., Art. 14, Rn. 7.

[65] Ibid., Rn. 9.

[66] Ibid., Art. 16, Rn. 5.

materially arranged by the controller.[67] For this purpose, the controller must make an instruction, for example, within the framework of a work or service contract.[68] The Directive provides for an exception only if there is a legal obligation. This is the case, for example, when a witness makes a statement in court.[69] The rules on the security of the data processing referred to in Article 17 shall cover both the data processing by the data controller and the contract data processing. In the case of SISSDEN, the figure of the contract data processing is not relevant so far, so that the focus is on the obligations of the controller. These are laid down and described in Article 17 (1) and (4). Accordingly, the responsible authority must take appropriate technical and organizational measures to ensure the security of the data processing. The measures are intended to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing. The Directive aims to provide the widest range of protection possible by listing these alternatives.[70] All necessary measures must be taken to prevent potential hazards.[71] This must be done before data processing is started.[72] The nature of the measures is not defined by the Directive. However, the physical security of the server rooms, the strict regulation of access to data, the control of access by means of access protection, and the protection of the data from external intrusion, should be considered.[73] The key concepts of information security provide a useful guide for the design of a security concept.[74]

Conclusion: SISSDEN must ensure that any data processing is confidential and secure.

5.1.1.6 Notification to the supervisory authority

According to Articles 18 and 19 of the Directive, the controller must notify any data processing to the cognizant supervisory authority. This is done by the SISSDEN partners in accordance with the respective national law.

Conclusion: SISSDEN is jointly responsible in the sense of the data protection directive and is bound to the directive for data processing. As long as the data processing is performed on the examined scale, it is legally permissible.

5.1.2 According to Regulation (EU) 2016/679 (GDPR)

With regard to the data protection assessment under the GDPR, it must first be examined which of the data collected in the context of SISSDEN should be regarded as personal data under the new legal situation. Insofar as personal data are available, it must be checked whether the processing of the data within the project can be justified according to the GDPR.

---

[67] Ibid., Rn. 6.

[68] Ibid., Rn. 7.

[69] Ibid., Rn. 11.

[70] Ibid., Art. 17, Rn. 3.

[71] Ibid., Rn. 4.

[72] Ibid.

[73] Ibid, Rn. 6.

[74] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," Availability, Reliability and Security (ARES), 2013 Eighth International Conference on , vol., no., pp.546-555, IEEE, doi: 10.1109/ARES.2013.72, 2–6 September 2013. [http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf]

5.1.2.1 Applicability of Regulation (EU) 2016/679

First of all the GDPR must be applicable in a substantive and territorial way.

5.1.2.1.1 Substantive applicability

According to Article 2 (1) of the GDPR, the GDPR is applicable as far as personal data is fully or partially processed automatically. In addition, it is applicable in cases where personal data is not automatically processed when the data is stored or stored in a file system. There are exceptions to this rule under Article 2 (2) of the Regulation. However, these are not relevant in the context of SISSDEN.[75]

5.1.2.1.1.1 Personal data

The legal evaluation with regard to the Data Protection Directive has shown that personal data can be present within SISSDEN (see above). It is questionable whether this result changes by the application of the GDPR. The crucial point is whether the GDPR leads to an extension of the protection area. Personal data is defined in Article 4 (1) of the Regulation as any information relating to an identified or identifiable natural person (called "data subject"). This definition, at least for the data processed under SISSDEN, is congruent with the definition of the Directive.

Conclusion: In the case of SISSDEN there is no legal difference between the Directive and the GDPR with regard to the presence of personal data.

5.1.2.1.1.2 Processing of personal data

According to Article 4 (2) of the GDPR, the processing of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organization, structuring, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The GDPR confirms the previous definition of the directive.[76] Processing is every handling of personal data.[77]

Conclusion: In the case of SISSDEN there is also a processing of personal data after the GDPR.

5.1.2.1.1.3 Exemptions from the applicability

Exemptions from the applicability of the GDPR within the meaning of Article 2 (2) of the Regulation are out of the question. In particular, SISSDEN does not constitute a competent authority pursuant to Art. 2 (2) (d) of the GDPR.

5.1.2.1.1.4 Controller

By the GDPR, so far only by the Article 29 Data Protection Working Party (see above: 5.1.1.1.1.4.) permitted, joint controllership is legally anchored. The provision is contained in Art. 26 of the Regulation. The aim of the new, explicit regulation is the clear allocation of responsibilities.[78] As regards content, Article 26 (1) presupposes that the definition of the purposes and means of processing personal data is common. In the case of SISSDEN, this is not a problem because both the nature and extent of the data processing, as well as the

[75] Ernst in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Auflage 2017, Art. 2 DS-GVO, Rn. 11ff.

[76] Schild in: BeckOK Datenschutzrecht, Wolff/Brink, 21. Edition, Stand: 01.08.2017, Artikel 4, Rn. 29-32.

[77] Ibid.

[78] Spoerr in: BeckOK Datenschutzrecht, Wolff/Brink, 21. Edition, Stand: 01.08.2017, Artikel 26, Rn. 2.

purpose of this, are coordinated by all project partners. Furthermore, the GDPR requires an agreement in a transparent manner.[79] This is not a requirement for a joint controllership, but its legal consequences.[80] The shared responsibility does not apply in the case of a missing agreement.[81] However, in the case of a missing or incomplete agreement, a fine under Art. 83 (4) may be imminent.[82] With regard to the requirement of transparency, recital 58 of the Regulation can be used as a reference for a wording.

Recital 58 - GDPR

The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

In addition to the content requirements, there are no formal requirements for the agreement. The agreement need not be made in writing nor signed.[83] Nevertheless, it is advisable to make the agreement in writing in order to ensure traceability and provability.[84]

Conclusion: SISSDEN is joint controller.

Recommendation: The project partners should conclude a written agreement on the joint controllership. Such an agreement can look like the following draft:

Joint controllership agreement for the Secure Information Sharing Sensor Delivery Event Network (SISSDEN)

between: [Name and address of each project partner]

[79] Martini in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Auflage 2017, Artikel 26, Rn. 22.

[80] Ibid.

[81] Ibid.

[82] Ibid.

[83] Martini in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Auflage 2017, Artikel 26, Rn. 25.

[84] Ibid.

Preface

(1) This agreement shall specify in a transparent manner which party shall fulfill the respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and the respective duties to provide the information referred to in Articles 13 and 14 GDPR, by means of an arrangement between the parties unless, and in so far as, the respective responsibilities of the parties are determined by Union or Member State law to which the parties are subject.

(2) The provisions of this agreement do not themselves constitute a legal basis for data processing. Unless a separate legal basis for processing is mentioned, processing within SISSDEN is carried out for the purposes of legitimate interests according to Article 6 (1) (f) GDPR.

(3) Irrespective of the terms of this arrangement, the data subject may exercise his or her rights under the GDPR in respect of and against each of the controllers.

§ 1 Joint controllership

The parties agree that they are joint controllers in the meaning of Article 26 GDPR.

§ 2 Purposes and means of processing

(1) The purpose and means of processing is the operation and development of the SISSDEN sensor network and the evaluation of the processed data for the purpose of research and defense against cyber attacks.

(2) If not not already specified under (1) the purpose and means of processing will be determined jointly.

§ 3 General provisions

(1) Contact point for data subjects according to Article 26 (1) GDPR is [PARTY].

(2) The parties and their employees undertake to treat all personal data processed within the framework of SISSDEN confidentially.

(3) Where Article 3 (2) GDPR applies, the affected controller or the processor will designate in writing a representative in the Union according to Article 27 GDPR.

§ 4 Distribution of responsibilities

(1) Responsible for providing the information according to Articles 13 and 14 GDPR is [PARTY].

(2) Responsible for the right of access according to Article 15 GDPR is [PARTY].

(3) Responsible for the right to rectification according to Article 16 is [PARTY].

(4) Responsible for the right to erasure, the right to restriction of processing and the notification obligation regarding rectification or erasure of personal data or restriction of processing according to Articles 17, 18 and 19 GDPR is [PARTY].

(5) Responsible for the right to data portability according to Article 20 GDPR is [PARTY].

(6) Responsible for the right to object according to Article 21 GDPR is [PARTY].

(7) Responsible for determination of technical and organisational measures to ensure a level of security appropriate to the risk of processing according to Article 24 (1) GDPR in conjunction with Article 32 GDPR as well as the data protection impact assessment according to Article 35 GDPR (if necessary) and the prior consultation with the supervisory authority when a data protection impact assessment under Article 35 GDPR indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk (Article 36 GDPR) is [PARTY].

(8) The technical and organisational measures after Article 24 (1) GDPR will be documented by [PARTY].

(9) The technical and organisational measures after Article 24 (1) GDPR will be reviewed and updated by [PARTY].

(10) Responsible for involvement and control of processors or other processors engaged by a processor (Article 28 GDPR) is [PARTY].

(11) Responsible for maintaining the records of processing activities according to Article 30 GDPR is [PARTY].

(12) The notification of a personal data breach to the supervisory authority (Article 33 GDPR) and the communication of a personal data breach to the data subject (Article 34 GDPR) is entirely the responsibility of [PARTY].

(13) If the designation of the data protection officer (Article 37 GDPR) is necessary, [PARTY] is responsible.

(14) The essence of this arrangement will be made available to the data subject by [PARTY].

§ 5 Severability Clause

(1) If a provision of the Agreement is or becomes invalid, illegal or unenforceable, that shall not affect the validity or enforceability of any other provision of this Agreement.

(2) The parties agree to replace, to the extent possible, any invalid Provision with a valid Provision that comes as close as possible to the parties original economic intent.

[Signatories]

Recommendation: All project partners of SISSDEN should declare themselves responsible for compliance with data protection regulations. One project partner should act as a first point of contact for data protection requests and be mentioned in this function on the website.

5.1.2.1.2 Territorial applicability

The territorial scope of the GDPR is set out in Article 3 of the Regulation. The anchoring of the lex loci solutionis in the GDPR results in relevant changes compared to the guideline. In future, the GDPR may also be applicable under Article 3 (2) if the controller is not established in the EU. In the case of SISSDEN, however, the innovations are irrelevant, since the applicability of the GDPR for all project partners already results from Art. 3 (1).

Conclusion: The GDPR is applicable in a substantive and territorial way.

5.1.2.2 Principles relating to data quality

The principles of data processing are regulated in the GDPR in Article 5. Although these principles are generally formulated, they are binding regulations. Infringements are fined according to Art. 83 (5). The principles include the following:

Principle	**Explanation**
Article 5 (1) (a) - “lawfulness”	Personal data may only be processed in a lawful manner.
Article 5 (1) (a) - “fairness”	The principle of fairness describes a duty of consideration in the sense of proportionality. The interests of the data subject should be considered.
Article 5 (1) (a) - “transparency”	The principle of transparency stipulates that data processing must be transparent to the data subject. This applies in particular retrospectively, but also prospectively for future processing. Explanations to the data subject must be clear and in plain language (suitable for the addressee).

Principle	Explanation
Article 5 (1) (b) - "purpose limitation"	The purpose of the provision is an essential principle of data protection law. It first includes the definition of a purpose for the data collection. This purpose must then be observed and adhered to in a second step.
Article 5 (1) (c) - "data minimisation"	Data minimization means three things. First, the processing of the data must be substantial for the purpose it is intended to achieve. Secondly, the survey must be limited to what is necessary for the purpose pursued. Thirdly, the survey must also be appropriate in the context of an appreciative analysis.
Article 5 (1) (d) - "accuracy"	Personal data must be accurate and as far as necessary for the processing to be updated.
Article 5 (1) (e) - "storage limitation"	The principle of storage limitation means that the storage period must be limited to what is strictly necessary. However, for scientific purposes, data may also be stored beyond this period.
Article 5 (1) (f) - "integrity and confidentiality"	These two principles serve to ensure data security within the meaning of Article 32 of the GDPR.
Article 5 (2) - "accountability"	With accountability, the European legislator transfers Opinion 3/2010 of the Article 29 Working Party to the GDPR.[85] Within the framework of the provision, accountability means compliance with the principles already mentioned and the verifiability of compliance.

Some examples in which form the principles of data processing may be relevant, can be found in D7.1 (confidential).

Conclusion: The project partners must ensure that the above principles are respected and can demonstrate this if necessary.

5.1.2.3 Criteria for making data processing legitimate

As already stated with regard to the Directive (see above), any processing of personal data is subject to a prohibition with reservation of permission. Such a permission may result from the exhaustive list of Article 6 (1) of the GDPR. As in the case of the Directive (see above), the justifications referred to in subparagraphs (a) to (e) are not applicable in the case of SISSDEN.

A justification can therefore only be derived from Article 6 (1) (f). As with the Directive, Article 6 (1) (f) requires a trade-off between the controller's interests in data processing and the interests of the data subject in the protection of his personal data.[86] In this context not

[85] Article 29 Working Party, WP 173, Opinion 3/2010 on the principle of accountability.

[86] Albers in: BeckOK Datenschutzrecht, Wolff/Brink, 21. Edition, Stand: 01.08.2017, Artikel 6, Rn. 45.

only legal but also economic and ideological interests of the controller must be considered.[87] In the case of SISSDEN, data subject's interest in his privacy is contrasted with SISSDEN's interest in fighting cybercrime. This interest of SISSDEN is on the one hand the scientific investigation of cybercrime cases, on the other hand, the project partners want to inform victims and relevant authorities about ongoing attacks. In order to ensure the long-term continuation and impact of the results of the project, commercialization of some parts of the project (Analytical Platform and Metrics Dashboard) is also planned after the end of the project period. However, the commercial usability is not in the foreground and is primarily intended to enable further research and development of the techniques used. In addition to IP addresses (honeypots and darknets, traffic monitoring, intrusion detection, malware analysis), SISSDEN also processes other personal data. Spampot collects the sender's e-mail address and other recipients. In the case of bruteforce honeypots, like cowrie, it might be possible that personal data such as names or dates of birth may be entered by an attacker. Furthermore, in cases where the protocol UDP is used, it is conceivable that an attacker sends further, still unknown, personal data. However, this is very unlikely. In addition, a malware could also subsequently download personal data into the sandbox as part of the malware analysis. This is also very unlikely. In these unlikely cases, a case by case approach must always be undertaken in which the interests of SISSDEN in the processing of the data and the interest of the data subject in its privacy are balanced. In all other cases SISSDEN collects only personal data as far as this is directly necessary for the warning of the victim and / or research purposes. An exact list of why the processing of the data is necessary in detail can be found above under "3. Considered Techniques".

However, the interest in data processing by SISSDEN may conflict with the interests of the data subject. Here comes first the interest (of both the victim and the attacker) not to be associated with a cyberattack. On the part of the victim, this interest will regularly consist in not suffering any financial losses due to an image damage. In addition, the attacker will not be interested in storing evidence in view of his criminal behavior. However, it is questionable whether this interest of the attacker is justified at all. This can be left aside if SISSDEN's interest in data processing is higher anyway. As mentioned above, the primary purpose of data processing by SISSDEN is to warn victims of cyber-attacks and to advance research in this area. Commercial interests are in the background. The interest of SISSDEN to warn victims of attacks is likely to be in the majority of cases also in the interest of the victim. Basically, the interests of SISSDEN therefore outweigh the privacy interests of the data subjects.

However, interest in data processing by SISSDEN may conflict with the interests of the data subject. Here comes first the interest (of both the victim and the attacker) not to be associated with a cyberattack. On the part of the victim, this interest will regularly consist in not suffering any financial losses due to an image damage. In addition, the attacker will not be interested in storing evidence in view of his criminal behavior. However, it is questionable whether this interest of the attacker is justified at all. However, this can be left aside if SISSDEN's interest in data processing is higher anyway. As mentioned above, the primary purpose of data processing by SISSDEN is to warn victims of cyber-attacks and to advance research in this area. Commercial interests are in the background. The interest of SISSDEN to warn victims of attacks is likely to be in the majority of cases also in the interest of the

[87] Ibid., Rn. 49.

victim. Basically, the interests of SISSDEN therefore outweigh the privacy interests of the data subject. This applies in particular, as the personal data is stored by SISSDEN only for a limited time.

In addition to the general justification under Article 6 lit. f GDPR can supplement SISSDEN's data processing with Article 89 GDPR. First Article GDPR is applicable to private as well as public research projects.[88] However, in order to benefit from the facilities provided by Article 89 of the GDPR, guarantees must be provided.[89] These are usually the anonymization or pseudonymization of the data.[90] However, given the need for these guarantees, it seems unlikely that SISSDEN should base its processing on this legal basis, as the data becomes worthless for SISSDEN's purposes through anonymisation or pseudonymisation. In addition, the data processing by SISSDEN is justified already under Article 6 (1) f of the GDPR, a recourse to Article 92 GDPR is therefore not necessary.

Conclusion: The data processing within SISSDEN is justified under Article 6 lit. f GDPR.

5.1.2.4 Rights of the data subject

5.1.2.4.1 Overview

On the one hand, the GDPR concretises already existing rights of the data subject resulting from the directive. On the other hand, new rights are created by the GDPR. This makes it necessary to reassess the rights of the data subject also in the case of SISSDEN. The essential rights of the data subject are taken up by the GDPR in Chapter 3 (Articles 12 - 23).

Article 12 sets out general obligations for the rights of the data subject. According to Article 12, the data subject must be informed of his rights in a concise, transparent, intelligible and easily accessible form. The information on existing rights should be provided in writing or otherwise, in accordance with Article 12 (1), in particular electronic form. The perception of the rights by the data subject is basically free of charge and should be made as simple as possible for the data subject. In the case of SISSDEN, information about the rights of the data subject should be provided on the project website.

Recommendation: SISSDEN has to provide an information about the rights of the data subject on the website of the project.

[88] Pauly in: DS-GVO BDSG, Paal/Pauly 2. Auflage 2018, Artikel 89 DSGVO, Rn. 12.

[89] Eichler in: BeckOK Datenschutzrecht, Wolff/Brink, 22. Edition, Stand: 01.11.2017, Artikel 89 DSGVO, Rn. 12.

[90] Ibid.

5.1.2.4.2 Detailed analysis

Article	Legal content	Importance for SISSDEN
Art. 13 GDPR	Article 13 GDPR regulates what information the controller must provide when collecting personal data directly from the data subject. A detailed list of the information to be provided can be found in Article 13 (1) and (2) GDPR. According to Article 13 (3) GDPR, information to the data subject is also required if the data is subsequently collected for a different purpose. According to Article 13 (4) GDPR, the information obligation is omitted if the data subject already has the information.	Article 13 GDPR is only applicable if the data are collected directly from the data subject. For this it is necessary that the data subject participates mentally or physically in the data collection.[91] However, this is not the case with SISSDEN. Therefore, Article 13 GDPR need not be taken into account.
Art. 14 GDPR	Article 14 GDPR contains the information obligations to the data subject if the personal data are not collected from the data subject.	Basically, SISSDEN would have to inform under Article 14 GDPR about data processing. However, Article 14 (5) (b) GDPR implies that information may be omitted if it proves impossible or would require a disproportionate effort. The latter is the case here as already explained under 5.1.1.4.1. An obligation to inform under Art. 14 GDPR does not exist for SISSDEN. However, SISSDEN should take appropriate measures to protect the rights and freedoms as well as the legitimate interests of the data subject, including the provision of this information to the public. A reasonable option for this is the privacy policy on the project website.

[91] Schmidt-Wudy in: BeckOK Datenschutzrecht, Wolff/Brink, 23. Edition, Stand: 01.02.2018, Artikel 13 DSGVO, Rn. 30.

Article	Legal content	Importance for SISSDEN
Art. 15 GDPR	Article 15 GDPR contains the right of access by the data subject. Thereafter, the data subject first has the right to know whether personal data about it is processed (first level) and if such data is processed on further information within the meaning of Article 15 (1) GDPR (second level). The data subject must make a request for this.	The right under Article 15 GDPR must also be respected within the framework of SISSDEN. For appropriate requests, SISSDEN should provide a contact on the project website.
Art. 16 GDPR	The data subject has the right to rectification if personal data are incomplete or inaccurate.	Within the framework of SISSDEN, this right will play a subordinate role, since the data processing within the project is not very inversive and the interests of the person concerned are hardly affected. Nevertheless, SISSDEN should create a process for handling such requests.
Art. 17 GDPR	Article 17 GDPR contains the so-called right to be forgotten. It's a right to erasure, which is used in different cases, e.g. in the case of unlawful processing	Within the framework of SISSDEN, this right will play a subordinate role, since the data processing within the project is not very inversive and the interests of the person concerned are hardly affected. Nevertheless, SISSDEN should create a process for handling such requests.
Art 18 GDPR	The data subject has the right to obtain from the controller restriction of processing if one of the prerequisites in Art 18 (1) is met. In this case the controller must restrict the processing an e.g. transfer data to another processing system, that is blocked for users.	It is very unlikely that a data subject will exercise this right. Nevertheless, SISSDEN should create a process for such requests.

Article	Legal content	Importance for SISSDEN
Art. 20 GDPR	A data subject who has provided personal data to a controller has the right to receive this data in a structured, common and machine-readable format. In addition, the data subject is entitled to transfer this data to another controller without hindrance by the person responsible for providing the personal data. However, this only applies if the processing is based on a consent or a contract and is carried out by automated means	Since SISSDEN processes the data on the legal basis of Article 6 (1) f GDPR there is no need to create a process for data portability.
Art. 21	The data subject has the right to object to processing by the controller at any time if the processing has been carried out in accordance with Article 6 (1) e or f GDPR. The controller shall then no longer process the personal data unless he demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	Since the legal basis of the processing carried out by SISSDEN is Article 6 (1) f GDPR is affected by Article 21. Therefore the project should create a process and name a contact address for objections from data subject. From a legal point of view, SISSDEN's interest in data processing can be regarded as very high (see above), so that an objections will only be justified in exceptional cases.
Art. 22	The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects similarly significantly affects.	The processing carried out by SISSDEN has no legal effect on the data subject. There are also no similarly significantly affects conceivable.

5.1.2.5 Controller's obligations

5.1.2.5.1 Records of processing activities

According to Art. 30 GDPR every data controller is obliged to maintain a record of processing activities under its responsibility. The information that the record must contain is listed in Art. 30 (1) GDPR and includes:

a. *the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;*
b. *the purposes of the processing;*
c. *a description of the categories of data subjects and of the categories of personal data;*

d. *the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;*
e. *where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;*
f. *where possible, the envisaged time limits for erasure of the different categories of data;*
g. *where possible, a general description of the technical and organisational security measures referred to in Article 32(1).*

Recommendation: SISSDEN has to maintain a record of processing activities under its responsibility.

Recommendation: The ICO (UK's data protection authority) has provided a documentation template for controllers which can be used by the project.[92] However using these templates is not mandatory.

5.1.2.5.2 Technical and organisational measures

According to Article 32 GDPR the controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing. The necessary consideration must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The techniques considered in this document (see above "3. Considered Techniques") do not pose a high risk to the data subject. The processed data are primarily IP addresses that, even in the case of actual assignment to a person, do not reveal any risky information. The same applies to the mail addresses collected in the context of Spampot, which at best allow the conclusion that a person has probably received or sent SPAM messages. From this information, however, no serious disadvantages arise for the data subject. Against this background, the data processed in this context does not require much protection. It is sufficient if the standard IT security measures are followed. These can be derived, for example, from the ISO / IEC 27000 series.

Conclusion: For the techniques considered in this document, there is no increased need for technical and organisational measures.

Recommendation: In the future, if the project is to be continued with commercial intent, IT security certification should be conducted in accordance with the ISO / IEC 27000 series or equivalent standards.

5.1.2.5.3 Data breach notification

The GDPR contains several obligations for data breach notifications in Article 33 and Article 34. In principle, a distinction must be made between a notification to the supervisory authority (Article 33 (1) GDPR) and a notification to the data subject. The notification to the supervisory authority pursuant to Article 33 GDPR is the standard case. Basically, the controller shall without undue delay and, where feasible, not later than 72 hours after

[92] The templates can be found on the internet page of the ICO under https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/ or rather https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx.

having become aware of it, notify the personal data breach to the supervisory authority. However, this does not apply if the personal data breach is unlikely to result in a risk to the freedoms of natural persons. In the case of SISSDEN, the techniques considered here are very unlikely to pose a risk to the data subject in the event of a breach of privacy (see above 5.1.2.5.2. Technical and organisational measures). Nevertheless, in the event of a breach of data protection, it should be examined on a case-by-case basis whether a risk has arisen for the data subject. If this is the case, the data protection supervisory authority should be informed. A notification of the data subject according to Article 34 GDPR is only necessary if the personal data breach is likely to result in a high risk to the freedoms of natural persons. This is even more unlikely in the case of SISSDEN, such as the emergence of a risk within the meaning of Article 33 GDPR at all. Nevertheless, a brief examination should take place in individual cases.

Conclusion: It is very unlikely that the supervisory authority or the data subject need to be notified in case of data breach.

Recommendation: If there should be a data breach, it should be checked briefly whether risks have arisen and whether someone has to be notified.

5.1.2.5.4 Data Protection Impact Assessment

The Data Protection Impact Assessment (DPIA) according to Article 35 GDPR is another documentation requirement, that must be fulfilled if “a type of processing [...] is likely to result in a high risk to the rights and freedoms of natural persons”. After Article 35 (7) GDPR the assessment shall contain at least “a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects [...]; and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation [the GDPR] taking into account the rights and legitimate interests of data subjects and other persons concerned.” The Article 29 Working Party has issued a working paper to clarify the cases in which a DPIA is necessary.[93] The first point concerns evaluation and scoring methods for which personal information is used. Since SISSDEN does no scoring of individual users, this doesn’t indicate a DPIA. The second point concerns automated decisions that may have legal or legal-like consequences for the data subject. This also doesn’t indicate a DPIA, because a discrimination of data subject on the basis of the data collected by SISSDEN is very unlikely. Point 3 concerns the systematic monitoring of the data subject. It is primarily about the video surveillance of public places. Point 4 concerns only special categories of personal data and thus excludes them. Point 5 deals with large-scale data processing. To assess whether data processing is taking place on a large scale the Article 29 of Working Party names four other criteria: "the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity”. Whether or not SISSDEN’s data processing is

[93] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev.01), adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017.

at a large-scale is questionable. The large amount of collected data could speak for a DPIA, the small number of data subjects in comparison to the population speaks rather against a data processing at a large scale. However, the Article 29 Working Party does not always see the need for a DPIA for every large scale data processing. So DPIA is not required after the Working Party if an online magazine is using a mailing list to send a generic daily digest to its subscribers. Point 6 concerns the merging of data collected for different purposes. This is not relevant in the case of SISSDEN since all data were collected for the same purpose (see above). Point 7 makes a DPIA necessary if the data subjects are particularly vulnerable persons, such as Children, workers, refugees or old people. Since the isn't the case at SISSDEN's processing this point also doesn't indicate a DPIA. Point 8 concerns data collection through innovative techniques. Here are mentioned application in the framework of the Internet of Things. Since it is primarily about techniques that monitor the person concerned daily and penetrate deeply into the privacy, this point also does not seem relevant for SISSDEN. Point 9 concerns data transfer to third countries. This criterion is very vague and in the opinion of the Article 29 Working Party does not necessarily make a DPIA necessary. A clear statement on this can currently not be made. Point 10 is similar to point 2 and requires an assessment if, for actual reasons, the data subject cannot object to the data processing (e.g., video surveillance in public space) or the data processing itself excludes the data subject from service (e.g. refusal of credit). As a result, the criteria for determining whether a DPIA is required, despite the work of the Article 29 Working Party, are too vague to make a clear statement. There is much to suggest that SISSDEN doesn't have to do DPIA. But until a clear legal situation exists, SISSDEN should nevertheless carry out a DPIA for reasons of caution.

Conclusion: There is much to suggest that SISSDEN doesn't have to do DPIA.

Recommendation: Until a clear legal situation exists, SISSDEN should nevertheless carry out a DPIA for reasons of caution.

5.1.2.5.5 Designation of a data protection officer

Data processing in the context of SISSDEN requires all data controllers within the consortium to designate a data protection officer in accordance with Article 37 GDPR. Therefore each project partner should appoint a data protection officer. The lead organisation's data protection officer should oversee the Joint Controllership (see above). The data protection officer should be independent and must be involved in all issues which relate to the protection of personal data (Article 38 GDPR). His minimal scope of tasks results from Article 39 I GDPR and includes the tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

Conclusion: SISSDEN partners have to designate a data protection officer, if they meet the criteria of Art. 37 GDPR.

Recommendation: The lead organisation's data protection officer should oversee the Joint Controllership.

5.2 Data sharing platform

5.2.1 Data sharing within the project

5.2.1.1 According to Directive 95/46/EC

The SISSDEN project partners are joint controllers for the data processing in the project (see 5.1.1.1.1.4), so no further justification for the data transmission between the project partners is necessary.

Conclusion: Since SISSDEN is a joint controller for data processing, personal data can also be passed on within the project.

5.2.1.2 According to Regulation (EU) 2016/679 (GDPR)

In comparison to the Directive, the application of the GDPR does not result in any relevant legal changes with regard to the admissibility of data transfer within the project.

Conclusion: Since SISSDEN is also a joint controller under the legal framework of the GDPR personal data may be passed on within the project.

5.2.2 Data sharing with ISPs and CERTs

5.2.2.1 According to Directive 95/46/EC

Within the framework of SISSDEN, project partners want to share their insights about ongoing attacks with ISPs and CERTs. These should be able to inform the operators of affected systems, so that they can close existing security gaps. The passed records contain the IP address of the affected system, i.e., personal data (see above). Only the IP addresses that belong to their assigned address range are passed on to the respective ISPs and CERTs. This ensures that only those organizations obtain personal data that can actually influence the course of an attack. We consider initially only ISPs and CERTs within the EU. Data transfers to organizations in third countries must be considered separately. ISPs and CERTs are third parties within the meaning of Article 2 (f) of the Directive. A legal basis for the data transfer can only be Article 7 (f) of the Directive (see above). It is questionable whether the balance of interests will change in favor of the person concerned if personal data are not only collected, but also passed on to the above-mentioned organizations. As already pointed out, SISSDEN provides an important contribution to the prevention of cybercrime and creates the possibility of effectively preventing security breaches. Data transfer to the responsible ISPs and CERTs is an essential part of the intended function. Without the possibility of data transfer to the organizations mentioned, a defense or hindrance of attacks is not possible. This is offset by the interest of the person concerned that his ISP or the respective CERT is not informed about a security breach on his system. At this point it is to be considered that the data subject at least is regularly in a contractual relationship with his ISP and the data transfer by SISSDEN is only transferred to combat security problems. In this case, SISSDEN's interest in the data transfer to improve IT security again underscores

contradictory interests of the data subject. In many cases, transmission will also be in the interest of the data subject. Data transfer to CERTs for the purposes of incident response is also expressly acknowledged as a legitimate reason in the GDPR.[94]

Conclusion: SISSDEN may pass on the relevant IP addresses to the relevant ISPs and CERTs without the consent of the data subject.

5.2.2.2 According to Regulation (EU) 2016/679 (GDPR)

As already mentioned, GDPR Network and Information considers security as overriding legitimate interest according to Article 6 (f) GDPR.[95] For this reason, a data transfer to ISPs and CERTs is also permitted under the GDPR.

Conclusion: SISSDEN may pass on the relevant IP addresses to the relevant ISPs and CERTs without the consent of the data subject also under the legal framework of the GDPR.

5.2.3 Data sharing with the public

5.2.3.1 According to Directive 95/46/EC

The data shared with the public is anonymized in accordance with Recital 26 of the Directive in order to dispense with a person's reference. The data that is then available are no longer personal data within the meaning of Article 2 (a) of the Directive. To ensure that the anonymization is carried out within the applicable data protection law, SISSDEN will implement the requirements of Article 29 Data Protection Working Party.[96] The Article 29 Data Protection Working Party has recognized that, in the case of search engines, the removal of the last octet of an IPv4 address is usually an adequate anonymization.[97] This is considered sufficient because the IPv4 address then only allows the conclusion to the provider or the subnet but it is no longer possible to identify an individual.[98] This means in specific that the information could belong to any of the 254 IP addresses. This form of anonymization is also considered to be sufficient in the case of SISSDEN. Since, after the anonymization, no personal data are available, the data can be shared publicly.

Conclusion: SISSDEN can share anonymized IP addresses with the public.

Recommendation: The last octet of the IP addresses should be stripped for anonymization. However, the consortium is may grant access to the non-anonymized reference data set for privileged research purposes, as described in the following (5.2.4).

5.2.3.2 According to Regulation (EU) 2016/679 (GDPR)

Since the GDPR is also not applicable to anonymized data,[99] data can be shared with public without a legal basis. The requirements for the anonymization (see above) have not changed under the GDPR.

---

[94] A. Cormack, "INCIDENT RESPONSE: PROTECTING INDIVIDUAL RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION", scripted, Volume 13, Issue 3, December 2016, DOI: 10.2966/scrip.130316.258, https://script-ed.org/wp-content/uploads/2016/12/13-3-cormack.pdf

[95] Recital 49 GDPR.

[96] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, 0829/14/EN, WP 216.

[97] Article 29 Data Protection Working Party, Opinion 01/2008 on data protection issues related to search engines, adopted on 04 April 2008, 00737/EN, WP 148, P. 20.

[98] Ibid.

[99] Recital 26 GDPR

Conclusion: SISSDEN can share anonymized IP addresses with the public also under the legal framework of the GDPR.

5.2.4 Reference Data Set for trusted recipients

Additionally, SISSDEN will share reference data sets for research purposes which are not anonymized. In this case the consortium has to install contractual safeguards with the recipient to ensure that the personal data is appropriately handled. Depending on the location of the recipient these safeguards may be a controller to controller agreement with regard to purpose limitation and data handling (EU recipient) or Standard Contractual Clauses (non-EU recipient) (see Section 5.3.2).

5.2.5 Sharing data with law enforcement agencies

5.2.5.1 According to Directive 95/46/EC

The Directive is, by virtue of an exception under Article 3 (2), not applicable in the event of data transfer to law enforcement agencies.

5.2.5.2 According to Directive (EU) 2016/680

Directive (EU) No 2016/680 concerns the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Directive shall apply, in accordance with Article 2 (1), only to competent authorities. These are finally listed in Article 3 (7). Article 3 (7) covers only a public authority or another body or entity entrusted by Member State law to exercise public authority and public powers. This is not the case with SISSDEN, which is why Directive (EU) 2016/680 is not applicable.

5.2.5.3 According to Regulation (EU) 2016/679 (GDPR)

According to Article 2 (7d) GDPR the Regulation does not apply when personal data is processed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. For this reason, there are no rules in the GDPR for data transfer to law enforcement agencies. However, a national obligation for a data transmission is recognized as a legal basis by the GDPR in Article 6 (1c).

5.2.5.4 Application of national law

In the absence of a European regulation, data transfers to law enforcement authorities must be based on the respective national law of the Member States.

Conclusion: There is no European law for data transfer between SISSDEN and law enforcement agencies. Therefore, national law must be applied.

5.3 Data transfer to third non-EU states

This section will introduce contractual and company-internal instruments to cope with the legal issues of international data transfers by the SISSDEN project partners.

The legislative regulation of European data protection enables the transmission of personal data within the area of the European Union. Still, any further disclosure across the borders of the EU/EEA into a third country is not per se covered by such statutory permission. The decisive factor for a lawful disclosure is the existence of an adequate level of protection for the personal data in question. For some countries outside the European Union, this adequate level of protection through legislative measures was acknowledged by the

European Commission. These countries are: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

Nevertheless, this leaves the question open how such an acknowledgement could be achieved in other countries that do not provide such automatic protection by national law. The EU has installed a list of instruments that are deemed to provide the necessary adequate level of protection for personal data, hence permitting the transfer thereof.

Such instruments are:

- The EU/US Privacy Shield
- EU Standard Contractual Clauses (EU SCC)
- Binding Corporate Rules (BCR)

In the following subsections, these instruments will be described and examined with regard to their suitability for data transfers within the SISSDEN project.

5.3.1 EU-U.S. Privacy Shield

On 6 October 2015, the Court of Justice of the European Union had declared the Commission's 2000 Decision on EU-US Safe Harbor invalid. To install a new legal basis for transfer of personal data to the US, the Commission adopted on 12 July 2016 its decision on the EU-U.S. Privacy Shield. Currently, more than 1,000 U.S. companies have registered under the Privacy Shield.

Although the new framework for the adequacy decision has been improved based on the ECJ's criticism, several parties have attacked the validity of the Privacy Shield.

Especially, the Art. 29 Working Party[100] has criticized the lack of specific rules on automated decisions and of a general right to object. Additionally, the Article 29 Working Party would have expected stricter guarantees concerning access by public U.S. authorities and the independence and the powers of the Ombudsperson mechanism. It regrets the lack of concrete assurances that bulk collection and indiscriminate collection of personal data do not take place.

The Privacy Shield has already been challenged before the ECJ similarly to its predecessor. On September 16, 2016 privacy advocacy group Digital Rights Ireland asked for the annulment of the adequacy decision.[101]

Conclusion: During the project duration of SISSDEN, consortium partners can transfer personal data to U.S. data controllers based on the Privacy Shield, if the recipient was registered. To this end, Shadowserver U.S. already started the registration process for Privacy Shield. Alternative legal grounds for the transfer may provide a more long-lived solution.

[100] Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf.

[101] Digital Rights Ireland v Commission, Case T-670/16. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:62016TN0670&from=DE.

5.3.2 EU Standard Contractual Clauses

An instrument to achieve the adequate protection of personal data, compliant with the requirements of the EU Data Protection Directive 95/46/EC, could be the usage of the European Standard Contractual Clauses provided by the European Commission. These complement the contract entailing the primary contractual service agreement and specify them with respect to the European requirements of minimal data protection standards. The possibility of using these clauses is at disposal for European citizens and organisations due to the principle of freedom of contract that underlies the contract law of all European countries. In 2011, this "freedom of contract" principle has been explicitly affirmed by the Commission's expert group on European Contract Law in its feasibility study. Besides the other affirmed principles of "contractual certainty" and "contractual fairness" it serves as a basis for the further harmonisation of contract law.[102] The European Data Protection Directive 95/46/EC explicitly open up the possibility of lawful data transfers on the basis of appropriate contractual clauses (Article 26 (2) European Data Protection Directive 95/46/EC).

According to Article 26 of the European Data Protection Directive 95/46/EC the European Commission is competent to find that specific Standard Contractual Clauses pose an adequate guarantee within the meaning of Article 26 Paragraph 2 in the context of the procedure described in Article 31 (2) 95/46/EC. The Standard Contractual Clauses developed by the Commission are not the only Contractual Clauses that can be recognized as adequate. In Principle, every company or trade association may draw up contracts and hand it in for the Commission's approval.[103]

5.3.2.1 Objectives

The first and foremost goal of providing these standard contractual clauses for usage is the warranty of adequate safeguards for the lawful transfer of personal data. Their contractual guarantees of data protection and provisioning of data subject's rights enable legal certainty and compliance with the European Commission's requirements regarding a sufficient level of protection for the data.[104] The European Commission has adopted several sets of Standard Contractual Clauses covering different roles of the data recipient. The recipient can either take the role of a data controller or a data processor. So an important pre-condition of using these clauses is the determination which role the involved parties obtain. This depends on the explicit and implicit competence as well as the factual control of the party. In a nutshell, the amount of decision power over the purpose and means of the data processing determines the classification either as controller or solely as processor.[105] Once the involved parties have been identified either as controller and processor, they need to use the fitting set of standard contractual clauses provided by the European Commission in the correct

[102] Commission Expert Group on European Contract Law, Feasibility study for a future instrument in European Contract Law, 3 May 2011.

[103] Cf. article 26 (4) EU Data Protection Directive 95/46/EC.

[104] See also Article 29 Working Party, WP 74, Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3rd June 2003, p.7.

[105] Article 29 Working Party, WP 169, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, p. 10 ff.; for an overview of and introduction to the criteria for role determination, see TClouds report R1.2.1.2 (Analysis of EU Law), p. 14 ff.

context. The Commission provides three different sets of clauses currently in force, whose applicability is determined to which parties the data is transferred. There are two different constellations of data transfers:

- Transfer of data from controller to another controller (C2C)
- Transfer of data from controller to a processor (C2P)

Two of the three sets provided by the European Commission cover the C2C constellation. These Commission decisions on these two sets are from the years 2001 and 2004:

- Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (2001/497/EC)

And the alternative set, amending the first:

- Commission Decision of 27 December 2004, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/915/EC)[106]

The two controller-controller sets are alternatively. Companies may choose their preferred contractual clauses.

The third set covers the C2P constellation, decided by the Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU). Before May 2010, a former version of clauses was implemented by Commission decision and in force since 2001.[107] This Commission decision however, was repealed and replaced by the 2010/87/EC Decision. So for the controller-processor data transfer there is no possibility to choose from the 2001 or the 2010 clauses. In cases of newly allocated agreements, the involved parties are bound to implement the 2010 version if using the European standard contractual clauses. An exception just may be valid for older contracts concluded before 15th May 2010, as long as the original agreements remain unamended to that date. Any substantial change of the agreement, for instance by involving new parties or changing the purpose of the transfer, leads to the downgrading of the old clauses as ad-hoc contract, that must be brought into line with the principles and safeguards entailed by the newer clauses of the decision 2010/87/EU. Also, such an ad-hoc contract must be examined and authorised by the concerned data protection authorities. Usually, in such cases it would be more appropriate and easier to directly install a new contract using the newer standard contractual clauses. 2010/87/EU.

5.3.2.2 Regulated content

This section will illustrate the substantive points of the standard contractual clauses sets and their most significant differences and effects compared to each other. One of the most prominent arrangements is the definition of a data exporter and the data importer. The data exporter is the controller entity that transfers the data while the data importer is the entity that receives the data from the controller. In contrast to the exporter, who is always the

[106] This set was approved by the Commission as a result of a request by an affiliation of business associations led by the International Chamber of Commerce (ICC)

[107] Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under the Directive 95/46/EC (2002/16/EC).

controller, the importer can be a controller as well as a processor entity. The specific definition of the data importer can be acquired out of the individual standard contractual clause that should be used, depending on the classification of the receiving party as controller or processor. As already introduced in the prior section, two of the three sets currently in force are related to transfers of personal data from a controller to another controller entity (C2C clauses). In contrast, the third set focuses on the data transfer from a controller to a processor and further sub-processing connections (C2P clauses). Thus, the analysis of the clauses will be broken down in two following sections, thematically divided into C2C clauses and C2P clauses.

5.3.2.3 C2C clauses 2001/497/EC and 2004/915/EC

The C2C clauses may be used within the SISSDEN project to cover personal data transfer from the SISSDEN consortium to e.g. ISPs or CERTs in third party countries. The recipient (data importer) in this case would be a data controller.

The foremost purpose of the EU standard contractual clauses is the creation of an adequate level of protection for the personal data, allowing the disclosure of said data from the controller to another party. This comes with the regulation of obligations for the individual contract parties and corresponding rights for concerned persons, namely the data subjects to enforce these. The breach of contractual obligations with regard to the personal data is explicitly subject to the liability of the data exporter and the data importer. Difficulties arise once several layers of vendors and customers are involved, igniting the need to conclude a multitude of contracts. This especially applies if data are transferred in a chain of several sub-processors, because each data exporter needs to conclude a contract with each data importer in a third country. The adjustment of contracts is even more complex in cases of changes regarding the data transfer itself. Also, once units of an internationally operating corporation are involved or the legal structures of the corporate form change, considerable administrative effort has to be made to align, adjust and newly conclude existing contracts. This also affects contractual structures such as master agreements with added appendices, e.g. related to economic aspects, such as Service Level Agreements, sales and distribution, marketing, or pricing.[108] In the standard contractual clauses provided by the Commission, the applicable law will also be regulated, which is especially of importance for companies with an establishment outside the EU, the EEA respectively. This also implies the determination of concerned data protection authorities and the enforcement of civil law claims against group companies in third countries.

The two sets of clauses 2001/497/EC and 2004/915/EC for the controller-controller data transfer however, show some essential differences. This affects partially some terminology but mostly obligations and liability regulations on both sides of the contract parties. So in the 2001 version (hereinafter: set I), clause 6 (2) provisions joint and individual liability of data importer and data exporter, regardless of causation and possibilities of indemnity and compensation agreements. This regulation was replaced by a liability rule following the causation principle under III. (a) of the 2004 version (hereinafter: set II). Also, punitive damages were explicitly excluded. Furthermore, in cases of dispute, the set I provided under 7 (2) an agreement of international commercial arbitration. This solution however, is quite intricate and expensive for the contract parties, thus in most cases not fitting for disputes in

[108] These may under certain circumstance be valid as long as they do not contradict the standard contractual clauses, see recital (5) of the Commission Decision 2001/497/EC or recital (4) of the Commission Decision 2010/87/EU.

the data protection field. Set II does not provide such an arbitration clause. Furthermore, clause 5 (c) of set I requires the contract partners to abide the advice of the concerned supervisory authorities while set II just provisions the accordance with binding decisions (clause II. (h) - (ii)). Beneficial for the contract parties is also the fact that set II opens up the possibility under clause VII. to supplement the contract with commercial clauses and to update the Annex B (under the condition that the concerned authority is informed).

Conclusion: Set II may appear much more desirable for companies intending to use the EU standard contractual clauses.

This also applies in the SISSDEN context, since the potential variety of involved parties and the increased flexibility in regard to data flows may require a more flexible coordination and content management of contractual agreements. Thus, set II seems more convenient for use within the project.

5.3.2.4 C2P clauses 2010/87/EU

The clauses for controller to processor transfer might become relevant for the SISSDEN consortium, if Shadowserver US would act as a processor on behalf of the SISSDEN consortium.

The new set of C2P clauses based on the Commission Decision 2010/87/EU cover the constellation of data transfers from a controller to a data processor in a third party country.

The most significant regulations are:

- Determination of the governing law, being the law of the data exporter's country
- Liability scheme, deploying the data exporter as primarily liable
- Introduction of a sub-processing clause
- Obligation regulations with explicit constraint demands for sub-processors
- Disclosure of contract copies to data subjects and exporters
- DPA powers for auditing and decision authority on agreements with sub-processors under contradicting law
- Deletion of arbitration clause

Clause 9 of the 2010 set of SCC explicitly determines the governing law with regard to data protection aspects as being the one of the member state the data exporter is established in. This rule also applies for sub-processing services through the whole chain of data processing operations. Corresponding to the applicability of the data exporter‘s national law, the new set of clauses introduces a liability scheme via clause 3 that determines the data exporter, namely the controller, as primarily liable towards the data subject‘s claims (clause 3 (1)). However, if the data exporter factually disappeared, ceased to exist in law or became insolvent, according to paragraphs (2) and (3), the data subject may follow the chain of contracts and issue his claim against the data importer, which is in this set of clauses and constellation the processor. The same procedure may take place if also the data importer is not assessable for the data subject‘s claims. In these cases the data subject may even issue his claim against the sub-processor. However, his liability is limited to his own processing operations under the clauses; thereby he may only be held responsible for issues that are within his own factual control. In conclusion, clause 3 (2) and (3) create kind of successor liability to ensure the protection of the data subject through the case-dependent utmost accessibility of a liable party.

The main novelty of the Commission Decision 2010/87/EU is the introduction of a regulation for sub-processing agreements, enabling a chain of processors and sub-processors. Currently, we do not foresee the need for involvement of sub-processors within the SISSDEN project.

Beyond the sub-processing regulations, the new set of clauses entails some more specific provisions. Just as in the set II of 2004 for C2C constellations, the arbitration clause has been deleted. Another fundamental regulation extracts from clause 5 (f), according to which the data importer is bound to make a copy of the sub-processing agreement available upon request of the data subject. This obligation however, is limited to the extent that he must disclose the contract copy but just a summary of security measures and may exclude commercial information. This procedure may suffice to suitably perform this information duty towards the data subject. Furthermore, clause 5 (j) provisions the sub-contracting must be communicated to the data exporter per default, regardless of a filed request. Clause 11 (4) regulates that the data exporter must keep a list of all sub-processing agreements to be able to eventually provide them to the data protection authority. This list shall be updated once a year. This kind of know-thy-sub-processor procedure entails the data importer sending a full contract copy so the data exporter may be able to fulfil his own obligation to keep track of the closed sub-contracts concerning his transferred data.

By the introduction of the new set of standard contractual clauses via Commission Decision 2010/87/EU, the data protection authorities have been empowered by clause 8 (2) with the authority to conduct audits of all data importers.

5.3.2.5 Validity and DPA oversight

The European Commission stated explicitly in their decisions that the standard contractual clauses may not be altered in any way, especially not by amending the individual sets or merging them.[109] However, it must be taken into account that besides the usage of the European standard contractual clauses the national law of the individual EU member states may require additional regulation. Since the EU SCC should not be changed to avoid risking their legal invalidity, such specifics consequently can only be settled in separate contracts, Service Level Agreements (SLA‘s) or in an annex to the SCC‘s, respectively. An example for such specific national requirements derives from Germany, whose law just permits the processing of personal data on behalf of others only under certain preconditions laid down in a ten point‘s catalogue in Article 11 BSDG (Bundesdatenschutzgesetz).[110] Generally, the allowance of data transfers is examined in a two-step evaluation by the local data protection authorities. First, the general legitimacy of a personal data transfer within the EU or EEA is examined by means of the national data protection law. Once data transfers into a third country outside the community are involved, they must be assessed in terms of permissibility according to section 4c BDSG, which requires the fulfilment of far more stringent provisions. Also, the 2004 set of the EU SCC is seen quite critical by German data protection authorities in regard to the German employee data protection law, because the

[109] Cf. recital (3) of the Commission Decision 2004/915/EC. Also, the amendment of 2001/497/EC by article 1 (1) of the 2004 decision commits the unchangeableness of the clauses. Furthermore, implemented by the Commission Decision 2010/87/EU for C2P constellations, the irrevocable nature of the clauses is stated in clause 10 of the contract text itself (Variation of the contract).

[110] Cf. EuroCloud Deutschland eco e. V. through its Guidelines Cloud Computing German Law, Data Protection & Compliance with advice on contractual regulation to achieve compliance with the German data protection law.

information obligation of the data exporter is limited. This may lead to gaps in the protection of said data if it is subject to company group-internal data transfers.[111] This issue is also seen critically by the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés, CNIL).[112] It must be noted that this second set is acknowledged by the European Commission as valid also for employee data. Still, it may be advisable to install extra protection mechanisms in favour of the company's (resp. controller's) employees.[113] Other EU member countries may have specific regulations in certain areas as well. So unlike in Germany, in the United Kingdom it is not necessary to undergo a two-step evaluation prior to the data export based on the EU SCC. Still, the UK Information Commissioner's Office (ICO) reserves the right to investigate the contractual agreement of a UK data controller in breach of contract cases.[114] In contrast, in France, the contract clauses regulating the transfer of personal data into third countries need to be reviewed and authorised by the French Data Protection Authority (CNIL). Some few and restrictively handled exceptions are made in cases of prior explicit consent of the data subject or indispensable necessity of the data transfer to safeguard the individual's life or the public interest.[115]

5.3.3 Binding Corporate Rules (BCR)

BCR are corporate codes of conduct that legally bind each entity of a conglomerate to company-specific, EU-compliant data handling systems. Under BCR, a multinational group develops its own in-house regulatory structure sheltering the data processing of its branches and units worldwide. Once approved, BCR empower the multinational group to transfer personal data of EU data subjects in-house, worldwide.

In WP 74, the Article 29 Data Protection Working Party states for the first time that BCR could be a suitable basis for cross-border data transfer.[116]

The term "binding corporate rules for international data transfer" was suggested by the Article 29 Data Protection Working Party (WP 29) as appropriate, because it reflects adequately the purpose of their existence.

- "Binding Rules" indicates that in order for these rules to be deemed as sufficient safeguards within the meaning of Article 26 (2) 95/46/EC, they must have internal and external binding effect
- "Corporate" refers to the context in which these rules can be applied; a multinational group drafts and implements these rules, usually under the responsibility of the headquarters.

[111] Cf. position paper of the working group "Internationaler Datenverkehr" ("International data transfer") of the German data protection authorities of 28 March 2007, p. 2 section II. 2.

[112] Laurence Dumure Lambert and Régine Goury in Meyer Brown L.L.P., New EU Standard Contractual Clauses for Commissioned Data Processing, publication of September 2010, p. 8.

[113] This is recommended by the ad-hoc working group "Konzerninterner Datenverkehr" (Intra-group data transfer) in its working report of 11 January 2005, which was constituted by initiative of the Duesseldorfer Kreis, an association of the German supreme supervisory authorities for data protection in the non-public sector.

[114] Mark A. Prinsley and Oliver Yaros in Meyer Brown L.L.P., New EU Standard Contractual Clauses for Commissioned Data Processing, publication of September 2010, p. 7.

[115] Ibid., footnote 13.

[116] Article 29 Working Party, WP 74 pp. 6-7.

- "International data transfer" reflects the reason for the application of this code of conduct; it provides a legal basis for cross border data transfers within a multinational group.

BCR are a tailor made solution for one multinational group. Therefore, the content of BCR differs depending on different conditions and needs of each conglomerate. Further implications on the variety of possible contents have the types of data processed as well as the legal requirements and characteristics of the countries where the data transfer takes place.[117] The Article 29 Data Protection Working Party has adopted a number of Working Papers adumbrating the substantial content of BCR[118] to facilitate the drafting of BCR for the applicants.

BCRs not only have to be internally enforceable by the corporate headquarters but the data subjects' rights have to be externally enforceable by data protection authorities and courts.[119]

Although, at first glance BCR may appear to be a canonical solution for data transfers between SISSDEN and US-based Shadowserver, for loose conglomerates like SISSDEN, BCR are unlikely to be a suitable tool for international data transfer. The diversity between the involved players and the broad scope of processing activities make it difficult to impossible to implement and enforce adequate BCR. For these conglomerates it would be necessary to differentiate subgroups within the same corporate group, set up severe limitations and conditions for the exchanges of information and particularise the rules.[120] Therefore, we deem SCC as the more suited tool within the SISSDEN consortium.

Conclusion: For sharing of personal data with data controllers outside of the EU we recommend the use of Standard Contractual Clauses. For the duration of the project the U.S./EU Privacy Shield may act as a sufficient legal basis for data transfer to the U.S. but its validity is already challenged before the ECJ.

[117] Mesaikou, Examining the Binding Corporate Rules as the most promising solution for the cross border data transfers of multinational companies under the EU Data Protection Directive, p. 16.

[118] Article 29 Working Party, WP 108, 2005; WP 133, 2007; WP 153, 2008; WP 154, 2008; WP 155, 2008.

[119] Article 29 Working Party, WP 108 p. 6.

[120] Article 29 Working Party, WP 74 p. 9.

6 Intellectual Property Rights Management

Intellectual property (IPR) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

IPR is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. These rights are outlined in Article 27 of the Universal Declaration of Human Rights, which sets out the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions.

An efficient and equitable intellectual property system can help all countries to realize intellectual property's potential as a catalyst for economic development and social and cultural well-being.

By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish (WIPO, 2016).

6.1 Introduction to IPR Management

The individual categories of IPR and how these are protected is illustrated in Table 6.1 below:

Category	**IPR Protection**
Innovative products & processes	Patent or Utility model
Distinctive signs	Trademark, collective mark, certification mark, in some case geographical
Creative designs including textile	Industrial design
Confidential business & technical information of commercial value	Trade secrets
Cultural, artistic & literary works including in most countries software & compilation of data	Copyright & related rights
Microchips	Protection of layout-designs or topographies of integrated circuits

Table 6.1: How IPR is protected

A strong judicial system has been developed to deal with both civil and criminal IPR offenses that enables right-owners to enforce their rights effectively. This is especially important in a world where expanding technologies have facilitated infringement of protected rights to an unprecedented level. Rights owners can, therefore, take action against infringers in order to prevent further infringement and recover the losses incurred from any actual infringement.

Avoiding litigation is an essential element of creative projects requiring due consideration of existing IPR as well as the application of the appropriate protection of new inventions. For

SISSDEN, this will require research of these areas which can be both complex and time-consuming for the novice to IPR. Reducing the risk of litigation and ensuring adequate protection of SISSDEN inventions is highly expedient.

6.1.1 Patents

A patent is an exclusive right granted by the State for an invention, which is a product or a process that provides a new way of doing something, or offers a new technical solution to a problem.

A patent provides its owner the exclusive right to prevent or stop others from making, using, offering for sale, selling or importing the patented invention without the owner's permission.

A patent is granted by either the national or regional patent office. It is, generally, valid for 20 years from the filing date of the patent application, provided the prescribed renewal (or maintenance) fee is paid on time. A patent is a territorial right and has no effect beyond the national boundaries of the country or region (group of countries) for which it was granted. In return for the exclusive rights, the inventor is required to disclose his invention to the public by describing in detail the invention in the patent application, which is published in an official journal or gazette.

6.1.2 Trademarks

A trademark is a distinctive sign that identifies certain goods or services produced or provided by an individual or a company. The system helps consumers to identify and purchase a product or service based on whether its specific characteristics and quality – as indicated by its unique trademark – meet their needs.

6.1.3 Industrial design

An industrial design refers to the ornamental or aesthetic aspects of an article. A design may consist of three-dimensional features, such as the shape or surface of an article, or two-dimensional features, such as patterns, lines or colour.

Industrial designs are applied to a wide variety of industrial products and handicrafts: from technical and medical instruments to watches, jewellery and other luxury items; from housewares and electrical appliances to vehicles and architectural structures; from textile designs to leisure goods.

To be protected under most national laws, an industrial design must be new or original and non-functional.

This means that an industrial design is primarily of an aesthetic nature, and any technical features of the article to which it is applied are not protected by the design registration. However, those features could be protected by a patent.

6.1.4 Trade secrets

In order to be protected as a trade secret, there are generally three requirements:

- The information must be confidential or secret
- The information must have commercial value because it is a secret, and
- The holder of the information must have taken reasonable steps to keep it confidential or secret

Trade secret protection lasts for as long as the information is kept confidential. Once the relevant information is made public, trade secret protection ends.

Broadly speaking, any confidential business information which provides a business with a competitive edge can qualify as a trade secret. For example, a trade secret may relate to technical matters, such as the composition or design of a product, a method of manufacture, the know-how necessary to perform a particular operation or business or commercial secrets of a very wide and potentially unlimited range of information.

6.1.5 Copyrights & related rights

Copyright laws grant authors, artists and other creators protection for their literary and artistic creations, generally referred to as "works". A closely associated field is "related rights" or rights related to copyright that encompass rights similar or identical to those of copyright, although sometimes more limited and of shorter duration. The beneficiaries of related rights are: performers (such as actors and musicians) in their performances; producers of phonograms (for example, compact discs) in their sound recordings; and broadcasting organizations in their radio and television programs.

Works covered by copyright include, but are not limited to: novels, poems, plays, reference works, newspapers, advertisements, computer programs, databases, films, musical compositions, choreography, paintings, drawings, photographs, sculpture, architecture, maps and technical drawings.

6.1.6 Protection of layout-designs or topographies of integrated circuits

Protection for the layout designs (topographies) of integrated circuits is not yet fully unified within IPR but broadly follows the Washington Treaty of 1989, incorporated by reference into the TRIPS Agreement of the World Trade Organization (WTO) signed in Marrakesh, Morocco on 15 April 1994 subject to the following modifications:[121]

> *"… the term of protection is at least 10 (rather than eight) years from the date of filing an application or of the first commercial exploitation in the world, but Members may provide a term of protection of 15 years from the creation of the layout-design; the exclusive right of the right-holder extends also to articles incorporating integrated circuits in which a protected layout-design is incorporated, in so far as it continues to contain an unlawfully reproduced layout-design; the circumstances in which layout-designs may be used without the consent of right-holders are more restricted; certain acts engaged in unknowingly will not constitute infringement."*

6.1.6.1 Definition of integrated circuit and layout-design

Article 2 of the IPIC Treaty gives the following definitions:

> *"(i) 'integrated circuit' means a product, in its final form or an intermediate form, in which the elements, at least one of which is an active element, and some or all of the inter-connections are integrally formed in and/or on a piece of material and which is intended to perform an electronic function,*

[121] https://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm

(ii) 'layout-design (topography)' means the three-dimensional disposition, however expressed, of the elements, at least one of which is an active element, and of some or all of the interconnections of an integrated circuit, or such a three-dimensional disposition prepared for an integrated circuit intended for manufacture ... "

Conclusion: There are legally defined protections for IPR that cover a wide-range of creations and innovations. These are not yet fully mature with some types of inventions remaining outside this scope. Software, for example, cannot yet be patented in the EU. This is of relevance to the SISSDEN project.

6.2 SISSDEN assets - a provisional IPR Audit

IPR audit is a systematic review of the IPR owned, used or acquired which is relevant for the assessment and management of risk, and which furthers the implementation of best practices in IPR asset management. In terms of business events such as IPO's, mergers, takeovers, etc., the scope is necessarily a thorough and detailed assessment of an entire organisation's assets. For SISSDEN the scope is an appropriately scaled down version that considers the architectural components relevant to the project. Project partners may contribute existing components (background) or be involved in the creation of new components (foreground). An IPR audit for SISSDEN will assess each partner component as either background or foreground in the context of the project's architectural requirements.

The following section is a guideline on how to carry out an IPR audit and why the process is necessary. The scope of an IPR audit for SISSDEN is specific to the project and partners should discuss the relevance of the guidelines and adapt these to project requirements.

6.2.1.1 Guidelines for a SISSDEN IPR audit

An IPR audit involves undertaking a comprehensive review of IPR assets, related agreements, relevant policies, and compliance procedures.

An IPR audit helps in the process of making, and updating, an inventory of its IPR assets, and to analyse:

- How the IPR assets are used or unused.
- Whether the IPR assets used are owned by individual partners or by others.
- Whether these IPR assets are infringing the rights of others or others are infringing on these rights
- Determine, in consideration of the above, what actions are required in respect of each IPR asset, its relevance to the business goals of the project.

The purpose is to identify ownership of project assets, to identify possible threats or conflicts of interest, and to provide guidance in the making of business and IPR strategies that may help maintain and improve the competitive position of SISSDEN in the relevant market(s).

In general, IPR audits can be classified into three main groups:

- General purpose IPR audit,
- Event-driven IP audit, and
- Limited purpose focused IP audit.

A general purpose IPR audit is mainly relevant to businesses or organisations undergoing strategic reorganisation which necessitates a comprehensive IPR audit. An event-driven IPR audit may be prompted by the need for "IPR due diligence" when a specific event such as a new joint venture, transactions involving IPR assets, launching a new product or service or licensing of an IPR asset. Thirdly, a limited purpose focussed IP audit tends to be situational and is typically used to justify a certain legal position or valuation of individual IPR assets.

There is no 'one size fits all' set of guidelines to IPR auditing: the scope is determined by the requirement. For SISSDEN the scope is narrowly limited to existing partner background or project work foreground.

Conclusion: An IPR audit is used to assess and manage the risk to intellectual property assets. The scope can be tailored to requirement which for SISSDEN encompasses existing partner background or project work foreground.

6.2.1.2 The IPR Audit

To carry out an effective IPR audit, a relevant level of knowledge about IPR issues is required. For a thorough assessment, this would involve a team of IPR experts, which may consist of internal or external expertise. For a relatively small sized project, such as SISSDEN, a basic awareness of the issues surrounding IPR should be sufficient. For SISSDEN, the involvement of external expertise would be a costly and, most likely, an unnecessary use of resources. However, as the project develops it might be necessary to revisit and to reassess SISSDEN IPR requirements – nevertheless even in the third year of the project the initial assessment stated above seems correct.

6.2.1.3 Developing a provisional register of partners' IPR assets

An essential item within an IPR audit is a register of IPR assets. For SISSDEN, it would suffice to compile a list of the background and foreground architectural components that partners are either using or will be involved in developing.

A vital element of the SISSDEN project is that existing background components, such as Access Rights to data feeds, have been granted by partners based on royalty-free non-commercial victim notifications and research for the duration of the project only. Additionally, initial honeypots will be mostly open source although, currently one exception to this scenario is that of "spampot". The rights surrounding the use of all components shall require assessment as appropriate.

For the SISSDEN IPR asset list, or register, proposed future developments should be included to serve as a reminder that IPR issues may be involved at a later stage of the project. As the current status stands software, the architectural component being developed during the lifetime of the SISSDEN project, cannot be patented in the EU.

A register of SISSDEN Initial Technical Architecture Logical Components is available in D3.4 Final technical architecture.

Conclusions and recommendations – It is advised that an IPR audit is adopted within SISSDEN processes. This is to incorporate a list of the background and foreground architectural components that partners are either using, or will be involved in developing.

The recommendation in D2.2 was for an initial IPR audit to be completed by M9. This is available in D3.3 Initial technical architecture, titled 'Initial Technical Architecture Logical Components'.

Due to the size and nature of the SISSDEN project it is not foreseen that the use of external expertise will be a requirement but this should be reassessed as the project progresses. This should be (and has been) carried out by M30.

A final audit of SISSDEN IPR should be completed by M30. This initial recommendation from D2.2 has been updated by later discussion, suggesting that the audit should be revisited post-project (in the reporting period) in order to verify whether any late developments affected the results. The results of the pre-final audit will be included in the confidential deliverable D2.9 "Final market strategy and sustainability plan" and any findings of the post-project review will be included in the final technical report.

6.3 Risks to SISSDEN assets

Inadequate asset protection is recognised as a major risk to IPR. An IPR audit provides an opportunity to assess the risk and to take preventative actions.

Another type of risk to intellectual property is unfair competition, which is also recognised as a major liability to intellectual assets and protection in law is available. This is provided for under Article 10bis of the Stockholm Act (1967, an amendment to the Paris Convention). It reads as:

> *"(1) The countries of the Union are bound to assure to nationals of such countries effective protection against unfair competition. Any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition.*
>
> *The following, in particular, shall be prohibited:*
>
> *-all acts of such a nature as to create confusion by any means whatever with the establishment, the goods, or the industrial or commercial activities, of a competitor;*
>
> *-false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial or commercial activities, of a competitor;*
>
> *-indications or allegations the use of which in the course of trade is liable to mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity, of the goods."*

This Article serves to supplement the protection of industrial property rights, such as patents and registered trademarks, in cases where an invention or a sign is not protected by such a right. Unfair competition covers many acts and requires adequate consideration during an IP audit and risk assessment.

Conclusion - For SISSDEN assessing the risk to IPR Assets is not considered a major task and can be facilitated through the Table of Initial Technical Architecture Logical Components, available in D3.3 and D3.4 (Initial / Final technical architecture), as outlined in 6.2.1 above.

6.4 Asset protection

6.4.1 Patent & IP searches relating to SISSDEN

The Patent protection scheme involves a number of processes and begins with; a) searching for existing patents and, b) patent filing.

a) Searching for existing patents: There are a number of ways to search for existing patents. WIPO provides free-of-charge database suitable for initial simple searches called Patentscope, https://patentscope.wipo.int/search/en/search.jsf. Here, it is possible to search through 58 million patent documents including 3 million published international patent applications (PCT).
   Fee-paying searchable database are also available and offer value-added patent information. A list of these is available through the Patent Information Users Group (PIUG) at www.piug.org/vendors.php.
b) Patent filing: This can be a complex process as patents are granted on a country specific basis and only for 20 years at a time. However, the Patent Cooperation Treaty (PCT) makes it possible to seek patent protection for an invention simultaneously in a large number of countries by filing a single “international” patent application instead of filing several separate national or regional patent applications.

6.4.2 Utility models

Utility models are similar to patents in providing protection for technical inventions and a limited exclusive right that prevents others from commercially exploiting the invention as a sort of “short-term patent”. This type of protection is suited to inventions making only small improvements or adaptations to an existing product, or for an invention that is intended for a short commercial life.

The time scale of protection is usually between 6 to 10 years. Utility model protection is only enforceable within the country in which it is granted.

Overall, a utility model is cheaper, registration is simpler and less stringent than that required of a full patent. It is useful when innovation is intended to be incremental and is especially useful in technology and mechanical innovation.

However, there is less legal security attached to utility models and third parties may question its value when considering a licensing agreement. It is especially useful when used to complement patent registration.

6.4.3 Trademarks

In principle, a trademark registration will confer an exclusive right to the use of the registered trademark. This implies that the trademark can be exclusively used by its owner, or licensed to another party for use in return for payment. Registration provides legal certainty and reinforces the position of the right holder, for example, in case of litigation.

6.4.4 Others

Trade secrets - Another form of asset protection is provided through trade secrets. Technical information such as designs and drawings of computer programs, commercial information such as list of suppliers and clients, advertising strategies, formulas and source code can all be protected as trade secrets.

The legal protection of trade secrets is covered under laws against unfair competition and practices such as industrial or commercial espionage, breach of contract and breach of confidence. Each case is considered independently. There is no “defensive” protection as trade secrets are not made public. Prior art may not automatically be claimed as technical information may be arrived at independently.

Defensive publication - Can be used as a form of stating prior art before filing a patent application by disclosing information in the public domain. However, this can limit the possibility of obtaining patent protection, thereafter.

6.4.5 Licensing of IP assets

Patenting an invention adds IP asset value and increases the possibility to license, sell or transfer to a third party. Legal ownership of a technology is demonstrated through appropriate intellectual property (IP) protection. Further, this alleviates suspicion between parties when discussing technology transfer. Once IP ownership is established it is possible to enter into a licensing agreement with an interested third party who will be able to use the patented product for a fee.

There are three main types of licensing agreements:

1) Technology License Agreement - the licensor authorizes the licensee to use the technology under certain agreed terms and conditions. It is, therefore, a contract freely entered into between two parties and contains terms and conditions so agreed. In a Joint Venture a license agreement may be concluded by the parties concerned regulating the use of the proprietary information.
2) Trademark Licensing and Franchising Agreement - a trademark or service mark is used to distinguish the goods and services of an enterprise with an implied reference to quality and reputation. To ensure the continued quality of reputation the trademark owner through law or by contract is advised to maintain a close connection with the licensee to ensure that the quality standards are maintained. With a franchise agreement, the franchiser may team up with another enterprise (franchisee) who may add additional expertise in providing goods or services directly to the consumer. The franchiser will ensure, through the supply of technical and management skills, that the franchisee maintains the quality and other standards in relation to the use of the trade or service mark.
3) Copyright License Agreement – this is mainly appropriate in creative or literary fields.

IPR ownership and licensing widens the possibility of business expansion through the manufacturing, selling, distribution and marketing of services and goods. However, a license agreement is restricted to countries where the IP is legally protected and it is important to ensure that full protection is available before entering into any license agreement.

Conclusions and recommendations - For SISSDEN the creation of IPR is mostly development of multiple discrete partner owned software components, plus generating a shared data set using a combination of these components. Since software is not currently patentable in EU, the opportunities for IPR asset protection may, at present, be limited. The situation will be monitored during the project lifetime and re-assessed accordingly.

6.5 Towards a business strategy

The value of IPR assets is established through a system of legal protections as outlined in previous sections. Without protections in place there is a risk that competitors may take advantage of the business opportunities that SISSDEN's new technologies will afford. For the architectural components used and created in SISSDEN, this is not considered to be a high risk although it is necessary to demonstrate that the issues have been fairly considered. As business opportunities are explored beyond the lifetime of the project the IPR situation will be revisited with a view to capitalising upon possible returns and profitability. The use of IPR protection, the possibility of licensing agreements, or other forms of agreements with third parties will be included within discussions on possible future business ventures.

In summary, the opportunities offered by IP protection are:

- IPR assets offer the opportunity to generate an income through the licensing, sale, or commercialization of the IPR-protected products or services.
- Investors and financing institutions will view IPR as added value.
- Protected IPR assets are more attractive in a potential sale, merger or acquisition.

IPR protection is a continuous process that begins with accounting for, and valuing, IPR assets. For SISSDEN this means clearly identifying all components being offered as background by individual partners and to track who owns and has access rights to them. This is provided for in the list of architectural components outlined above. As the project develops, components built as foreground necessitate review and assessment as to future business opportunities and what added value IPR can usefully, and cost-effectively, contribute.

The project's Consortium Agreement and Grant Agreement regulate the SISSDEN approach to IPR according to best practice as set out in the DESCA project (www.desca-2020.eu/). The CA is a legally approved agreement signed by all partners and, as such, forms the basis for all SISSDEN work. The rules for determining ownership of results of the project are therefore clear. However, the full range of expected results (foreground), and anticipated exploitation, is not expected to be known in detail until later in the SISSDEN project. For that reason, it is recommended that:

- an IPR review focused on exploitation of background and planned foreground as foreseen in the initial architecture is executed initially at M9,
- a final IPR review is only completed at M30, once the work on foreground results is nearing completion and the full range of developed IP assets is possible to assess.
- discussion at M30 also revealed a need to perform a minor review post-project (during the reporting period) in order to verify if any late developments in the project affected the results.

Further information is available at the Horizon2020 IPR Helpdesk https://www.iprhelpdesk.eu/.

Conclusions and recommendations: It is important to know and understand the value of SISSDEN assets to be able to maximise business opportunities beyond the lifetime of the project. The initial advisory register of assets can be found in D3.3 Initial technical architecture, titled 'Initial Technical Architecture Logical Components'. A similar updated table can be found in D3.4 Final technical architecture and will most likely be updated once more for D6.7 Architecture whitepaper.

6.6 Glossary & Acronyms

European IPR Helpdesk - The European IPR Helpdesk is a project funded by the European Commission under Grant Agreement No 641474, and managed by the Executive Agency for Small and Medium-sized Enterprises (EASME). It provides free-of-charge, first-line advice and information on Intellectual Property (IP).

European Patent Office (EPO) - The European Patent Office for Europe supports innovation, competitiveness and economic growth across Europe through its services delivered under the European Patent Convention.

Hague Agreement Concerning the International Registration of Industrial Designs - The Hague Agreement governs the international registration of industrial designs. First adopted in 1925, the Agreement effectively establishes an international system – The Hague System – that allows industrial designs to be protected in multiple countries or regions with minimal formalities.

IPIC Treaty or Washington Treaty (Intellectual Property in Respect of Integrated Circuits) - The Washington Treaty was adopted in 1989 and provides protection for the layout designs (topographies) of integrated circuits.

Locarno Agreement Establishing an International Classification for Industrial Designs – establishes a classification for industrial designs (the Locarno Classification). The competent offices of the Contracting States must indicate in official documents reflecting the deposit or registration of industrial designs the numbers of the classes and subclasses of the Classification to which the goods incorporating the designs belong. This must also be done in any publication the offices issue in respect of the deposit or registration of industrial designs.

Madrid Agreement Concerning the International Registration of Marks - the International Registration of Marks is governed by the Madrid Agreement, concluded in 1891, and the Protocol relating to that Agreement, concluded in 1989. The system makes it possible to protect a mark in multiple countries by obtaining an international registration that has effect in each of the designated Contracting Parties.

Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks - establishes a classification of goods and services for the purposes of registering trademarks and service marks (the Nice Classification). The trademark offices of Contracting States must indicate, in official documents and publications in connection with each registration, the numbers of the classes of the Classification to which the goods or services for which the mark is registered belong.

Paris Convention for the Protection of Industrial Property - Adopted in 1883, The Paris Convention applies to industrial property in the widest sense, including patents, trademarks, industrial designs, utility models, service marks, trade names, geographical indications, and the repression of unfair competition. This international agreement was the first major step taken to help creators ensure that their intellectual works were protected in other countries.

Patent Cooperation Treaty (PCT) - makes it possible to seek patent protection for an invention simultaneously in multiple countries by filing an "international" patent application. Such an application may be filed by anyone who is a national or resident of a PCT Contracting State. It may generally be filed with the national patent office of the Contracting

State of which the applicant is a national or resident or, at the applicant's option, with the International Bureau of WIPO in Geneva.

Patent Law Treaty (PLT) - adopted in 2000 with the aim of harmonizing and streamlining formal procedures with respect to national and regional patent applications and patents and making such procedures more user friendly. With the significant exception of filing date requirements, the PLT provides the maximum sets of requirements the office of a Contracting Party may apply.

Singapore Treaty on the Law of Trademarks - The objective of the Singapore Treaty is to create a modern and dynamic international framework for the harmonization of administrative trademark registration procedures. Building on the Trademark Law Treaty of 1994 (TLT), the Singapore Treaty has a wider scope of application and addresses more recent developments in the field of communication technologies.

Strasbourg Agreement Concerning the International Patent Classification – establishes the International Patent Classification (IPC) which divides technology into eight sections with approximately 70,000 subdivisions. Classification is indispensable in the retrieval process of patent documents during the search for "prior art", and used by patent-issuing authorities, potential inventors, research and development units and others concerned with the application or development of technology.

Trademark Law Treaty (TLT) - The aim of the Trademark Law Treaty (TLT) is to standardize and streamline national and regional trademark registration procedures. This is achieved through the simplification and harmonization of certain features of those procedures, thus making trademark applications and the administration of trademark registrations in multiple jurisdictions less complex and more predictable.

Vienna Agreement Establishing an International Classification of the Figurative Elements of Marks - establishes a classification (the Vienna Classification) for marks that consist of, or contain, figurative elements. The competent offices of Contracting States must indicate in official documents and publications relating to registrations and renewals of marks the numbers of the categories, divisions, and sections of the Classification to which the figurative elements of those marks belong.

WIPO (World Intellectual Property Organization) - An intergovernmental organization which in 1974 became one of the specialized agencies of the United Nations system.

WIPO Convention - The constituent instrument of WIPO, signed at Stockholm on July 14, 1967, came into force in 1970 and amended in 1979.

WIPO Copyright Treaty (WCT) - A special agreement under the Berne Convention which deals with the protection of works and the rights of their authors in the digital environment. In addition to the rights recognized by the Berne Convention, they are granted certain economic rights. The Treaty also deals with two subject matters to be protected by copyright: (i) computer programs, whatever the mode or form of their expression; and (ii) compilations of data or other material ("databases").

7 Conclusions and recommendations – summary

This section aggregates the conclusions and recommendations from this report, as a quick-reference extract. *Recommendations are marked with italics.* No additional content is provided.

7.1 Criminal law

7.1.1 German criminal law

- The main perpetrator of a DDoS attack commits a criminal offence according to the German Criminal Code, Section 303b.
- The operators of honeypots lack the necessary knowledge and intent to act as an accessory for data sabotage, unless intentionally neglecting security measures (Section 303b I Nr. 2, 27 of the German Criminal Code).
- Based on these considerations: Although the honeypot operator is not justified by research purposes, deploying and operating honeypots does not constitute sufficient intent for an accessory of computer sabotage (Section 303b I Nr. 2, 27 of the German Criminal Code).
- Deploying and operating honeypots may constitute the risk for a negligent offense, if individuals are hurt in the attack.
- *To minimize the risk of negligent offenses, it is important to rate limit outbound traffic of the honeypot to the minimum necessary for analysing the attack.*
- *To minimize the risk of negligent offenses, it is important to restrict network access of the malware in the sandbox and the outbound data rate to the minimum necessary for analysing the malware behaviour. In addition, reasonably expectable harmful actions that are typically performed by malware should be contained, such as sending email spam.*
- Port scans and network probes are not considered criminal offenses according to German criminal law.
- *If a port scan accidentally overloads the scanned system, the same argumentation as for DDoS attacks above is applicable. Thus, it is recommended to monitor port scans and exercise reasonable care to limit the (unlikely) risk of overloading systems with the port scan requests.*

7.1.2 Polish criminal law

- All the criminal provisions of Polish criminal law require intentional behavior of the offender therefore they are not applicable to the SISSDEN research. Parallel to the considerations for German and Dutch Criminal law, the central question is, whether SISSDEN deploying vulnerable systems or sharing network traffic data with third parties could negligently enable attackers to misuse these data and systems to carry out attacks. Without judicial precedent with regard to IT security research it is difficult to predict, whether a court would consider researchers publishing network traffic data or deploying honeypot systems as negligent behavior or to be causal for a following attack by a third party.
- Unlike German and Dutch criminal law however, Polish law provides a number of cases excluding the criminal liability when the offender acts for the purpose of

security of an information system, computer system or teleinformatic network or for the purpose of developing of the method of that security. Therefore, the risk of possible infringement of criminal law in Poland with SISSDEN systems is possibly lower.

7.1.3 Dutch criminal law

- The criminal provisions requiring intentional behaviour are not applicable to the SISSDEN research. Parallel to the considerations for German Criminal law, the central question is, whether SISSDEN deploying vulnerable systems or sharing network traffic data with third parties could negligently enable attackers to misuse these data and systems to carry out attacks. Without judicial precedent with regard to IT security research it is difficult to predict, whether a court would consider researchers publishing network traffic data or deploying honeypot systems as negligent behaviour or to be causal for a following attack by a third party.
- *Considering the risk, it is to be advised that SISSDEN systems have to be closely monitored and data must only be shared after a vetting process to rule out negligent behaviour. Considering the Dutch characteristic of prosecutorial discretion, the criminal offenses are phrased broadly. It is therefore crucial to document the IT security research purpose of SISSDEN's systems and data sharing platform as well as document the monitoring and technical and organisation security measures the SISSDEN researchers put in place to prevent misuse.*

7.2 Privacy and data protection law

7.2.1 Processing of personal data

7.2.1.1 Directive 95/46/EC

- Within the framework of SISSDEN personal data is present.
- The prerequisite "processing of personal data" is regularly fulfilled.
- SISSDEN is joint controller.
- *All project partners of SISSDEN already declared themselves responsible for compliance with data protection regulations. One project partner should act as a first point of contact for data protection requests and be mentioned in this function on the website.*
- The Directive 95/46/EC is applicable in a substantive and territorial way.
- SISSDEN may process the data obtained by honeypots. The personal data in the case of NTP and SSDP response payloads must be deleted after measuring the size of the response payload.
- For SISSDEN there is no obligation to inform the data subject about the processing. The data subject, however, has a right of access and a right to object with legitimate reasons.
- *SISSDEN has to provide a contact opportunity on the website of the project to allow the data subject to opt-out from data acquisition and processing.*
- SISSDEN must ensure that any data processing is confidential and secure.
- SISSDEN is jointly responsible in the sense of the data protection directive and is bound to the directive for data processing. As long as the data processing is performed on the examined scale, it is legally permissible.

7.2.1.2 GDPR

- In the case of SISSDEN there is no legal difference between the Directive and the GDPR with regard to the presence of personal data.
- In the case of SISSDEN there is also a processing of personal data after the GDPR.
- SISSDEN is joint controller.
- *The project partners should conclude a written agreement on the joint controllership.*
- *All project partners of SISSDEN should declare themselves responsible for compliance with data protection regulations. One project partner should act as a first point of contact for data protection requests and be mentioned in this function on the website.*
- The GDPR is applicable in a substantive and territorial way.
- The project partners must ensure that the above principles are respected and can demonstrate this if necessary.
- The data processing within SISSDEN is justified under Article 6 lit. f GDPR.
- *SISSDEN has to provide an information about the rights of the data subject on the website of the project.*
- *SISSDEN has to maintain a record of processing activities under its responsibility.*
- *The ICO (UK's data protection authority) has provided a documentation template for controllers which can be used by the project. However using these templates is not mandatory.*
- For the techniques considered in this document, there is no increased need for technical and organisational measures.
- *In the future, if the project is to be continued with commercial intent, IT security certification should be conducted in accordance with the ISO / IEC 27000 series or equivalent standards.*
- It is very unlikely that the supervisory authority or the data subject need to be notified in case of data breach.
- *If there should be a data breach, it should be checked briefly whether risks have arisen and whether someone has to be notified.*
- There is much to suggest that SISSDEN doesn't have to do DPIA.
- *Until a clear legal situation exists, SISSDEN should nevertheless carry out a DPIA for reasons of caution.*
- SISSDEN partners have to designate a data protection officer, if they meet the criteria of Art. 37 GDPR.
- *The lead organisation's data protection officer should oversee the Joint Controllership.*

7.2.2 Data sharing platform

- Since SISSDEN is a joint controller for data processing, personal data can also be passed on within the project.
- Since SISSDEN is also a joint controller under the legal framework of the GDPR personal data may be passed on within the project.
- SISSDEN may pass on the relevant IP addresses to the relevant ISPs and CERTs without the consent of the data subject.
- SISSDEN may pass on the relevant IP addresses to the relevant ISPs and CERTs without the consent of the data subject also under the legal framework of the GDPR.

- SISSDEN can share anonymized IP addresses with the public.
- *The last octet of the IP addresses should be stripped for anonymization. However, the consortium is may grant access to the non-anonymized reference data set for privileged research purposes, as described in the following (5.2.4).*
- SISSDEN can share anonymized IP addresses with the public also under the legal framework of the GDPR.
- There is no European law for data transfer between SISSDEN and law enforcement agencies. Therefore, national law must be applied.

7.2.3 Data transfer to third non-EU states

- During the project duration of SISSDEN, consortium partners can transfer personal data to U.S. data controllers based on the Privacy Shield, if the recipient was registered. To this end, Shadowserver U.S. already started the registration process for Privacy Shield. Alternative legal grounds for the transfer may provide a more long-lived solution.
- Set II[122] may appear much more desirable for companies intending to use the EU standard contractual clauses.
- For sharing of personal data with data controllers outside of the EU we recommend the use of Standard Contractual Clauses. For the duration of the project the U.S./EU Privacy Shield may act as a sufficient legal basis for data transfer to the U.S. but its validity is already challenged before the ECJ.

7.3 Intellectual Property Rights Management

- There are legally defined protections for IPR that cover a wide-range of creations and innovations. These are not yet fully mature with some types of inventions remaining outside this scope. Software, for example, cannot yet be patented in the EU. This is of relevance to the SISSDEN project.
- An IPR audit is used to assess and manage the risk to intellectual property assets. The scope can be tailored to requirement which for SISSDEN encompasses existing partner background or project work foreground.
- *It is advised that an IPR audit is adopted within SISSDEN processes. This is to incorporate a list of the background and foreground architectural components that partners are either using, or will be involved in developing.*
  The recommendation in D2.2 was for an initial IPR audit to be completed by M9. This is available in D3.3 Initial technical architecture, titled 'Initial Technical Architecture Logical Components'.
  Due to the size and nature of the SISSDEN project it is not foreseen that the use of external expertise will be a requirement but this should be reassessed as the project progresses. This should be (and has been) carried out by M30.
  A final audit of SISSDEN IPR should be completed by M30. This initial recommendation from D2.2 has been updated by later discussion, suggesting that the audit should be revisited post-project (in the reporting period) in order to verify whether any late developments affected the results. The results of the pre-final audit will be included in

[122] In the context of discussion of C2C clauses 2001/497/EC and 2004/915/EC. Set II refers to the latter.

the confidential deliverable D2.9 "Final market strategy and sustainability plan" and any findings of the post-project review will be included in the final technical report.

- For SISSDEN assessing the risk to IPR Assets is not considered a major task and can be facilitated through the Table of Initial Technical Architecture Logical Components, available in D3.3 and D3.4 (Initial / Final technical architecture), as outlined in 6.2.1 above.
- *For SISSDEN the creation of IPR is mostly development of multiple discrete partner owned software components, plus generating a shared data set using a combination of these components. Since software is not currently patentable in EU, the opportunities for IPR asset protection may, at present, be limited. The situation will be monitored during the project lifetime and re-assessed accordingly.*
- *It is important to know and understand the value of SISSDEN assets to be able to maximise business opportunities beyond the lifetime of the project. The initial advisory register of assets can be found in D3.3 Initial technical architecture, titled 'Initial Technical Architecture Logical Components'. A similar updated table can be found in D3.4 Final technical architecture and will most likely be updated once more for D6.7 Architecture whitepaper.*

8 Bibliography

[1] BeckOK StGB, 32. Edition, 01.09.2016

[2] BeckOK Datenschutzrecht, Wolff/Brink, 21. Edition

[3] Bert-Jaap Koops, 'Cybercrime Legislation in the Netherlands', Electronic Journal of Comparative Law, vol. 14.3 (December 2010)

[4] Translation of the German Criminal Code by Prof. Dr. Michael Bohlander https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

[5] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," Availability, Reliability and Security (ARES), 2013 Eighth International Conference on , vol., no., pp.546-555, IEEE, doi: 10.1109/ARES.2013.72, 2–6 September 2013. [http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf]

[6] A. Cormack, "INCIDENT RESPONSE: PROTECTING INDIVIDUAL RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION", scripted, Volume 13, Issue 3, December 2016, DOI: 10.2966/scrip.130316.258, https://script-ed.org/wp-content/uploads/2016/12/13-3-cormack.pdf

[7] Fischer, Kommentar StGB, 64. Aufl. 2017

[8] Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009

[9] Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. Aufl. 2012

[10] Lackner/Kühl, StGB, 28. Aufl. 2014

[11] Laue, Strafrecht und Internet – Teil 1, jurisPR-StrafR 13/2009

[12] Meyer Brown L.L.P., New EU Standard Contractual Clauses for Commissioned Data Processing, publication of September 2010, p. 8.

[13] Münchener Kommentar zum StGB, 2. Aufl. 2014

[14] Paal/Pauly, Datenschutz-Grundverordnung, 1. Auflage 2017

[15] Ratkic, Denial-of-Service-Attacken im österreichischen und deutschen Strafrecht, Graz, 2014

[16] Schönke/Schröder, StGB, 29. Aufl. 2014

[17] Schweda, Bundestag verabschiedet IT-Sicherheitsgesetz, ZD-Aktuell 2015

[18] Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015

[19] STOCK, B., PELLEGRINO, G., ROSSOW, C., JOHNS, M., AND BACKES, M. Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification. In USENIX Security Symposium (2016)

[20] WIPO Intellectual Property Handbook WIPO PUBLICATION No. 489 (E) ISBN 978-92-805-1291-5 WIPO 2004 Second Edition Reprinted 2008, http://www.wipo.int/portal/en/

[21] Würmeling, Einsatz von Programmsperren – Zivil- und strafrechtliche Aspekte, CR 1994