SPEAR

Secure and PrivaTE smArt gRid

(Grant Agreement No 787011)

D4.1 – Forensic Law and Regulations

2019-04-30

Version 1.0

Published by the SPEAR Consortium
Dissemination Level: Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme *under grant agreement No 787011*

Document Control Page

Document Details

Document Version	**0.9**
Document Owner	LUH
Contributors	PIMEE, TEC, VETS, SCHN, ED, PPC, CERTH
Work Package	WP 4 – Forensic Readiness and Privacy-Preserving
Deliverable Type	R
Task	Task 4.1 – Cyber Investigation Law and Regulations
Document Status	Final
Dissemination Level	Public

Document History

Version	Author(s)	Date	Summary of changes
0.1	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-01-15	ToC
0.2	Eider Iturbe Zamalloa, Erkuden Rios Velasco (TEC)	2019-02-15	ToC
0.3	Igor Kotsiuba (PIMEE)	2019-04-08	Chapter 1
0.3.1	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-04-09	Integration of chapters
0.4	Eider Iturbe Zamalloa, Erkuden Rios Velasco (TEC)	2019-04-09	Chapter 2
0.5	Christos Dalamagkas (PPC)	2019-04-11	Chapter 2
0.6	Eider Iturbe Zamalloa, Erkuden Rios Velasco (TEC)	2019-04-11	Chapter 2
0.7	Nikos Vakakis (CERTH)	2019-04-12	Chapter 2
0.8	Eider Iturbe Zamalloa, Erkuden Rios Velasco (TEC)	2019-04-15	Integration of Chapter 2
0.9	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-04-18	Integration of all chapters

0.10	Erkuden Rios Velasco (TEC)	2019-04-24	Review of all chapters
0.11	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-04-28	Incorporation of all review comments
1.0.1	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-04-29	Final version to the WP4, TM and PC
1.0	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-04-30	Final released

Internal Review History

Reviewed By	Date	Summary of Comments
Igor Kotsiuba (PIMEE)	2019-04-25	High quality, some grammar mistakes and terminology unification need to be done.
Pablo Gomez-calvente Moreno (ENEL)	2019-04-25	High quality, acceptable subject to some corrections

Legal Notice

The information in this document is subject to change without notice.

The Members of the SPEAR Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

The Members of the SPEAR Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Possible inaccuracies of information are under the responsibility of the project. This report reflects only the author's view and that the Agency and the Commission are not responsible for any use that may be made of the information it contains.

Table of Contents

Acronyms 6
List of Figures 8
List of Tables 9
Executive Summary 10
1. Introduction 11
1.1 Context 12
1.2 Methodology 13
1.3 Structure of the document 13
2. Forensics in SPEAR use cases 14
2.1 Use Case 1: Hydro power plant scenario 15
2.2 Use Case 2: The Substation scenario 17
2.3 Use Case 3: Combined IAN and HAN scenario 20
2.4 Use Case 4: Smart Home scenario 23
2.5 Honeypots in the use cases 27
3. Legal Framework of Electronic Evidence and Forensics Processes 29
3.1 Challenges associated with Network-based evidence 30
3.1.1 Technical Challenges 30
3.1.2 Legal Challenges 30
3.2 Laws, Guidelines and Standards applicable to digital evidence including network-based evidence 32
3.2.1 International Law 33
3.2.2 European Instruments 33
3.2.3 National Laws and Procedures relating to electronic evidence 38
3.2.4 Relevant Guidelines and Standards 40
4. Implications of the legal assessment on the SPEAR Forensic Framework 45
4.1 Positive Requirements 45
4.2 Negative Requirements 47
4.2.1 Lawful Processing Basis 49
4.2.2 Fair processing safeguards 50
4.2.3 Further relevant GDPR compliance requirements 51
5. Conclusions 53
References 54

Acronyms

Acronym	Explanation
AMI	Advanced Metering Infrastructure
CoE	Council of Europe
CERTH	Centre for Research and Technology Hellas CERTH
CD	Compact Disc
CJEU	Court of Justice of the European Union
CFREU	Charter of Fundamental Rights of the European Union
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
D	Deliverable
DDoS	Distributed DoS
DEFR	Digital Evidence First Responders
DES	Digital Evidence Specialist
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DNP3	Distributed Network Protocol
DPIA	Data Protection Impact Assessment
EAPTTLS	Extensible Authentication Protocol Tunneled Transport Layer Security
ENF	Electric Network Frequency
ENISA	European Union Agency for Network and Information Security
EIO	European Investigation Order
ECHR	European Convention on Human Rights
eIDAS	electronic IDentification, Authentication and trust Services
EU	European Union
GPS	Global Position System
GOOSE	Generic Object Oriented Substation Events
GDPR	General Data Protection Regulation
HAN	Home Area Network
HMI	Human Machine Interface
HVAC	Heating, ventilation, and air conditioning
HTTPS	Hypertext Transfer Protocol Secure
IAN	Industry Area Network
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
IDS IEC	Intrusion Detection System International Electrotechnical Commission
IED	Intelligent Electronic Device

IP	Internet Protocol
IPS ISO	Intrusion Prevention System International Standardisation Organisation
ISP	Internet Service Provider
KV	Kilovolt
LEAs	Law Enforcement Authorities
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MMS	Manufacturing Message Specification
MQTT	Message Queuing Telemetry Transport
NTP	Network Time Protocol
NIS	Network and Information Security
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OLAF	European Anti-Fraud Office
OPC	Open Platform Communications
OTS	One Time Signature
OSCAR	Obtain Information, Strategies, Collect Evidence, Analyse and Report
PCAP	Packet Capture
PLC	Programmable Logic Controller
PPC	Public Power Corporation
PII	Personal Identifying Information
RADIUS	Remote Authentication Dial-in User Service
RAM	Random Access Memory
RFC	the Request for Comment
RBAC	Role Based Access Control
REST	Representational State Transfer
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCHN	Schneider Electric France SAS
SPEAR	Secure and PrivatE smArt gRid
SPEAR-FRF	SPEAR Forensic Readiness Framework
SFTP	Secure File Transfer Protocol
SMB	Server Message Block
SSH	Secure Shell
SSL	Secure Sockets Layer
SWGDE	Scientific Working Group on Digital Evidence
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VETS	VETS Lenishta OOD
Wi-Fi	Wireless Fidelity

List of Figures

Figure 1: The Hydro power plant scenario architecture diagram 15

Figure 2: The Substation Scenario architecture diagram 17

Figure 3: The Combined IAN/HAN architecture diagram 21

Figure 4: The Smart Home Scenario architecture diagram 23

List of Tables

No se encuentran elementos de tabla de ilustraciones.

Executive Summary

This report focuses on studying and applying in the SPEAR project context the international and local regulatory framework regarding network forensics and digital evidentiary requirements in judicial processes. The aim is to identify all the appropriate regulatory requirements for the SPEAR Forensic Readiness Framework (SPEAR FRF) including those related to the collection, preservation, and use of digital evidence sources. With this aim, the report studies the cyber investigation law and regulatory frameworks in relation to the use of SPEAR FRF in each of the use cases of the project and extracts the implications and requirements for the applicability and exploitation of the SPEAR FRF.

In general, two broad types of requirement are identified and examined: first, those aspects that the SPEAR FRF SHOULD incorporate to ensure good use of the output for evidence in the future —positive requirements; and, in the second place, things the project should NOT do, so as to avoid privacy or other rights violations—negative requirements. The fulfilment of the positive requirements is geared to maximizing the usability of digital evidence gathered in the course of the operation of a smart grid—from forensic readiness process to the preservation of evidence. The aim is to configure the SPEAR system architecture so that when used in the future (i.e. exploitation phase), users by default are encouraged to follow current best practice in terms of collection and preservation of digital evidence. These requirements include the need to: obtain evidence lawfully; integrate strategies that go to show the chain of custody and data integrity right from the beginning of the process in an auditable, repeatable and reproducible manner; ensure that data acquisition, storage and analysis do not contaminate evidence; and integrate the human rights aspect right from the beginning.

The negative requirements span the period from the research phase to the (later) exploitation of the SPEAR FRF (in the hands of subsequent CSIRT and other users), and in particular the need for compliance with rules of EU data protection law, primarily contained in the GDPR. Key relevant data protection issues are analysed with reference to personal data envisaged to emerge from the use cases, with consideration of the lawful basis (as required by the GDPR) for the project's collection/storage of such data; other key requirements for the processing to qualify as fair, and adequately protective of the interests of the data subjects are also assessed, together with other regulatory compliance issues that arise under the GDPR. Adherence to privacy-preserving requirements in processing personal data in forensics processes will be critical, not only during the project development, but thereafter (as a default feature of the FRF design) to provide for data-protection compatible usage of the SPEAR end-product.

The output of this task will be utilised, especially, in Task 4.2 Smart Network Forensics and Task 4.4 Privacy-Preserving Framework.

.

1. Introduction

The transformation of the energy sector occasioned by innovation in information and communication technology is significant in terms of improved energy generation, distribution and transmission to the final consumer. However, it also harbours some cybersecurity risks, as the smart grid is susceptible to several vulnerabilities on each of these levels. It is therefore impossible to avoid cyber-incidents. The hackers who struck the power centres in Ukraine, for example, were skilled and stealthy strategists who carefully planned their assault over many months, first doing reconnaissance to study the networks and siphon operator credentials, then launching a synchronized assault in a well-choreographed manner [1]. Evidently, attacks against smart grids can arise from various parts of a power system: supervisory control and data acquisition (SCADA), electric transportation infrastructure, smart meters, advanced metering infrastructure (AMI), an energy storage subsystem and any vital components of the smart grid [1]. To cope with this challenge in distributed networks, the system needs to be monitored and information that will enable effective investigation of cybercrimes as well as predict system failures and manage Smart Grid, need to be logged.

One item of good news is that unlawful activities carried out with or through information technologies also leave footprints of perpetrators, which may be of use for evidential purposes, and where forensic science has helped in reconstructing incidents and generating evidence to prosecute crime [2]. Often, meticulous efforts are required to identify, collect and analyse this data. However, in some situations, the information systems appear not to have the capabilities to collect, preserve, and correlate reliable forensic data – i.e. attain digital forensic readiness [3] [4]. Forensic readiness is the "achievement of an appropriate level of capability by an organisation in order to be able to identify, collect, acquire, preserve, protect and analyse digital evidence" [5]. For its part, digital forensics "deals with the recognition, preservation, acquisition and analysis of digital information, with the objective of addressing forensic questions relevant to the legal inquiry being carried out" [6] [7]. It also deals with the study of the scientific processes, procedures, technologies and rules used to better protect the integrity of digital evidence [6]. The value of digital forensics lies in its legal purpose: that is why in most cases, much emphasis is placed on the legal acceptability or admissibility of the resultant evidence in court [3]. The forensics result can also be used for other internal purposes and audit.

Over the years, various branches of digital forensics have emerged, including computer forensics, mobile devices forensics, database forensics, network forensics [8]. The SPEAR project is concerned with the network forensics aspect and this will be the focus of this deliverable. Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection [9]. Cyberattacks that could be committed using a network are numerous, including Denial of Service (DoS) attacks, setting up bots, installing malware, etc [10].

There are two main approaches used to collect network data for forensic examinations: (1) collection by full brute force method—here all packets passing through a certain traffic point are captured and recorded in the storage with a subsequent analysis in batch mode. This approach requires large amounts of storage; (2) collection by intellectual method—here each packet is preliminarily analysed, but only specific information is stored for future analysis [1]. With appropriate monitoring tools, data could be obtained that can assist in identifying the source of an attack. If, for example, the Internet Protocol (IP) address or Media Access Control (MAC) address of the host is known at a specific time, other data from the Internet can be used to find out who uses a particular computer by extracting user account information from network traffic. It is notable, moreover, that obtaining network evidence presents both technical and legal challenges due to several factors such as the dynamic and volatile nature of the network system; indeed, advanced attackers may modify and disguise applications to conceal their presence using anti-forensics tools or encryption of data in transit. Here they may also be fortified by the knowledge that investigation of their activity is subject to certain legal constraints protecting fundamental rights, etc.

Several guidelines and best practices have been developed over the years to solve these challenges from both the scientific community and authorities on how to obtain and preserve network forensic evidence. These include guidelines from the Scientific Working Group on Digital Evidence (SWGDE) [11]; the National Institute of Standards and Technology (NIST) [12], the European Union Agency for Network and Information Security (ENISA) [9] [8]; the standard 27037 from the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC) [5], the Council of Europe (CoE) [10], etc. It is notable, though, that these documents have not resulted in a consensus on the methodology for conducting network forensics. However, a commonly used methodology for digital evidence processing is the "Obtain Information, Strategies, Collect Evidence, Analyse and Report" (OSCAR) method, which will for the time being (subject to the development of later bespoke methodologies) be deployed for the SPEAR Forensic Readiness Framework (SPEAR FRF). Similarly, multiple tools have been developed that support the collection of network data for forensics, such as packet capture, intrusion detection system and network flow sensors [9]. With the aid of these tools, a large amount of network data can be captured such as IDs, Proxy, traffic data, content data, logs, Wi-Fi network data, etc. In an industrial environment such as the smart grid, this data is important for forensic investigation, although currently, the forensic readiness of most critical infrastructure remains in its infancy [4].

The analysis of data circulating in smart energy grids infrastructures poses distinct challenges due to particular features of traffic monitoring in such infrastructures and analysis systems: a network forensics investigator and an attacker often have a similar skill level. For the investigation of the incident and for its accomplishment, both parties usually use the same tools and applications; for example, programs for obtaining information about network configurations. In a scenario where there are no firewalls, intrusion detection systems, or packet filters in an organization before the attack, it is difficult for a network researcher to get enough information to conduct an investigation. In some cases, there can be new challenges such as decentralized energy infrastructures, significant portions of personal data or digitalization of payments and energy distribution among parties.

1.1 Context

The SPEAR Forensic Readiness Framework (FRF) is being developed with the intention of providing technical solutions and assistance in the field of forensic readiness of smart grids. It aims to bring valuable solutions to gathering network-based evidence for cybersecurity and will develop proactive forensic tools in line with three main methodologies, namely planning, implementation and assessment. The framework will, firstly, provide insights as to how smart grids can be made forensics ready, and secondly, suggest best ways of collecting and securing network traffic data that may be useful for evidential purposes. The use of honeypots as a specific proactive forensic tool will also be explored.

This report, and indeed, the SPEAR FRF does not cover how law enforcement authorities should handle forensic evidence or how to present digital evidence in court proceedings, as these issues are matters that no longer arise within the SPEAR context, but for the relevant law enforcement authorities (LEAs) after they have received evidence from the SPEAR FRF. Rather, this report will address the questions of:

1. What conditions need to be fulfilled to ensure that the forensic evidence obtained in a system using SPEAR may be used by LEAs (should they wish to do so) as reliable and admissible prosecution evidence in judicial processes (methodological/procedural aspects)?
2. What legal compliance needs to be observed by the SPEAR FRF so as not to breach fundamental rights of individual actors (particularly, their privacy and data protection rights) due to the data collection / processing in the course of achieving forensic readiness?

To address these questions, this report will examine laws and regulation applicable in the area of network forensics and how these could impact on the SPEAR FRF, using the use cases as examples, and will provide guidance on how to design the SPEAR FRF to be relevant for future evidence-gathering while respecting the privacy of the associated actors. In the end, the output of this report will assist other tasks of the project in designing and achieving a SPEAR FRF objectives by adopting established principles and methodology to develop a sustainable framework.

1.2 Methodology

The objective of Task 4.1 Cyber Investigation Law and Regulations in SPEAR is to examine laws and regulations applicable in the area of network forensics, which will ultimately inform the design of the SPEAR FRF to be relevant for its purpose. For completing the tasks described in this report, desktop research and consultations with end-user partners of the project have been relied upon. The desktop research relating to forensic laws and regulations was carried out using the doctrinal research method. The doctrinal method is a method of "*research which provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments"* [13]. It incorporates a two-stage process, first locating the sources of the law applicable to a particular issue, and second, interpreting and analysing the text of the law [13]. In the first step on this Deliverable, laws relating to rules of evidence, cybercrime and human rights were identified from both international and national perspectives. In the second step, only the provisions of the laws that relate to digital evidence that are relevant to the SPEAR FRF were interpreted and analysed with the assistance of secondary sources (e.g., guidelines, opinions and policy documents, etc.) on the subject.

Input was also received from Deliverable *D2.1 User, Security and Privacy Requirements*, to obtain the relevant data for analysing the forensic readiness of the end-user systems, as well as the nature of data that could be obtained from their system for forensic purposes and how the data relate to personal data. A series of teleconferences and email exchanges were undertaken with the end-user partners to validate the data and complete some tables.

1.3 Structure of the document

This deliverable is divided into five main sections, each with several subsections. After the executive summary, the parts are as follows:

- Chapter 1 introduces the subject matter and provides an overview of the context, and methodology used in completing this report.
- Chapter 2 analyses the forensic evidence processing aspects of the SPEAR use cases.
- Chapter 3 discusses the legal framework of digital evidence and forensic processes relevant to SPEAR FRF.
- Chapter 4 focuses on the implications of the legal environment on the development of the SPEAR FRF and suggests how to design the tool to be legally compatible for its purpose.
- Chapter 5 concludes the deliverable.

2. Forensics in SPEAR use cases

For the purposes of developing the SPEAR FRF, four use cases have been established at four end-user partners, as follows: Use Case 1 (Hydro-Plant Scenario, partner VETS); Use Case 2 (Substation Scenario, partner ENEL); Use Case 3 (Combined HAN and IAN Scenario, partner PPC; and Use Case 4 (Smart Home Scenario, partner CERTH).

In each case, the project will monitor and collect data flowing within the respective use case networks, both in relation to their ordinary functioning, i.e. the default position when they are not under external pressures from a cyber-attack or another anomalous factor (e.g. extreme weather conditions) and when they are subject to such pressures. A comparison of the network flow data for these distinct situations will be crucial for training the SPEAR system to recognize which data patterns are indicative of (different forms of) cyberattacks. In addition, there are two further potential outcomes from processing network traffic data gathered during a cyber-attack: analysis of the data may yield a better understanding of the strategies employed by the attacker in mounting the particular attack; and (thirdly) the data may constitute evidence that may subsequently be handed over to a law enforcement authority (LEA) for the purpose of investigating and/or prosecuting the perpetrator of the attack.

During the SPEAR development phase (i.e. the lifetime of the project) the data gathered will be used only for the first two above purposes, namely for enhancing SPEAR's ability to recognize when (and in what form) a cyber-attack on one of the networks is in progress; and improving the understanding of attacker strategies. However, during the project exploitation phase, the expectation is users of the SPEAR system may frequently choose (or be legally required [14]) to share the cyber-attack data gathered by the system with their relevant LEAs for the latter to use as potential evidence against the attacker. For this reason, the project needs to incorporate into its system architecture methods of handling the data in accordance with key digital forensic evidence requirements (aimed to ensure that such evidence will qualify as admissible and reliable evidence in subsequent judicial proceedings).

For potential forensic data, Deliverable *D4.2 Smart Network Forensics Specifications* will work with the following information:

1. What network devices (hubs, switches, routers, Dynamic Host Configuration Protocol (DHCP) servers, Domain Name System (DNS) servers. Authentication servers, Network-based Intrusion Detection System (NIDS)/ Network-based Intrusion Prevention System (NIPS), Firewalls, Proxies, Application Servers, Central Log Servers) can be used to extract information? It can also be specified according to the type of network-based evidence:
    a. full content data (exact copies of all the traffic, i.e. PCAP format),
    b. session data (aggregated traffic metadata),
    c. alert data (typically generated from NIDS), and
    d. statistical data (generated for example from Wireshark)
2. What logs (network and host) can be used and where they can be found by a forensic expert? The most prevalent (but not exhaustive) sources for host and network-based forensics are: network-based sources and host-based sources. Since in successful attacks the attackers might manipulate the compromised host in order to stop logging any useful information or even log false information, it becomes apparent that network data might be the only evidence available. Network-based sources include:
    a. full packet captures (in form of the tcpdump or Wireshark tools),
    b. network flows (NetFlow),
    c. NIDS/NIPS
    d. application specific network data.
3. How this evidence acquisition occurs (can be either by "passive" or "active" means)

During the strategic planning of steps in the forensic process, it can be prioritised what data to collect based on various parameters, such as likely forensic value, effort for obtaining data, volatility of data. More information regarding the forensic process will be included in Deliverable D4.2.

The remainder of this section describes the data that can be recovered from the SPEAR use cases that can potentially become digital evidence to be used in court. The potentiality for such data to be utilised as digital evidence is determined through the forensic process, which will be defined in Deliverable *D4.2 Smart Network Forensics Specifications* within SPEAR.

2.1 Use Case 1: Hydro power plant scenario

Figure 1 below represents the hydro power plant scenario:

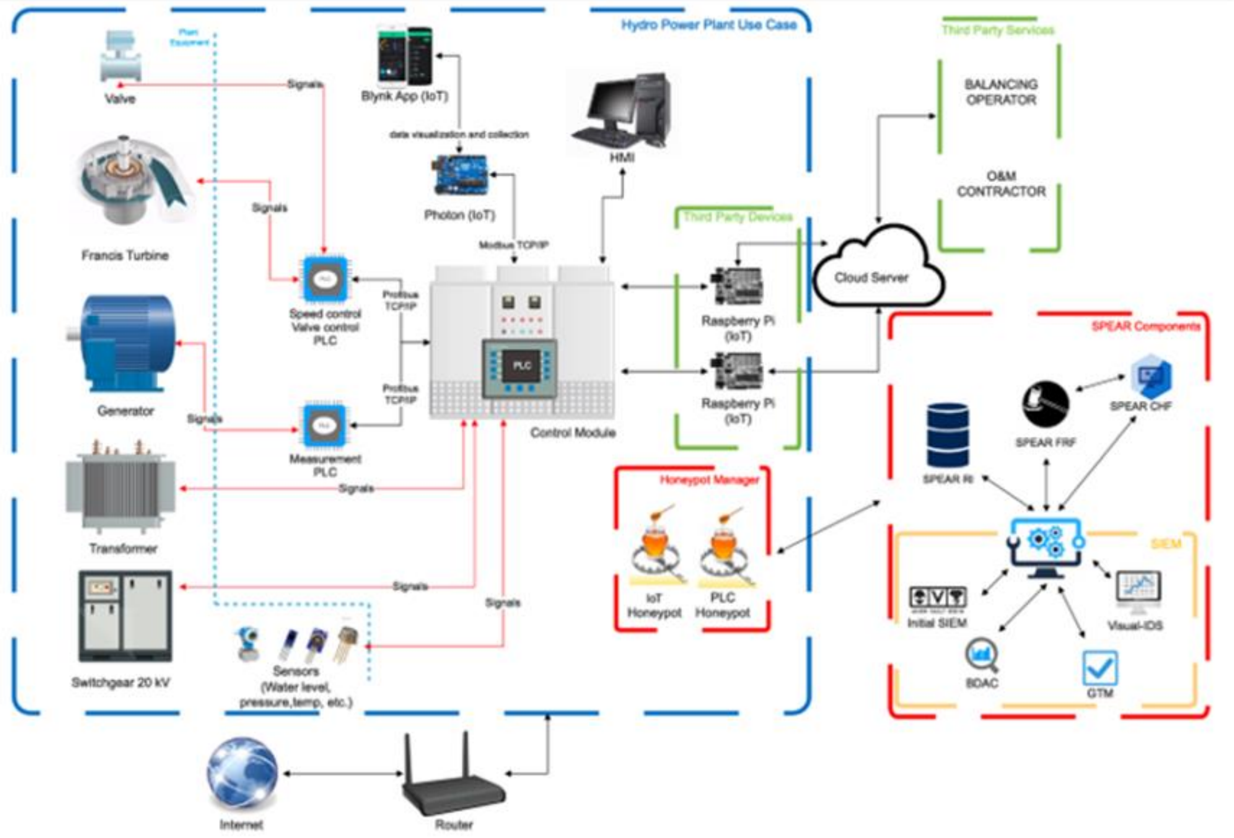


Figure 1: The Hydro power plant scenario architecture diagram

The potential data that can be collected from the hydro power plant scenario, including that which may comprise personal data (PII), is described in Table 11. Please see Section 4.2 for more details on constraints for associated PII processing in forensics.

Table 1: Data handled by Use case 1

Category	Description	Data protection mechanisms deployed	Associated PII
Network data	**Modbus** Transmission Control Protocol **(TCP)/IP** [15] communication protocol used by hydro plant devices to send operational data.	No encryption mechanism nor authentication defined in the standard.	Only operational data, No PII.
Network data	**Profinet** [16] communication protocol used by hydro plant devices to send operational data.	No encryption mechanism nor authentication defined in the standard.	Only operational data, No PII.
Third party data	The operator will use an IoT app called Blynk app [17] for data visualisation in her mobile. Blynk app works through a centralized server that provides the communication between the operator's mobile and the Smart grid's device.	Transport Layer Security (TLS) connection between the mobile and the Blynk app server. TLS is possible between the Smart grid's device and the server.	IP address of the operator's mobile is PII. And it is being handled by a third party.
Operational data	The operational data are measurements regarding the operational readiness of the hydro power plant (More details below). The operational data is captured by sensors distributed in the plant and sent to the control module PLC through the network using the protocols identified above. It is stored in the Human Machine Interface (HMI) in txt files in CSV format.	In transmission: No, since depends on the communication protocols used above. In storage: No encryption. No access control mechanisms.	Only operational data, No PII.

The operational data which is transmitted and stored in this use case is listed below:

- Level of the water in the basin
- Pressure in the pressure pipe before the turbine
- Position of the closing valve on the pressure pipe.
- Pressure and temperature of the oil in the "Guide vane" hydrostatic lock system
- Position of the Guide vanes
- Rotation speed of the turbine
- Temperature of the bearings of the generator
- Temperatures of the coils of the generator

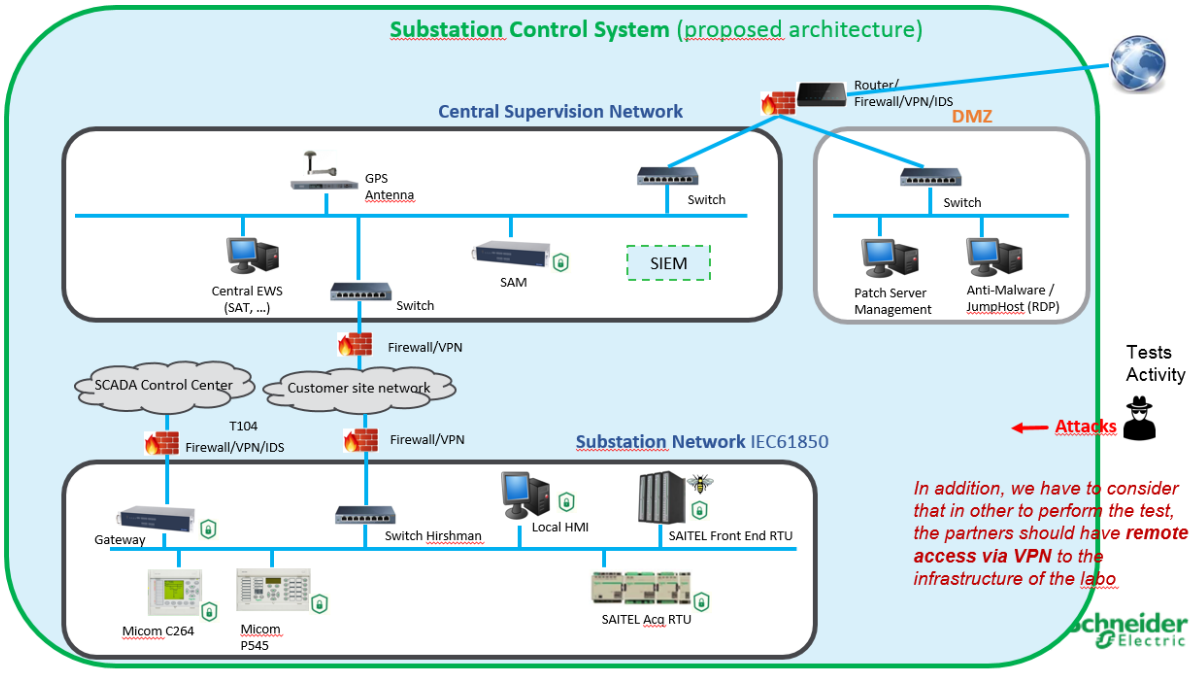
The operational data which is only transmitted in this use case is listed below:

- Voltage and Current of the generators.

- Position of the switch gear at 20kv (connection line) (open or closed-circuit barker).
- Position of the switch gear at 1kv (generator) (open or closed-circuit barker).
- Electricity available for own needs, etc.
- Conditions of the key sensors.

2.2 Use Case 2: The Substation scenario

Figure 2 below represents the substation scenario:



In addition, we have to consider that in other to perform the test, the partners should have ***remote access via VPN*** *to the infrastructure of the labo*

Figure 2: The Substation Scenario architecture diagram

The potential data that can be collected from the substation scenario, including that which may comprise personal data (PII), is described in Table 22. Please see Section 4.2 for more details on constraints for associated PII processing in forensics.

Table 2: Data handled by Use case 2

Category	Description	Data protection mechanisms deployed	Associated PII
Network data	**Modbus TCP/IP** [15] communication protocol used by substation devices to send operational data.	No encryption mechanism nor authentication defined in the standard.	Only operational data, No PII.

Network data	**IEC61850** Generic Object Oriented Substation Events **(GOOSE)** [18] communication protocol used by substation devices to send operational data.	No MAC used (IEC 62351 [19] establishes the countermeasures to guarantee the security of communications.)	Only operational data, No PII
Network data	**IEC61850** Manufacturing Message Specification **(MMS)** communication protocol used by substation devices to send operational data.	No TLS implemented (IEC 62351 [19] establishes the countermeasures to guarantee the security of communications)	Only operational data, No PII
Network data	**T104 (compliant with of IEC 60870-5-104)** [20] communication protocol used by substation devices to send operational data.	No TLS implemented 62351-5: Secure Authentication (IEC 62351 [19] establishes the countermeasures to guarantee the security of communications.)	Only operational data, No PII
Network data	Distributed Network Protocol **(DNP3)** communication protocol communication protocol used by substation devices to send operational data.	No TLS implemented 62351-5: Secure Authentication (IEC 62351 [19] establishes the countermeasures to guarantee the security of communications.)	Only operational data, No PII
Network data	Network Time Protocol (**NTP**) [21] to synchronize the clocks of computers over a network.	No authentication [22]	Time related data, No PII.
Network data	Hypertext Transfer Protocol Secure **(HTTPS)** to access services provided by the RTU, such as web interface to access the stored operational data.	TLS at TCP level.	The database with the operational data in the RTU can contain the location of the nodes where the energy will be distributed. But this information is not transmitted through the operational network. It can only be recovered through HTTPS using a web interface in the RTU.

Network data	Secure Shell (**SSH**)	SSH provides strong encryption, server authentication, and integrity protection (RFC 4253 [23]).	Authentication credentials such as user and password are sent at user authentication layer. Credentials of the system. The IP of the connected device is not stored.
Network data	Syslog Protocol over UDP [24]	No TLS implemented	User alias is sent.
Network data	Remote Authentication Dial-In User Service (**RADIUS**) for centralized Authentication, Authorization, and Accounting management for users who connect and use a network service [25].	Radius can be used over TLS (RFC 6614 [26]). In the substation implementation, there can be two modes, no encryption at all or TLS (more precisely Extensible Authentication Protocol Tunneled Transport Layer Security (EAPTTLS) mode)	Authentication credentials such as user and password are sent.
Network data	Samba implementing Server Message Block (SMB) protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers [27].	It uses Lightweight Directory Access Protocol (LDAP) for authentication or kerberos, so there are security mechanisms.	Authentication credentials such as user and password are sent.
Logging data	Sequence of events logging in the RTU	In transmission: It is not transmitted. In storage: It is not encrypted. The access is controlled by Role Based Access Control (RBAC) in the file system, Secure File Transfer Protocol (SFTP) and webserver.	Only operational data. No PII.
Operational data	The operational data are measurements regarding the operational readiness of the substation (More details below).	In transmission: Depends on the	The database with the operational data in the RTU can contain the location of the nodes

	The operational data is captured by distributed devices in the substation and sent through the network using the protocols identified above.	communication protocols used above. In storage: No encryption. Only access though HTTPS.	where the energy will be distributed. But this information is not transmitted through the operational network. It can only be recovered through HTTPS using a web interface in the RTU.

The operational data which is transmitted and stored in this use case is listed below:

- Active Power
- Reactive Power
- Apparent Power
- Current
- Frequency
- Voltage
- Temperature
- Trafos Position

2.3 Use Case 3: Combined IAN and HAN scenario

Figure 3 below represents the combined IAN and HAN scenario:

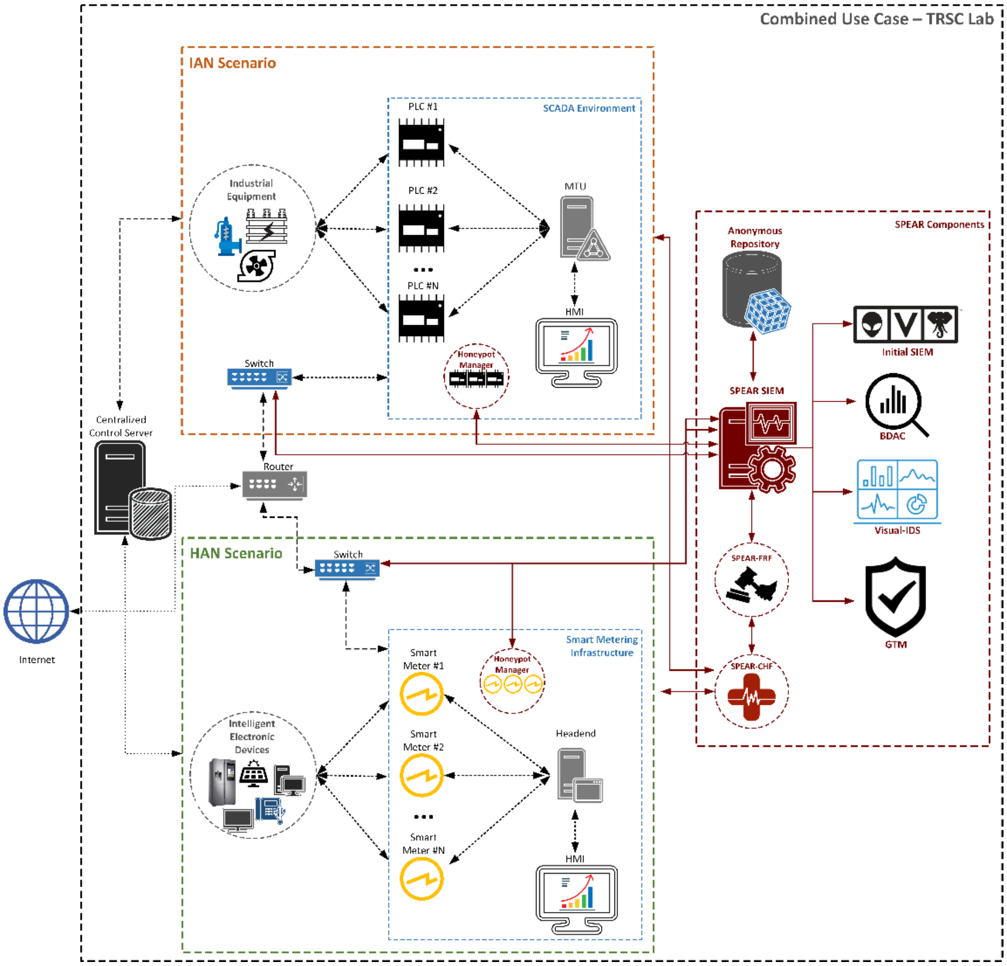


Figure 3: The Combined IAN/HAN architecture diagram

The potential data that can be collected from the combined IAN and HAN scenario, including that which may comprise personal data (PII), is described in Table 33. Please see Section 4.2 for more details on constraints for associated PII processing in forensics.

Table 3: Data handled by Use case 3

Category	Description	Data protection mechanisms deployed	Associated PII
Network data	**Modbus TCP/IP** communication protocol used by IAN and HAN devices to send operational data.	No encryption mechanism nor authentication defined in the standard.	Potential PII: IP addresses of the source and destination may be considered PII provided any application/service maps these IPs with users.

Network data	**SSH**	SSH provides strong encryption, server authentication, and integrity protection (RFC 4253 [15]).	Authentication credentials such as user and password are sent at user authentication layer. Credentials of the system.
Network data	**HTTPS** is used to access management interfaces of various physical devices or virtual machines (e.g. the management interface of the router). (HAN scenario)	TLS on top of the transport layer.	Potential PII: IP addresses of the source and destination may be considered PII provided any application/service maps these IPs with users.
Network data	**NTP** is used by VMs and devices for time synchronization.	No encryption mechanism nor authentication defined in the standard.	Potential PII: IP addresses of the source and destination may be considered PII provided any application/service maps these IPs with users.
Network data	**PCOM/TCP** [28] a proprietary protocol by Unitronics for remote management of the PLC (TCP port 20256)	No encryption mechanism nor authentication is provided.	Potential PII: IP addresses of the source and destination may be considered PII provided any application/service maps these IPs with users.
Operational data	The operational data are measurements regarding the operational readiness of the use case (More details below). The operational data is captured by the PLC and smart meters and sent through the network using the protocols identified above.	The operational data is transmitted over the abovementioned communication protocol (Modbus TCP/IP). In storage: Operational data is stored temporarily in the PLC and the AMI headend. No encryption is applied.	Measurements from smart meters are considered as PII since they may indicate energy pattern corresponding to user demand.

The operational data which is transmitted and stored in this use case is listed below:

Analogue data regarding the following:

- Battery voltage
- Generator speed

- Generator motor voltage and current
- Exciter motor voltage and current
- Generator motor temperatures
- Energy consumption

Digital data (boolean values) regarding the following:

- L1, L2 and L3 phases of power grid 20 KV
- If the generator and the exciter have acquired rated rounds per minute
- If the generator has overcurrent or overvoltage

2.4 Use Case 4: Smart Home scenario

Figure 4 below represents the smart home scenario:

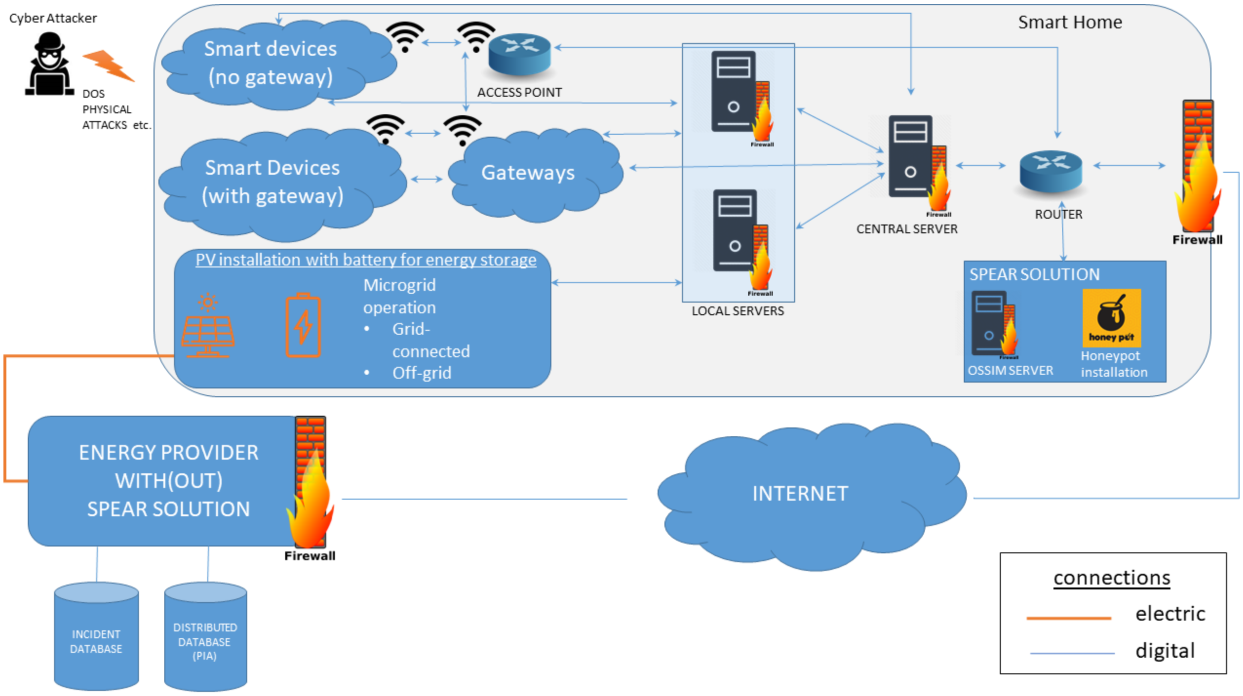


Figure 4: The Smart Home Scenario architecture diagram

The potential data that can be collected from the smart home scenario, including that which may comprise personal data (PII), is described in Table 44. Please see Section 4.2 for more details on constraints for associated PII processing in forensics.

Table 4: Data handled by Use case 4

Category	Description	Data protection mechanisms deployed	Associated PII

Network data	**Modbus TCP/IP** communication protocol used by inverters/ chargers to send operational data.	No encryption mechanism nor authentication defined in the standard.	Potential PII: IP addresses of the source and destination may be considered PII provided any application/service maps these IPs with users.
Network data	OPC **BACnet** communication used by HVAC system of Smart Home to send / receive operational data [29].	No security mechanism implemented	The HVAC measurements could potentially lead to the formation of the personal profile of the occupants.
Network data	**HTTPS (REST)** protocol used ● by power smart meters to send electricity measurements to the central Smart-Home server ● for monitoring of the inverters/chargers ● for the communication of the local server of the smart appliances with the central Smart-Home server ● by people counters to send measurements to the central Smart-Home server	HTTP over TLS/SSL	Smart meter electricity measurements and people counters could potentially lead to the formation of the personal profile of the occupants.
Network data	Message Queuing Telemetry Transport **(MQTT)** messaging protocol for communication of several sensor gateways and local servers with the Smart-Home central server	No TLS/ Secure Sockets Layer (SSL) currently implemented	Some sensor measurements such as motion detectors could lead to the formation of the personal profile of the occupants.
Operational data	The operational data are electrical measurements of the Smart-Home building, battery measurements, PV measurements and sensor data sent from the sensor gateways to the central Smart-Home server.	In transmission: Depends on the communication protocols used above. In storage: The operational data stored only in the .pcap files in	The formation of the personal profile of the occupants from the operational data should be investigated.

		the form of a payload. If there is encryption, the payload is not readable. If there is no encryption the payload could be read.	

<u>The operational data which is transmitted and stored</u> in this use case is listed below:

- Over the BACnet protocol, the Heating Ventilation and Air Conditioning (HVAC) units send data regarding room temperature, temperature set point, fan speed, operation mode, operation status and the location of the swing.
- Smart Meters as wired energy analysers (3 Phase Circuits, 1 Phase Circuits) over the Modbus protocol measure the values shown in Table . The measurements of the 1-Phase Circuits are the same variables as the measurements of Phase 1 (L1) in a measurement set of a 3-Phase Circuit.

Table 5: Operational data from Smart Meter in CERTH's Smart Home use case scenario

Measurement	Description
Cost	Cost (€)
KWh_S	Active Energy Total (kWh)
Kvarh_Tot	Reactive Energy Total (kVArh)
W_L1	Active Power Line 1 (W)
W_L2	Active Power Line 2 (W)
W_L3	Active Power Line 3 (W)
W_S	Active Power Total (W)
VAR_L1	Reactive Power Line 1 (VAr)
VAR_L2	Reactive Power Line 2 (VAr)
VAR_L3	Reactive Power Line 3 (VAr)
VAR_S	Reactive Power Total (VAr)
PF_L1	Power Factor Line 1
PF_L2	Power Factor Line 2
PF_L3	Power Factor Line 3
PF_S	Power Factor Total
A_L1	Amperage Line 1 (A)
A_L2	Amperage Line 2 (A)
A_L3	Amperage Line 3 (A)
V_L1_N	Voltage Line 1 (V)
V_L2_N	Voltage Line 2 (V)

V_L3_N	Voltage Line 3 (V)
V_L1_L2	Voltage Line 1 to Line 2 (V)
V_L2_L3	Voltage Line 2 to Line 3 (V)
V_L3_L1	Voltage Line 3 to Line 1 (V)
VA_L1	Apparent Power Line 1 (VA)
VA_L2	Apparent Power Line 2(VA)
VA_L3	Apparent Power Line 3(VA)
VA_S	Apparent Power Total (VA)
Hz	Frequency (Hz)
Energy_preds	Load Prediction (LR)
LdPred2	Load Prediction (LR & ANN)
Energy	Active Energy Current (kWh)

- In the Smart Home, there are a lot of smart sensors measuring and sending operational data. All the sensors are listed below in Table 66.

Table 6: Operational data from Smart Sensors & Actuators in CERTH's Smart Home use case scenario

Smart Sensors and Actuators	Description
Dimmer	Dim Level, CO2
Temperature	Temperature
Luminance	Luminance
Humidity	Humidity
SmartPlug- Power Meter + On/Off Actuator	State, Consumption
People Counter	Entry/Exit
Magnetic Contact for doors windows	State
Panic Button	Signal
Motion Sensor	State
CO	CO
Smart Lamp	Dim Level, Colour Temperature
Smart Spot Light	Dim Level
Water Sensor	PH, Temperature, Water Level, Water Leakage
Environmental Platform/Agricultural Sensor	Wind Speed, Wind Direction, Rain Concentration, Leaf Wetness, Soil Temperature, Soil Moisture / Water Tension, Temperature, Humidity, Pressure

- In the Smart-Home there are smart devices and appliances sending operational data over the network and they are listed in Table.

Table 7: Operational data from Smart Appliances in CERTH's Smart Home use case scenario

Type of smart device	Measurements
Smart Plugs	Power consumption, Operation State
Smart Oven	Selected Program, Active Program, Set-point Temperature, Duration, Elapsed Program Time, Remaining Program Time, Program Progress, Power State, Remote Control Active, Remote Control Start Allowed, Local Control Active, Operation State, Door State, Current Cavity Temperature, Preheat Finished (Event), Program Finished (Event)
Smart Dishwasher	Selected Program, Active Program, Start In Relative, Remaining Program Time, Program Progress, Power State, Remote Control Active, Remote Control Start Allowed, Operation State, Door State
Smart Refrigerator	Power State, Door State, Images from the fridge
Smart Dryer	Selected Program, Active Program, Program Finished, Drying Target, Remaining Program Time, Program Progress, Power State, Remote Control Active, Remote Control Start Allowed, Operation State, Door State
Smart Washing Machine	Selected Program, Active Program, Temperature, Spin Speed, Remaining Program Time, Program Progress, Power State, Remote Control Active, Remote Control Start Allowed, Local Control Active, Operation State, Door State, Program Finished

2.5 Honeypots in the use cases

In all the use cases, customized honeypots will be deployed. The Honeypots in the use cases are equipment designed to capture traffic from attacks and they trace the commands performed by the attackers. These attacks may originate from insiders or outsiders of the Smart grid system. The network attack traffic together with device logs are analysed in order to learn how the attacks are generated and propagated. The only information processed by Honeypots about the attackers are the IP Address from which the attack was generated, and the commands or actions attempted to be performed by the attackers. Therefore, unless the IP Addresses refer to personal equipment used to perpetrate the attack, no personal information is processed by honeypots. Usually, no personal equipment is used to launch the attacks, but they are made from public IP Addresses (e.g. public Wi-Fi networks, networks of public Libraries, etc.) or from anonymised networks such as Tor.

3. Legal Framework of Electronic Evidence and Forensics Processes

Over the years, people's interactions have significantly moved to the online environment; activities such as banking, purchases, social interactions, industrial operations, etc., now increasingly happen over internet platforms. These activities also leave traces that could form evidence in the future in either criminal or civil cases. This invariably means that evidence collected for crime prosecution is now increasingly in the digital form compared to physical evidence that hitherto used to be the case (both in relation to new forms of online (or cyber-) crime and traditional offline crime). As regards the latter, it is notable that physical and analogue evidence can be digitized, thereby increasing the volume of electronic evidence overall. Electronic evidence could be obtained from various sources including but not limited to:

- computer systems [30] —laptops, phone, tablets, etc.;
- storage devices—hard disks, USB sticks, etc.;
- removable media—compact disk, digital video disk, etc.;
- peripheral devices— scanners; printers, tape drives, etc.;
- computer networks and connection devices—Local Area Network, Wide Area Network, Wireless Access Point, etc.

From these sources, various kinds of data can be obtained as digital evidence including sound, text, video, photograph, traffic data, content data, metadata, etc.

Reflecting the breadth of the above, the Council of Europe defines electronic evidence widely as "*any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceeding*" [9] Such evidence may be located or stored anywhere (e.g., in the cloud, composed of server-farms in various regions of the world), which makes it difficult to prosecute cybercrime in several instances due to the complex issues involved in obtaining evidence from another jurisdiction that may have different disclosure rules. There are also other challenges due to the nature and volatility of such evidence; they could be manipulated, deleted, etc., which raises the issues of the authenticity of the evidence. In this regard, just as with physical evidence, electronic evidence needs to be authenticated and verified, as this can affect the admissibility and weight of the evidence in legal proceedings. Over the years, emphasis has been laid on the method of collection, preservation and exchange of electronic evidence to ensure the integrity of such evidence. In this respect, a number of key principles of electronic evidence gathering have crystallised, including:

1. **Data Integrity**: No action taken should materially change any data, electronic device or media which may subsequently be used as evidence in court.
2. **Audit Trail:** A record of all actions taken when handling electronic evidence should be created and preserved so that they can be subsequently audited. An independent third party should not only be able to repeat those actions, but also to reproduce the same result.
3. **Specialist Support:** If it is expected that electronic evidence may be found in the course of a planned operation, the person in charge of the operation should notify specialists/external advisers in time and arrange their presence if possible.
4. **Appropriate Training:** First responders must have the necessary and appropriate training to be able to search for and seize electronic evidence if no specialists are available at the scene.
5. **Legality:** The person and agency in charge of the case are responsible for ensuring that the law, the evidential safeguards and the general forensic and procedural principles are followed to the letter [10].

The first two principles are especially relevant for the SPEAR FRF as it could guide in the collection and logging of network attack traces that would be relevant for proceeding in the future. In this respect, therefore, establishment and employment of proper procedures, techniques and tools are important in network forensics framework. These procedures should also be capable of dealing with various technical and legal challenges specifically associated with network-based evidence, as further described below.

3.1 Challenges associated with Network-based evidence

3.1.1 Technical Challenges

A number of particular technical challenges have been associated with gathering network-based evidence for forensics purposes [31]. These include but are not limited to:

- **Acquisition and volatility:** network-based evidence is volatile in the sense that certain network data can change over a short period of time, even when data processing is going on (e.g. with dynamic IP addresses). Vital evidence can also be lost in a few seconds, such as during log analysis because logs change rapidly. In some cases, permission required to get evidence e.g., from relevant Internet Service Providers (ISPs), may take some time, thereby increasing the chances of evidence loss [31]. Live forensics additionally present challenges because items such as the Random Access Memory (RAM) are changing during the data acquisition. This means that the results are not reproducible as the initial data has changed [32]. This presents a delicate scenario in terms of how to acquire the network traffic data and store it without losing the integrity of the data, as well as traceability and auditability of the evidence sources.

- **Encrypted data:** The use of forensic methods at the Ethernet level is done by listening to bit-streams using monitoring tools or sniffers. Several tools collect all data at this level and allow the user to filter different events. However, data can only be recovered using these tools if they are sent or received unencrypted. Almost all protocols widely used in critical infrastructures and particularly in smart grids applications are gaining support or have already created for native end-to-end Transport Layer encryption using TLS. Secure web connections over HTTPS has been a standard for online merchants, webmail, and financial sites for several years. As TLS-based encryption becomes more common for legitimate uses, it has also become more common for malicious purposes. Nearly any protocol being used in smart energy infrastructures can be wrapped in an TLS to help avoid detection and logging (eg., reverse command shells, and malware beaconing activity).

3.1.2 Legal Challenges

Apart from the technical challenges cited above, there also several legal challenges associated with gathering network-based evidence. In a broad sense, these have a positive and a negative aspect: the first relates to ensuring that the evidence gathered DOES have the necessary quality (in terms of meeting applicable legal standards) to be admissible and useful (in the hands of LEAs) for prosecuting cyber-attackers; the second goes to ensuring the collection and processing of evidence DOES NOT violate rights of anyone (be they cyber-attack victims, attackers, or third parties). Here privacy/data protection are the key issues.

Previously, the rules on data protection as these apply to data collection in SPEAR for the research purposes of the project (advancing pattern recognition of cyberattacks and knowledge of cyberattack strategies) were outlined in Deliverable D2.1. However, in the present Section (under 3.1.2.2) the further privacy/data protection requirements in the further context of processing and retaining such data for later evidential purposes are given attention. First, though, we address the positive rules in respect of reliability and admissibility of digital evidence.

3.1.2.1 Challenges related to relevance and admissibility

One of the fundamental conditions for receiving evidence in court proceedings is that the evidence must be a plausible and reliable indicator of the fact in issue that its adducer is seeking to prove, which ultimately affects its admissibility in court [33]. Conditions and rules of admissibility vary in national systems, and may involve a complex area of law: from rules of the court to substantive law. A broad distinction here is between civil law systems, which favour an ‘inquisitorial’ approach to proof of facts (in which the court itself may take an active role in seeking relevant evidence) and the ‘adversarial’ approach of the common law, where the parties to the proceedings exclusively determine which evidence to present and the court (typically supplemented in criminal cases by a lay jury as fact-finder) has a more passive role as adjudicator between the respective factual contentions of the parties. Under the latter system, there are often special additional rules for checking the likely probative (versus prejudicial) value of certain forms of evidence before it comes before the (lay) jury. By contrast, in jurisdictions using the inquisitorial approach, it is generally left for the court (with a professional judge as fact-finder) to determine the strength of evidence or its probative value when it has been adduced in the proceeding.

As noted, in the context of SPEAR, the issue of usability of electronic evidence will be relevant during the exploitation phase, following the project lifetime, when users of the system may elect (or be required) to provide it to their relevant LEAs; as such, the legal technicalities concerning the admissibility of such evidence will be a matter for the LEA operating under the rules of criminal procedure in its particular jurisdiction. Nonetheless, the arrangements in SPEAR should seek to ensure such evidence is collected and stored in accordance with underlying best practice principles for digital forensic governance (see further section 3.2.1.3 below), so that – at the point of handover from the SPEAR user to the LEA – it has a significant likelihood of acceptance as admissible and cogent evidence in potential criminal proceedings. In general, issues that may affect the admissibility and weight of evidence include:

- **Evidence management:** Often, inadequate protocols and procedures to collect, preserve and process electronic evidence lead to contamination of the evidence or compromising of the chain of custody. The chain of custody aims to guarantee the integrity of the data between its creation and its usage in court, therefore the court must be satisfied that evidence has always been safeguarded from the moment of the collection to the trial. National law regulates the issue of chain of custody and how it affects the admissibility of evidence. In some countries, a distinction is drawn between compliance with the chain of custody of the flow of metadata and that of content data. Breach of custody of content data may have a serious consequence leading to the inadmissibility of the evidence [34]. Admissibility could also be affected by unvalidated procedures or implausible interpretations of evidence, or factors that compromise the reliability of analytical findings and/or the inferential conclusions supposedly based on them [2].

- **Establishing identity:** Establishing the identity of a person acting unlawfully is not an easy task in the online world. Internet users are often not readily identifiable from their user names and possibly IP addresses (which could be dynamic, i.e. liable to change) they use in the course of a communications session. In many cases, painstaking efforts will need to be made to map a user's electronic identity to his or her actual real-world identity, and may involve law enforcement authorities obtaining relevant data from a third party such as the user's ISP, who are themselves regulated in terms of the circumstances in which they can disclose such data [35]. This may also require obtaining a court order, which elongates the process [36] [37].

3.1.2.2 Challenges related to constraints on evidence gathering (so as not to infringe privacy laws and/or fundamental human rights)

- **Privacy and Data Protection:** As was examined in SPEAR Deliverable *D2.1 User, Security and Privacy Requirements*, the processing of data that relates to identified or identifiable human being is regulated by numerous legal instruments, such as (in the EU) the GDPR, and Directive 2016/680, the e-Privacy Directive, which applies where such data is obtained from a network traffic. The rules set out in these instruments regulate what type of data can be processed, logged, monitored or retained from a network traffic and the legal basis for such processing. Where specific safeguards mandated by law for the protection of privacy rights are violated, it may be immaterial whether the data belongs to an attacker or a legitimate end-user; in either situation, the person who collected/processed the data may be liable to serious penalties (Art 83, GDPR). Moreover, such violation may also impact on the lawfulness and admissibility of the evidence in court. Thus, in some jurisdictions obtaining evidence unlawfully may affect its admissibility in court (the 'fruit from the forbidden tree' doctrine) [38]. Similarly, as described in detail in Deliverable D2.1, insofar as the collection of the data itself was lawful, there are further principles of fair processing, such as data minimization must be adhered to when processing personal data. This, however, presents a trade-off between the needs of forensic experts to collect as much data as possible to link the incident under investigation and the legal constraint not to collect data indiscriminately. A similarly important point to mention here is the data retention period applicable to services providers may be limited as to how long personal data obtained for telecommunications can be stored. Where this data is deleted after this retention period, the evidence that could be based on them may not be recovered. Following the invalidation of the Data Retention Directive by the CJEU [39], various EU states have devised their own laws on data retention. This means that network traffic data stored by the ISPs have a limited lifespan.

- **Constraints in monitoring communications:** One avenue through which public or private entities may safeguard information systems is by proactively monitoring the network traffic. As a rule of thumb, the right to monitor such traffic will generally differ between public communication networks and private communication networks, such as a corporate intranet operating over a WAN. In most jurisdictions, monitoring traffic over public communication networks is more strictly controlled; different rules may also apply depending on whether it is the law enforcement agencies or private entity doing the monitoring [35].

  Monitoring a private network may also trigger some legal constraints. For example, under the UK's Regulation of Investigatory Powers Act 2000, it is a criminal offence to intercept a communication being transmitted over a private communication system except in the circumstances permitted under the Act, such as where the person has a right to control the operation or the use of the system (system controllers) or there is express or implied consent of the affected persons to make the interception [40]. However, this exemption is only applicable when the interception is carried out for a lawful business practice [35] [41]. Privacy and data protection law may also affect how personal data obtained through such monitoring may be processed, such as in the case of employee data.

  Private entities could also monitor traffic on private communications networks using honeypots and related deception techniques. Some of the ethical issues presented by the use of honeypots have been documented in Deliverable D2.1 such as data protection compliance issues. It is notable that in some jurisdictions, such as the United Kingdom, where the honeypot has been established by, in co-operation with, or at the instigation of public law enforcement agencies, there is the possibility that it could be characterized as a form of entrapment [35] [42]. This may affect the use of the evidence in actual proceedings. The legal implications of the specific honeypots to be established in the SPEAR Use Cases are addressed further below in section 4 of this Deliverable.

3.2 Laws, Guidelines and Standards applicable to digital evidence including network-based evidence

At the outset, it is important to point out that there is no comprehensive international or European legal framework on the processing of electronic evidence. Traditionally, how electronic evidence is collected, assessed and regulated is a matter of national law. Therefore, national law is always the primary point of reference, although there are differences in national legislation and approach among nations, a factor that makes handling transnational electronic evidence difficult in most cases. However, there are several international and European instruments and policy documents that are relevant to electronic evidence, which often inspire national laws, or may require implementation into the national legal system.

In this regard, numerous instruments that may affect how electronic evidence is acquired, processed, exchanges and stored can be identified. Addressees of these laws take various forms, from States to law enforcement and judicial authorities. Private entities may also be implicated, where general rules such as data protection rules apply. For example, EU laws such as Directive 2014/41/EU regarding the European Investigation Order (EIO) in criminal matters and Directive 2016/680 on data protection by law enforcement agencies contain rules that affect electronic evidence, but only apply to law enforcement and judicial authorities (or entities that fall with the definition of competent authority) and therefore, may not be directly relevant to the SPEAR FRF design [43]. On the other hand, there are laws that may have an immediate impact in the design and framework of the SPEAR FRF in terms of containing rules and principles applicable to the SPEAR platform or that need to be mirrored to implement good practices in the use of the SPEAR forensics tool. Most important in this regard are the rules that affect the collection of data that may be used as evidence, where such data falls within the legal definition of personal data. Furthermore, there are guidelines and standards which focus on methodology for acquisition, storage, integrity etc., of electronic evidence or that contain good practices that increase the admissibility of the evidence that need to be considered as well.

Given this state of affairs, this report will look at the issue from international, regional and national perspectives, but with a focus – in view of the primary planned market for the SPEAR product – on common approaches that apply broadly across the European continent. In the remainder of this Chapter 3, the key applicable laws and standards are introduced and described in a generic way; thereafter, the following Chapter 4 goes on to assess their specific implications and application to the work of the SPEAR project.

3.2.1 International Law

As stated earlier, there is no single international law instrument that focuses on electronic evidence, however, rules and principles of fundamental rights and freedoms have a bearing on the issue of criminal law and evidence. Protecting fundamental rights such as a fair hearing, freedom of expression, personal data protection and privacy are relevant in such matters. This means that measures taken to obtain and exchange electronic evidence must be proportionate, and respect core human rights values such as dignity, equality, and the rule of law. For example, the right to a fair trial in criminal proceedings, where electronic evidence forms part of the prosecution case, demands that the accused should be given necessary information on the case against him or her so as to prepare their defence. Denying them such rights due to the electronic nature of the evidence (or indeed for strategic cyber-defence reasons, such as to avoid disclosing the way in which the evidence was gathered) may affect the case. Respect for these values means that law enforcement, prosecution and the judiciary authorities should execute investigative powers and procedures subject to human rights and liberties as prescribed under international instruments such as the United Nations International Covenant on Civil and Political Rights (ICCPR) [44]. Article 14 of the ICCPR, for instance, recognises that anyone accused of a criminal offence shall be entitled to a fair trial and have adequate time and facilities for the preparation of their defence. Article 17 equally recognizes the right to privacy.

3.2.2 European Instruments

3.2.2.1 Council of Europe

3.2.2.1.1 The European Convention on Human Rights (ECHR)

The ECHR guarantees certain rights that are relevant for gathering and processing electronic evidence. The most important rights in this context include the right to respect for an individual’s private and family life, their home and their correspondence and the right to a fair trial. The right to private life is not absolute; it may be interfered with by a public authority “in accordance with the law and as necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others” [45]. Courts have on several occasions attempted to balance the need for public security and right to privacy and have emphasized the need to be proportionate (i.e. strike an appropriate balance between the affected interests) in any measure aimed at interfering with fundamental rights [46].

Regarding the right to a fair trial, Article 6 of the ECHR guarantees that in the determination of civil rights and obligations or of any criminal charge against a person, such a person shall be entitled to a fair hearing. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law, and everyone charged with a criminal offence has the minimum rights to have adequate time and facilities for the preparation of their defence, among others. The relevance of this provision to the SPEAR framework lies in the ability to verify evidence and ensure its integrity by a third party, which could affect the defence of an accused as well as the admissibility of the evidence in a trial.

3.2.2.1.2 The Cybercrime Convention

The Cybercrime Convention (often referred to as 'the Budapest Convention') is perhaps the only international treaty that contains both substantive and procedural provisions that are relevant for electronic evidence. It requires the state parties to adopt legislation and measures in their respective domestic laws to combat cybercrime. Regarding the substantive law element (that define the acts to be criminalized), the Convention requires state parties to legislate offences against the confidentiality, integrity and availability of computer data and systems, such as illegal access, illegal interception, data interference, system interference, etc. The nature of these offences is relevant for SPEAR, as cyberattacks are covered within their definition. For the purpose of criminal investigations or proceedings, the Convention also contains procedural rules on the collection of evidence in electronic form where a substantive criminal offence is suspected. These rules relate to expedited preservation of stored computer data, including traffic data (Arts 16 and 17); production order (Art 18); search and seizure of computer data (Art 19); real-time collection of traffic data (Art 20); and interception of content data. Importantly, the Convention notes that the powers and procedure it provides shall be subject to adequate protection of human rights and liberties (Art 21).

Although the Convention does not include precise methodology on how to obtain electronic evidence, the Council of Europe has published guidelines for the collection, preservation and use of evidence—the Electronic Evidence Guide [10]. This non-binding guide is meant for law enforcement and judicial authorities, but is also valuable for other practitioners as it provides guidance and good practices on the handling of electronic evidence to ensure its authenticity for later admissibility in court. As discussed further in Section 4 below, this includes certain guidance relevant to network forensics that the SPEAR framework could mirror. For example, regarding the time when an IP address is used by device of forensic interest, it recommends that "the investigator must be able to pinpoint with absolute precision the exact moment in which a given IP address becomes relevant for his investigation […] (IP X.X.X.X on 24/05/2012 16:30:12h (UTC-10)" [10]. This goes to the issue of creating an authentic timestamp of the evidence for its integrity.

3.2.2.1.3 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

This Convention is the first binding international instrument in the specific area of data processing by automatic means and seeks to regulate at the same time the transborder flow of personal data. Its scope cover data processing in the private and public sectors. Originally adopted in 1981, the Convention was recently updated to bring it in line with the advancements in information technologies, and to harmonise it with the GDPR [47]. The Convention provides principles of processing personal data to which state parties shall undertake to apply. These principles were updated in the modernised version to include principles of transparency, proportionality, accountability, data minimisation, privacy by design, etc., and are similar to those incorporated into the GDPR as analysed in Deliverable D2.1. The Convention also enshrines rights of the data subjects, exemptions, as well as safeguards for transborder flows of personal data among the parties and issues of mutual cooperation among them.

Although the convention does not specifically mention electronic evidence, by implication, any personal data that undergoes automatic processing within the territory of the state parties and forms evidence is covered by the principles of this Convention. A more specific area where these principles have been applied is in the Police sector as seen in Recommendation 87 (15) discussed below.

3.2.2.1.4 Recommendation 87 (15) of the Committee of Ministers to member states regulating the use of personal data in the police sector

Recommendation 87 (15) represents a sectorial approach to protecting personal data in the law enforcement circle. The Recommendation contains several principles relevant to the collection and transfer of personal data including electronic evidence in the police sector [48]. These principles include: Control and notification; Collection of data; Storage of data; Use of data by the police; Communication of data; Publicity, right of access to police files, right of rectification and right of appeal; Length of storage and updating of data; and Data security.

While Recommendation 87 (15) is targeted at the police sector, some of the contents of these principles appear relevant for the development of the SPEAR FRF and will be highlighted below.

- Under Principle 2.1, collection of data shall exclude open-ended, indiscriminate collection of data by the evidence gatherer. Similarly, Principle 3.1 provides that the storage of personal data should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of the law. These reinforce the broader data protection principles of data minimisation (set out in the 1981 CoE Convention, and parallel EU data protection legislation) as well as the principle that data must be adequate, relevant and not excessive in relation to the purposes for which it is stored.
- Under Principle 4, personal data collected and stored should be used exclusively for the purposes for which it is collected. This, again, reinforces the data protection principle of purpose limitation.
- Under Principle 6, data subjects have the rights of access and rectification of data.
- Principle 7 requires that personal data are deleted if they are no longer necessary for the purposes for which they were stored.
- Principle 8 enjoins the responsible body to take all the necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration.

These principles are core to protecting the rights to privacy and data protection, and are certainly relevant for systems that intend to process personal data for evidential purposes. Recently, the Council of Europe also published non-binding guidelines on electronic evidence in civil and administrative proceedings targeted at judicial and other dispute-resolution authorities including legal practitioners [49]. They reiterated fundamental principles that guide the courts in handling electronic evidence and relevant provisions of these guidelines, as they bear on recommended practices for SPEAR, will be discussed further below.

3.2.2.2 European Union

It is worth reemphasizing that at the EU level, there is no harmonised legal framework or rules on digital evidence handling in terms of acquisition, admissibility, etc. These issues are mainly dealt at the national level. However, there are few legal instruments that can be directly or indirectly relevant to the collection, storage, processing and exchange of electronic evidence at the EU-level, which require implementation by the Member States. The European Commission has also proposed an electronic evidence rules in the form of a Regulation and a Directive, which is undergoing legislative processes now [50]. Instruments that are relevant to SPEAR FRF will be considered below.

3.2.2.2.1 Charter of Fundamental Rights of the EU (CFREU)

The CFREU contains provisions that can affect how electronic evidence is obtained and processed. Articles relating to the right to privacy (art 7), the right to data protection (art 8), the right to a fair trial (art 47) and presumption of innocence and right of defence (art 48) are relevant in this regard. The rights to privacy and data protection, for example, impose constraints on how personal data can be collected, requiring a legal basis for such collection. As already mentioned, the right to a fair trial in criminal cases means that the accused shall have the facilities, including having all the relevant information about the case they require to properly prepare their defence.

3.2.2.2.2 General Data Protection Regulation (GDPR)

Gathering and exchanging electronic evidence impact data protection rights where the data at issue relate to an identified or identifiable person. Where this is the case, the general principles of data protection need to be considered in the data processing. These principles include the principles of lawfulness, fairness and transparency; data minimisation; purpose limitation; accuracy; storage limitation; integrity and confidentiality and accountability. The data controller shall also enable the exercise of the data subjects' rights and observe other obligations. These principles and obligations provide constraints on how personal data may lawfully be processed and/or stored, as previously explained in Deliverable D2.1- User, Security and Privacy Requirements.

Admittedly, the GDPR does not apply to competent (law enforcement) authorities when they process data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Art 2 (2) (d)). This exception could also extend to private investigators / CSIRTS in cases where an LEA delegates a particular cyber-investigation to them. In such a case the investigator would instead be bound by the data protection rules set out in the Law Enforcement Directive 2016/680. Nonetheless, in the majority of cases where a private cyber-investigator does not act on behalf of an LEA, they will be bound by the more general GDPR principles; here it is immaterial that the data is processed for purposes related to crime prevention or investigation (or that the investigator intends later to turn the evidence over to an LEA). This applies to the SPEAR FRF because the tool will be used largely by CSIRTS not acting as a competent LEA.

There are provisions in the GDPR relating to data on criminal offences. Article 6 (4) (c) provides that the data controller shall take the nature of data relating to criminal convictions and offence, among others, into consideration when accessing the compatibility of further processing data that was initially collected. Article 10 also provides:

> Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

This provision may be interpreted to cover only data related to already concluded criminal cases. It does not, therefore, restrict the processing of other data that may be useful in a future criminal proceeding as evidence (provided always that the controller can point to another basis for such processing, and adheres to the other relevant processing principles and safeguards of the GDPR).

3.2.2.2.3 Directive (EU) 2016/680 on Data Protection in Law Enforcement

The Data Protection for Law Enforcement Directive [51] lays down the specific rules relating to the protection of natural persons when their 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, including the safeguarding against and the prevention of threats to public security. Competent authorities referred to include public authorities such as the judicial authorities, the police or other law-enforcement authorities as well as any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. It provides safeguards to protect the right to personal data when processed by competent authorities and incorporates data protection principles to be observed in such cases. These principles are listed in Article 4 of the Directive and are similar to the ones mentioned in the GDPR, which have been analysed in Deliverable D2.1. As discussed in the preceding subsection, this Directive will not apply to SPEAR end-users, except in circumstances where they fall under the definition of a competent authority under Article 3 (7) (b) of the Directive.

3.2.2.2.4 Directive on Privacy and Electronic Communications (e-Privacy Directive)

The e-Privacy Directive [52] aims to secure privacy in the digital age, and more specifically the confidentiality of communications and provides rules regarding tracking and monitoring of communications. It enjoins the Member States to provide for measures to be taken by providers of electronic communications service to prevent unauthorised access to communications including both the contents and any data related to such communications when transmitted over public communications networks and publicly available electronic communications services. It prohibits listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data, except when legally authorised (Art 5). However, Article 5 (2) provides that this does not preclude “any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.”

The e-Privacy Directive draws a distinction between traffic data, location data, and content data. Traffic data refers to ‘any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof’; location data ‘means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service’ while content data refers to ‘any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data’ [53]. Different rules apply to the processing of these data. For example, due to its special sensitivity, processing of the content of telecommunication is not permitted, except under certain circumstances such as by LEAs and pursuant to a court order.

It is also notable that a data retention directive amending the e-privacy Directive, which required the providers of publicly available electronic communications services or public communications networks to retain traffic and location data for a minimum period of six months and up to two years, for the purpose of preventing, investigating, detecting, and prosecuting serious crimes had been invalidated by the CJEU in the case of *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources* [39]. Although this state of affairs is of limited relevance to SPEAR, it is important to note that the Members States have their own instrument on retaining such data in a non-harmonised manner, which is more relevant to ISPs and LEAs per se.

3.2.2.2.5 Directive 2013/40/EU on Attacks against Information Systems

This instrument (often known as the ‘Botnet Directive’) approximates the criminal law of the Member States in the area of attacks against information systems. It establishes minimum rules concerning the definition of criminal offences and the relevant sanctions in this area, as well as for how competent authorities and EU agencies shall cooperate in this area. The Directive requires that member states create in their national law offences such as illegal access to information systems, illegal system interference, illegal data interference, illegal interception, production, sales, etc., of tools used for committing these offences, as well as the incitement, or aiding and abetting of such activities.

The Directive recognises that its application shall respect human rights and fundamental freedoms, including the protection of personal data, the right to privacy, freedom of expression and information, the right to a fair trial, the presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties. Although the Directive does not dwell on evidence, the offences it defines are relevant for SPEAR, such as when an attack is a DoS or DDoS and interferes with the system. The EU Member States have implemented this Directive and there is a legal basis for prosecuting such attacks.

3.2.2.2.6 The eIDAS Regulation

The eIDAS Regulation [54] aims to ensure the proper functioning of the internal market while at the same time providing an adequate level of security of electronic identification means and trust services. It lays down conditions under which the Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State, as well as the rules for trust services, in particular for electronic transactions. It also establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, and certificate services for website authentication.

Paper and electronic documents are used daily in commerce and everyday activities. Such documents may later form evidence in relevant legal proceedings [55]. The eIDAS Regulation ensures that electronic signatures are admissible as evidence in legal proceedings and that they are not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the ground that they are in electronic form (the principle of functional equivalence). Although the Regulation does not dwell on the collection, preservation, use and exchange of network-based evidence, certain facilities that it provides such as the electronic time stamps can be relevant in addressing the integrity of evidence in legal proceedings.

3.2.3 National Laws and Procedures relating to electronic evidence

As earlier indicated, diverse national rules regulate the law of evidence, which have emerged as a result of discrete legal traditions in different jurisdictions. These include procedural law – civil or criminal, rules of courts, fundamental rights, etc., which affect what is admissible and how it can be introduced as evidence in a court proceeding. In practice, a number of factors come into play here including how the prosecutors build their case and their advocacy skill, the lawfulness of obtaining the evidence and the exclusionary rules, etc. An important factor too will be whether the finding of fact will be made by a lay jury (as in common law systems, or a professional judge (in civil law systems), as well – of particular salience in complex forensic situations – how far the court will have the benefit of expert technical advice. While these aspects are beyond the scope of SPEAR, lessons could be learnt from certain national rules on safeguards to be adopted when collecting and preserving evidence, the rules of personal data protection, and what factors could facilitate the admissibility of electronic evidence before the national courts.

Although there is a conceptual difference between the inquisitorial and adversarial systems as pointed our earlier, some common features in the national systems regarding electronic evidence can still be identified. For instance, just as in the case of non-electronic evidence, electronic evidence is subject to cardinal requirements of relevance, reliability and admissibility. The first of these aspects concerns simply whether, in factual causal terms, the evidence bears on the probability of the particular contention of the prosecution (which has the burden of proof) being true. As regards reliability, this goes to the state of the item of evidence itself as an authentic and accurate record of what occurred. In the context of new forms of electronic evidence, there have been varying degrees of resistance to / distrust in different jurisdictions of such evidence, based on concerns that – compared to traditional, tangible items of evidence (such as a paper record) it may be easier to falsify. However, increasingly, as its use has become more commonplace and better understood, such concerns have diminished [56]. At least, the courts will now generally be prepared to admit the evidence and leave it for the party adducing it to provide all possible ancillary evidence to strengthen the primary evidence. This may involve calling a forensic or computer expert to prove the authenticity and non-manipulation of the data. Such developments, and more general progress within the EU in facilitating the transfer/obtaining of evidence across member state borders (under the EIO Directive 2014/41/EU), have also fostered hopes for progress at the EU level in framing common minimal standards for the admissibility of electronic evidence. However, as yet these initiatives remain nascent [57]. For the time being, once electronic evidence has been transmitted to the courts, it will be managed by each country's own national judicial information system for collecting and preserving evidence. In Bulgaria, for example, this is regulated by Ordinance No 5 [58].

The remainder of this section will focus briefly on relevant aspects of computer crime and evidence law in the countries where the SPEAR validation exercise will take place, namely Bulgaria, Greece, Spain, and France. Although, as noted before, any evidence collected within the development phase of the SPEAR FRF will be used for research purposes only, and not handed to the LEAs in those countries for use in investigating or prosecuting cyberattacks, this survey points up the variations of detail currently typical between different jurisdictions (even within the common EU framework) in dealing with digital evidence. When the SPEAR FRF is available as a final product to users across Europe and beyond (in the project exploitation phase) such differences will naturally be multiplied. First, as one would expect, given that each is a signatory to the 2001 Budapest Convention (and more recently also bound by the EU Botnet Directive), all four jurisdictions have relevant substantive offences criminalizing cybercrime, including cyberattacks on computer networks.

In Bulgaria, several forms of conduct, which may affect the integrity of an IT system, are criminalized. These include the unlawful copying, use or obtaining access to data in a computer system without permission; the installation, modification, deletion or destruction of a computer program or computer data without consent by a person administering or using the computer system, etc., (Art 319a-c of the BL Criminal Law). These provisions provide the basis for prosecuting such crimes, which impact upon the security of smart grid systems. Similar provisions can be found in the respective Criminal Codes of France (i.a. Article 323-1 FCC), Greece (i.a. Article 370 GCC), and Spain (i.a. Article 197 SCC). As regards the evidence relevant for prosecuting such crimes, as noted these will be managed by the relevant national judicial information system for collecting and preserving evidence.

Electronic evidence is admissible in the Bulgarian legal system and has the same probative value as other non-electronic evidence [59]. As for the safeguards to be adopted when collecting evidence (in general), Bulgarian law provides for several procedural measures to be respected, for instance, by the investigative authorities. For instance, with regard to the search and seizure procedure, when circumstances regarding the private life of the citizens have been disclosed during the search, necessary measures shall be taken so that they are not made public (Article 163, Para 5 of the Bulgarian Criminal Procedure Code). Interception and seizure of correspondence shall be allowed only when it is necessary for the detection and prevention of serious crimes. Third parties may collect facts which may be considered electronic evidence, and must be presented in court in accordance with the procedures under the Criminal Procedure Code [59].

For its part, in Spain a relaxed approach prevails, in which special procedural formalities (such as certification) are not a prerequisite for electronic evidence to be admitted; rather, pursuant to the principle of free judicial evaluation the judge may assess for him/herself the probative weight to be given to each item of evidence (including in electronic form) and whether in the circumstances its value outweighs the risk of unfair prejudice to potential defendants. In this regard, the judge will need to be satisfied of the authenticity of the evidence (its authorship/circumstances of creation are as the prosecution claims) and its integrity (the content has not been altered between the time of its creation and use in court). If suspicions arise regarding either of these matters, it is likely the judge will deny the effectiveness of the electronic evidence [60]. This is also broadly the position in France, where moreover there is emphasis on the parity by default of evidence embodied in different media (Loi no 2000-230 du 13 mars 2000) [61].

In certain jurisdictions, there are also automatic rules of exclusion in cases where the evidence has been collected unlawfully (for example in violation of the defendant's protected constitutional rights). This exclusionary approach, which serves as a powerful check on the zeal of law enforcement authorities, is well-known in the US, where it operates as an effect of the Fourth Amendment (prohibition on unreasonable search and seizures). By contrast, in Europe, it generally has less influence; instead as noted for France and Spain the approach of free evaluation of evidence (by the court) takes precedence, where the judge has a discretion to exclude such evidence but is not required so to do. Nonetheless, in Greece there is a legal constraint on obtaining evidence in breach of human rights, including privacy rights. Though it is not conclusively settled whether this automatically results in the exclusion of the evidence in question as inadmissible, there is a Constitutional provision prohibiting the use of evidence acquired in violation of certain articles of the Constitution [62].

Lastly, there is the matter of the differential application of privacy/data protection laws as between different national systems. This aspect was explored in Deliverable D2.1, where it was noted that – even after the introduction of the GDPR - discrepancies in this area continue to apply also between EU member states, where the GDPR has allowed for this. Similarly, in terms of the practices and procedures of the responsible data protection supervisory authorities in the different member states (acting pursuant to Article 55 et seq), these may also vary, including in respect of the prior consultation expected from data controllers with such authorities for particular types of high-risk data processing. As noted in Deliverable D2.1, here it is advisable that prior to the deployment of the use case tools during the SPEAR project development phase, the project end-user partners liaise as appropriate with their relevant authority to check how far any special authorizations may be needed, in particular for deploying honeypots. (There are some hints in French legal literature 63 that this was at least at one time the case in France, where the relevant supervisory authority, CNIL, is competent [64]. As noted, this diversity evident in various dimensions of national law on electronic evidence will only be amplified in the exploitation phase of the SPEAR Project, when in principle users from any jurisdiction may deploy the system. A further point is that the relevant positive laws we have been considering are not static, but liable to change. Indeed, they are currently in the process of ongoing reassessment and reform, under pressure of rapid technical change in the IT sector, with the likelihood of further initiatives to achieve rules of mutual recognition at European level. For these reasons, the approach of the SPEAR project will not tie itself to a (fruitless) attempt to be compatible with the current rules of a particular jurisdiction but be directed to the achievement of sound principles of e-evidence management, in the form of generally accepted cyber-investigator community standards (as reflected in key current good practice guidance). We consider this key good standard guidance in the next section.

3.2.4 Relevant Guidelines and Standards

This section describes some standards and guidelines in the area of digital forensics that are commonly used in Europe and across the globe. Although they are meant to apply in a broad environment and cover mainly situations where an incident has occurred and the forensic investigators want to start the investigation, the methodology and procedures they present are nevertheless relevant in a smart grid environment. Thus, they may serve to guide the design of a framework for achieving forensic readiness, particularly, in strategizing how to obtain critical data and maintain the chain of custody over time.

3.2.4.1 ENISA Handbooks and Guidelines

ENISA is the cybersecurity agency of the EU and has published several guidelines and teaching materials on digital forensics, including network forensics [8, 9], [65]. These publications offer a set of detailed best practice, principles, methodologies, tools and procedures for carrying out digital forensics and provide a good source for any entity designing its forensics framework.

With respect to the prerequisites to enable a system to be suitable for network forensics (forensic readiness), ENISA suggests developing a policy on how to monitor the network, what will be monitored (the targets) and what additional data sources besides logs, flow- and packet capture data will be needed [7]. Emphasis is also placed on the collection and storage of data. To maintain the integrity of the evidence, collected data (e.g., logs) must be protected from tampering, or deletion, unauthorised access. Apart from providing some technical details on the nature of forensic data acquisition, several methodologies are presented these materials such as OSCAR, ISO 27037 as well as formative underlying principles of digital evidence.

As noted earlier, ENISA documents also stress the importance for organisations that collect data for forensics purpose to know what legal constraints to comply with (so as not to infringe rights of others). In this regard, the impact of the GDPR relating to privacy protection in the EU on network forensics as privacy-related data, such as IP addresses, packet captures as well as log files may contain personal data. As previously discussed in Deliverable D2.1, data protection laws impose restraints on the processing of personal data which also applies to network-related data processed for forensic purposes.

3.2.4.2 ISO/IEC 27037 Standard

ISO/IEC 27037 - Guidelines for identification, collection, acquisition and preservation of digital evidence, [5] provides guidance on specific processes that forensic investigators – Digital Evidence First Responders (DEFR), Digital Evidence Specialist (DES), incident response specialist and forensic laboratory managers – need to undertake in handling digital evidence. It suggests practical ways that affected investigators can carry out their investigations without compromising the integrity of the digital evidence, thereby increasing the overall likelihood of admissibility of such evidence (across various distinct jurisdictions). The Standard does not cover the aspect of forensic readiness or analysis; it is also subject to specific requirements of national laws and regulations.

The guidance emphasizes three ‘fundamental principles’ of digital evidence:

- **Relevance**: relating to the evidence proving or disproving an element of the specific case being investigated;
- **Reliability:** to ensure digital evidence is what it purports to be;
- **Sufficiency:** the need to collect enough potential digital evidence to allow the element of the matter to be adequately examined or investigated [5].

How to satisfy these principles are provided in the document. For example, it recommends that all processes to be used by the relevant investigator should be validated with respect to the environment and circumstances in which the processes are to be used. DEFR and DES should also ”‘document all their actions, determine and apply a method for establishing the accuracy and reliability of the potential digital evidence copy compared to the original source and recognize that the act of preservation of the potential digital evidence cannot always be non-intrusive” [5].

Regarding the processes of handling digital evidence, the Standard covers only the initial key processes of identification, collection, acquisition and preservation.

- **Identification:** This represents the process of identifying the physical and logical forms of the digital evidence. In this process, both devices containing the data and the data itself are identified, and their collection prioritised based on volatility. Identification should involve a systematic search and labelling to ensure that relevant devices, and data that may be hidden, are not overlooked.
- **Collection:** This is the process of removing the digital evidence from their original location to a controlled environment for later acquisition and analysis. The state of the device—powered on or off—will determine the approach and tool of collection. Documentation is important in this process, including of those devices not collected, and reasonable care must be taken not to damage the evidence during collection.
- **Acquisition:** This is the process of producing a digital evidence copy and documenting the method used and activities performed. The method and tools used for this process are very important and should be documented, be reproducible or verifiable by a competent person. Acquisition should not introduce changes to evidence and should take the least intrusive form possible. Where verification of digital evidence is not possible due to the volatility of the data, the best method of acquisition should be utilised and documented.
- **Preservation:** This is the process of preserving the digital evidence to ensure its usefulness during the investigation. The integrity of the evidence is very important here and requires safeguarding the evidence from tampering or damage. This also goes to the issue of the ‘chain of custody’ of the

evidence, where the chronology of the handling of the evidence is documented and maintained throughout the lifetime of the evidence. Local laws may affect the period of data retention and should be complied with.

As will be seen in the next section, the content of ISO/IEC 27037 reflect other common approaches in this area such as the OSCAR method. However, as the standard dwells on the initial forensics processes, it corresponds largely with the aim of SPEAR FRF.

3.2.4.3 OSCAR Methodology

OSCAR is a Network forensics investigative methodology recommended by Sherri Davidoff and Jonathan Ham. It is an acronym for Obtain information, Strategize, Collect evidence, Analyse and Record [66]. These processes will, the proponents suggest, assist in achieving a successful outcome in the forensic investigation and enhance admissibility of the evidence.

- **Obtain information**: This refers to the process at the beginning of an investigation where information about the incident (including time date, individuals involved, systems and data affected, etc), as well as the environment in which it occurs (e.g., legal issues, resource, organisational structure and policy, etc.) is gathered by the investigator.
- **Strategize**: This is the planning phase of the investigation where potential sources of evidence are assessed and prioritised. The expected effort required to obtain the evidence, and the expected volatility are addressed here as the plan for evidence acquisition is made.
- **Collect evidence**: This is the point of collecting evidence from the identified sources. Important things for the investigator during this process include to: “document”—keep a log of all systems accessed and all actions taken during evidence collection and stored securely; “capture the evidence”—packets and writing them to a hard drive, copying logs to hard drive or CD, or imaging hard drives of web proxies or logging servers; and “store/transport”—ensure that the evidence is stored securely and maintain the chain of custody. Making cryptographically verifiable copies is among the tips offered for this process.
- **Analyse**: This is the process of analysing the evidence gathered from the various sources, making correlations, interpretation, building a case, among others. The analysis could point to a widening of sources of evidence.
- **Report**: This is the point of reporting and explaining the results of the investigation. It should represent the fact and be written in a language understandable by laypersons, while not sacrificing the scientific value.

As this is the methodology provisionally adopted for the SPEAR FRF, an analysis of the requirements for implementing these processes to facilitate the use of the evidence is further made in Chapter 4 below.

3.2.4.4 Guidelines on Digital Forensic Procedures for OLAF Staff

The European Anti-Fraud Office (OLAF) has issued these Guidelines on Digital Forensic Procedures as an internal rule to facilitate the work of its staff regarding the identification, acquisition, imaging, collection, analysis and preservation of digital evidence [67]. The application of these guidelines is directed primarily to the work of OLAF in conducting investigations within the institutions, bodies, offices and agencies of the EU on fraud related cases [68]. However, many of the rules it has developed for conducting digital forensic operations are relevant for cyber-investigators more generally (including in contexts such as the SPEAR FRF), as they are aimed at ensuring the integrity of the forensic data and the chain of evidence in order to increase the admissibility of the evidence in judicial proceedings. This is particularly true of Article 9 of the Guidelines with respect to the safeguards for protecting personal data, including traffic data, which will be further considered – in relation to its suggestiveness for operations in SPEAR – in Chapter 4.

3.2.4.5 NIST Guide to Integrating Forensic Techniques into Incident Response

The NIST guide provides general recommendations for performing a forensic process on sources such as files, operating systems, network traffic, and applications [12]. The guide suggests four phases of conducting digital forensics—collection, examination analysis and reporting. It also includes provision specific to network forensics: the major sources of network traffic data, techniques for collecting data from these sources and the potential legal and technical issues in such data collection.

Key recommendations in the guide with respect to using data from network traffic include:

- Organisations should have policies regarding privacy and sensitive information.
- Organisations should provide adequate storage for network activity related logs.
- Organisations should configure data sources to improve the collection of information.
- Analysts should have reasonably comprehensive technical knowledge.
- Analysts should consider the fidelity and value of each data source.
- Analysts should generally focus on the characteristics and impact of the event [12].

3.2.4.6 Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings

The Council of Europe recently adopted these guidelines to facilitate the use of electronic evidence in court proceedings across the Member States [49]. It is intended that these guidelines should be adapted in the judicial sphere to address issues arising in relation to electronic evidence in civil and administrative proceedings. Although these guidelines deal with judicial authorities, it nevertheless helps other entities such as parties to a dispute, in understanding how courts view electronic evidence, including its relevance, reliability, storage and preservation, among other matters. A key statement to be found is that “the treatment of electronic evidence should not be disadvantageous to the parties or give an unfair advantage to one of them.” The guidelines are also subject to national rules. The most important clauses in the Guidelines that are relevant for the SPEAR FRF are highlighted below:

- Electronic evidence should be collected in an appropriate and secure manner, and submitted to the courts using reliable services, such as trust services.
- Systems and devices used for transmitting electronic evidence should be capable of maintaining its integrity.
- As regards reliability, courts should consider all relevant factors concerning the source and authenticity of the electronic evidence.
- Courts should be aware of the value of trust services in establishing the reliability of electronic evidence.
- As far as a national legal system permits, and subject to the court’s discretion, electronic data should be accepted as evidence unless the authenticity of such data is challenged by one of the parties.
- As far as a national legal system permits, and subject to the court’s discretion, the reliability of the electronic data should be presumed, provided that the identity of the signatory can be validated and the integrity of the data secured, unless and until there are reasonable doubts to the contrary.
- Electronic evidence should be stored in a manner that preserves readability, accessibility, integrity, authenticity, reliability and, where applicable, confidentiality and privacy.
- Electronic evidence should be stored with standardised metadata so that the context of its creation is clear.
- The readability and accessibility of stored electronic evidence should be guaranteed over time, taking into account the evolution of information technology [16].

On the assumption that evidence gathered through the SPEAR FRF will be later handed over to LEAs and cyber-investigators, the relevance of these guidelines to evidence gathering is by and large to the cyber-investigators. However, they provide insight into the judicial processes of the courts in terms of conditions for admissibility of evidence that can affect the design of SPEAR FRF.

4. Implications of the legal assessment on the SPEAR Forensic Framework

The goal of this Chapter is to concretise and analyse the implications of the discussion in the previous section on the development of the SPEAR FRF. At its core, the Chapter has two main objectives: to indicate what the SPEAR FRF SHOULD incorporate (to ensure good use of the output for evidence in the future- positive requirements), and things it should NOT do (to avoid privacy violation- negative requirements). The discussion, therefore, will follow this path. In addition, the implications for the FRF will be referenced at two discrete stages: first, the implications in terms of governing the work of the relevant SPEAR partners in building the tools (during the project lifetime); and secondly, the implications for the way the FRF may later be deployed as a product (project exploitation phase).

4.1 Positive Requirements

These positive requirements aim to maximize the usability of digital evidence gathered in the course of the operation of a smart grid. They traverse throughout the action lifecycle of the framework—from forensic readiness process to the preservation of evidence, and they should be reflected or configured in the SPEAR system architecture so that when used in the future (i.e. exploitation phase), users by default are encouraged to follow current best practice in terms of collection and preservation of digital evidence.

As shown in Chapter 3, there is a complex legal framework in the regional and different national laws of evidence and procedure, which makes it impossible to reflect all these differences in a single framework. However, the aim should be to design SPEAR so that users operate in line with key pan-European principles set out in concrete guidance, such as those from the Council of Europe, ENISA Guidance and ISO standard, thereby addressing the challenges noted in Chapter 3, and promoting reliability/authenticity of the evidence (also transparency – see below). These key relevant guidance and laws as identified in Section 3.2. offer the best model to implement the OSCAR processes for the SPEAR FRF. They also offer forensic investigators insight as to what to pay attention to during collection and storage of the data, in particular, to ensure its reliability at the moment of capture and prevent later contamination. The positive requirements emanating from them will be explained below using the OSCAR processes to exemplify their implementation, while noting that this does not preclude applying other methodologies.

1. **Obtain evidence lawfully.**

It is necessary to ensure that all potential data or evidence is obtained lawfully and in accordance with underlying best practice principles for digital evidence governance. This requirement stems from the fact that data controllers (LEAs, private investigators) must have a lawful basis (eg., authorization, legal obligation) for obtaining data as this may affect the admissibility of the evidence in court. In addition, the failure to abide by lawful practice may have negative consequences for the investigator, particularly where operating (as a non-LEA) under the ordinary law, in terms of itself becoming potentially liable to legal penalties (a point further stressed in the second part of this Chapter – negative requirements). The lawfulness of evidence gathering is emphasized in key guidelines and in national laws considered in Chapter 3 above. For instance, the ENISA Handbook notes: “It should be understood that investigators have to abide by the law, especially since matters may be taken to court” [7]. Minimum requirements (under EU data protection law) for obtaining data lawfully in the case of SPEAR FRF can include obtaining the consent of the Smart Home occupant (see use case 4), having authorization to monitor a smart grids network of an end-user, or relying on legitimate interest of the data controller (i.e. the investigator) to process data.

Although the first step of the OSCAR method (Obtaining information), envisages that an incident has already occurred and the forensic investigator has been called upon to begin the investigation, it should be noted that the SPEAR FRF in practice will begin a stage earlier by ensuring that the system is capable of revealing data necessary for a forensic investigation should an incident occur. This rather fits well into the OSCAR second step (Strategize), which is the process of assessing the resources and planning the investigation. In this regard, a natural part of forensic readiness will involve proactively identifying and prioritizing potential sources of evidence so that data collection and preservation are systematic. This also serves to secure that resultant data is collected in accordance with the principles of fair and lawful data processing.

2. **Integrate strategies that go to show the chain of custody and data integrity right from the beginning of the process in an auditable, repeatable and reproducible manner.**

This requirement suggests having a strategy before an incident occurs with respect to the data collection to prove such an incident in the future. This goes to the core of forensic readiness to support that all relevant data that could be obtained from a network is proactively identified and prioritised (especially for the volatile data), so that data collection and preservation are done in a systematic manner. The ISO 27037 identification process highlights:

> The identification process should identify digital storage media and processing devices that may contain potential digital evidence to the incident. [This…] includes an activity to prioritize the evidence based on their volatility [so as…] to ensure the correct order of the collection and acquisition process to minimize the damage to the potential digital evidence.

The exercise of identifying relevant network devices, logs, and how the evidence could be acquired in the use cases is an example of the strategize process that should be further explored and concretised in Deliverable D4.2 at the outset to balance the needs of sufficiency, reliability and relevance of evidence with other competing principles such as the data minimization principle (as further discussed in the next section).

Other strategies that go to show the chain of custody and data integrity include documentation of all processes right from the initial data collection, through preservation and storage, to the point of potential handover to a competent LEA. This requires that subsequent data collection, preservation and analysis shall be auditable, repeatable and reproducible by an independent reviewer [69]. Mechanisms such as having unique identifiers, timestamping, logging of access to a database where evidence is stored, use of electronic signatures, etc., are some of the recommended practices for demonstrating the integrity of evidence.

3. **Ensure that data acquisition, storage and analysis do not contaminate evidence.**

More importantly, appropriate, reliable and reputable tools and methods should be employed for data capture and storage to avoid damage or contamination of potential evidence, as well as allow for verification of the process of the data collection process. Furthermore, where any initial analysis is made by the end users, this should be done by qualified forensics experts so as to avoid compromising or contaminating the evidence. This point has been highlighted in the CoE Electronic Evidence Guide (discussed in Chapter 3 above), which recommends also that analysis should be done on a copy of the data. This requirement goes to the integrity of the evidence and may affect its admissibility and probative value. It is relevant during the OSCAR processes of collect evidence and analyse.

4. **Integrate the human rights aspect right from the beginning.**

It is equally important that data collection respect the human rights aspect as discussed in Chapter 3, as digital evidence can be open in principle to challenge, when subsequently used in court. An essential aspect of a defendant's right to a fair trial (guaranteed by Article 6 of the European Convention on Human Rights) is that they have a fair opportunity to prepare their defence by knowing the details of the evidence that the prosecution will rely on in the case against them, so that they may contest the accuracy / veracity of items of evidence, where in dispute. This translates in the context of SPEAR FRF into a requirement that the steps relating to how evidence was gathered and stored are comprehensively logged and transparent (open to external review/checking). Issues pertaining to the rights to privacy and data protection are also relevant here, as further discussed in the next section.

4.2 Negative Requirements

In this section, we consider the negative requirements in relation to researching and (later) exploiting the SPEAR FRF on the partners (and subsequent users), in particular as expressed in EU data protection law, primarily in the GDPR. Though in substantive terms the key obligations are also typically couched in positive terms (things the relevant data controllers are required to do), their rationale is not (except incidentally) to enhance the usability of data as forensic digital evidence, but to avoid the occurrence of privacy infringements (contrary to the protected interests of any natural person to whom the data relates (data subject)). For the forensic data gathered in SPEAR, as per the Section 2 Use Cases, and honeypots, the key data protection relevant issues in the context of the SPEAR FRF to consider are:

- Where the forensic data collected/stored includes personal data, what is the lawful basis (as required by the GDPR) for the collection/storage?
- What other main requirements need to be observed by the users of the data for the processing to qualify as fair, and adequately protective of the interests of the data subjects?
- What other regulatory compliance issues arise under the GDPR?

These questions are next considered further by reference to the data collected in each use case in turn (as described in Chapter 2 above). First, in Use Case 1, the Hydro power plant scenario, the data comprises network data transmitted between the plant tools (in Modus TCP/IP and ProfiNet protocols), which are operational data. The purpose of such processing in the FRF is to gauge the patterns of data flow during normal operations, so that SPEAR is then equipped to recognise contrasting (anomalous) patterns potentially indicative of a cyberattack. The relevant operational data includes measurements captured by sensors in the plant environment, capturing matters such as water-levels in the basin, steam-pressure in turbines, etc. In addition, staff working at the hydro power plant will use the 'Blynk' IoT app for data visualization on their mobile. As noted, in section 2, this app works through a centralized server that provides the communication between the operator's mobile and the Smart grid's device.

As regards the question of which of the above data constitutes personal data under EU data protection law, the starting point is Article 4(1) of the GDPR, which defines this as: "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*." As discussed in Deliverable D2.1, this is a broad definition, which looks at the potential of data – even that which at first sight appears quite disconnected from an individual natural person – to be associated, including by combining it with other available data, with a person and allow the holder of the data to single out and make inferences about the activities of the relevant person.

This question will turn on the specific context in which the data is collected, and what possibilities are open to the collector/holder ('data controller') to link it together with other data so as to identify the data subject. Hence, in Use Case 1, in relation to operational data collected from a sensor (equipped with an IP and a MAC address) that measures water-levels in one of the plant basins and transmits this data through the plant's IT network, this, at first sight, admittedly does not look much like personal data. However, suppose that the sensor only connects to the network when switched on by a particular employee at the plant; here the data collected from the sensor – in particular, the metadata showing the times at which it transmits – may allow inferences about the relevant employee's work patterns, and in such case could qualify as personal data in accordance with the GDPR definition.

Similarly, as regards the ‘Blynk app’ data, it is probable this would qualify as the personal data of relevant employees who are provided with the app: the traffic data that show the communication patterns between the mobile and the hydro-plant network, recording the employee’s use of the app again allow inferences about their behaviour. Moreover, the fact that SPEAR only collects the IP address of the mobile device, and does not associate it with the name of the employee whose mobile it is, will not alter the position. As noted in Deliverable D2.1, it is sufficient (according to the 2016 CJEU decision in *Patrick Breyer v Bundesrepublik Deutschland* (Case C-582/14)) that a lawful channel, linking the address and the name, is available elsewhere (in the hands of the relevant internet service provider of the IP address.

In Use Cases 2 and 3, the Substation scenario, and Combined IAN and HAN scenario, the majority of the forensic data collected by SPEAR also takes the form of operational data, which record data flows (using different communication protocols between the various hardware devices that are connected to the internal substation network. As in Use Case 1, the purpose of processing this data is to familiarize the FRF with ordinary flow patterns of the relevant networks (under conditions of normal functioning). As analysed for Use Case 1, this data, recording technical-physical processes in the environment will not ordinarily qualify as personal data under the GDPR. This would only be so if the context permits concrete inferences from the patterns of flow from given hardware devices to the characteristics or behaviour of specific natural persons (typically the staff who maintain or operate the devices). In addition, in Use Case 2, network data recording remote connections by staff will be captured; including the credentials and authentication steps by the employee to log into the network.

Moreover, in Use Case 3, the network contains smart meters that retain data from various Intelligent Electronic Devices (IEDs) placed at offices and non-industrial environments. In these cases, the data collected by SPEAR will be personal data (as before, the question whether the project itself can or wishes to associate a given IP address or user credential with a particular named person is not material. It is enough that a lawful link between such data and the given person exists elsewhere (in the hands of the substation manager or smart meter provider, respectively).

Turning to Use Case 4, the Smart Home scenario, here while some of the data collected appears to be operational network data of a non-personal nature, other forms of data are implicated that have the clear potential to be personal data. This encompasses all data that, by revealing the patterns of energy consumption in the home, make it possible to profile the activity of its occupants. Examples include the MQTT messaging protocol for communication of sensor gateways and local servers with the Smart-Home central server (which relay sensor measurements of movement in the home, as well as the HVAC measurements communicated over the OPC BACnet.

In addition, as described in section 2.5, each of the above Use Case scenarios will deploy honeypots as a cyber-attack research tool, which capture data relating to the IP Address from which the attack was generated, and the commands or actions attempted to be performed by the attackers. In Deliverable D2.1, the ethical aspects of using honeypots as a research tool were addressed, and ethical recommendations derived. In relation to the data protection law aspects, the IP address of a personal computer will qualify in principle as personal data (following the decision in the *Breyer* case referred to above). However, in the case of attacks captured by honeypots, the IP addresses usually do not relate to personal equipment, as the attacker is likely to shield his/her identity by utilizing a public IP Address (e.g. public Wi-Fi networks, networks of public Libraries, etc.) or operating via anonymised networks such as Tor. Moreover, insofar as private computers are used, these may be co-opted without their owners’ knowledge or consent, as with the armies of ‘zombie’ computers typically deployed in DDoS attacks.

In such cases, it is doubtful that the relevant IP addresses qualify as personal data. Even so, it cannot be excluded that in other cases the IP addresses captured do represent personal data, e.g. in respect of novice attackers, who naively launch an attack from their own computer without using screening technologies. Insofar as the partners that process the honeypot data for the SPEAR FRF are not able to distinguish those addresses from the rest (and treat them differently), they should proceed generally on the (cautious) basis that the rules of the GDPR will apply to all private IP addresses in the honeypot [70].

Following the analysis of data protection rules presented in Deliverable D2.1 – it is next germane to clarify the roles of the key actors involved (be reference to the legal definitions found in the GDPR). First, as regards the relevant data subject(s), according to Article 4(1), these are the "identified or identifiable natural person(s)" (to whom the data relates. In Use Cases 1-3, it is apparent that these will be staff employees at the respective facilities (hydro-plant, substation) of the SPEAR end user partners. In relation to Use Case 4, they will be the occupants of the Smart Home, who during the development phase of the project will putatively be staff members of partner CERTH. And in the case of the honeypot data, these will be the cyber-attackers (assuming, as discussed above, that the attacker used his own computer in the attack).

As regards the role of 'data controller', this is defined in Article 4(7) GDPR, as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". As is apparent, this allows for multiple controllers, operating as 'joint controllers' in the framework of data processing for a common purpose. In the context of SPEAR, these will in the first place be the technical partners that collect and process the data for the project purposes. However, given their role in facilitating and permitting the data collection from their networks, the relevant end user partners will also qualify as data controllers in relation to the project. Here, as suggested by the CJEU's 2018 'Facebook Fan-page' decision [72], it does not matter whether or not a project partner that facilitates the collection of personal data by another partner will itself use that data.

Having established that in some cases personal data will be gathered in the Use Cases for the SPEAR FRF, and the identity of the putative data subjects and controllers, the following sections address the key points that the project should have regard to in order to ensure compliance with the GDPR rules. As noted, the EU data protection framework was examined in Deliverable D2.1, and a number of privacy requirements were derived for the project to adhere to. The present discussion applies this to the context of the forensic data used in the SPEAR FRF and focuses on matters specifically relevant there:

4.2.1 Lawful Processing Basis

The data controller needs to point to a lawful basis for processing personal data. As presented in Deliverable D2.1, Article 6 of the GDPR provides a list of potential lawful bases of which the most pertinent, in the context of developing the SPEAR FRF during the Project lifetime are: (a) the data subject's specific consent; and (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of the data subject. Subsequently, as noted earlier, where the SPEAR framework is deployed by end-users (in the project exploitation phase) beyond the research context, so as to enhance their cybersecurity, such users – where bound by the NIS Directive as providers of critical infrastructure - would also point to the need to process the data to comply with a legal obligation (per Article 6 (c) of the GDPR).

For Use Case 4, the explicit consent of the Smart Home occupants (CERTH employees) will be obtained in line with the consent form developed in Deliverable D9.1. In respect of the data from the other Use Cases, where it is less clear in advance if personal data will be concerned, it is suggested that – insofar as it is – then the legitimate interests ground under Article 6(f) provides a sound alternative basis [71]. Indeed, in the case of cyber-attacker data captured in the honeypots, it is difficult to see how any other basis could apply. In fact the GDPR, in Recital 49, reinforces the general suitability of the legitimate interest ground to be used in the context of cybersecurity initiatives, as follows:

> "(49) *The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate*

> *interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems*."

Importantly, where the data controller relies on its legitimate interests to process data, this should be subject to a balancing test by the controller to ensure any conflicting interests of the data subject are properly addressed. As the Article 29 Working Party noted in its 2014 Opinion on the notion of legitimate interests [844/14/EN WP 217], the data controller should consider the use of additional safeguards to minimize risks to the subject and ensure the balance remains in favour of processing. In this regard the Working Party mentions in particular the use of encryption and pseudonymisation as important techniques, and the intention with the SPEAR FRF is that these will indeed be utilized as far as possible.

4.2.2 Fair processing safeguards

As discussed in Deliverable D2.1, there are also a number of principles of fair processing, set out in Article 5 of the GDPR, with which the data controller needs to comply. A key underlying aim is to secure that, where the controller does have a lawful ground for processing, as little personal data as possible is nevertheless processed, consistent with achieving the controller's purposes. This idea is expressed especially via the principles of purpose limitation (Art 5(1)(b) - according to which personal data should be used strictly for the purpose for which it was collected); data-minimization (Art 5(1)(c) - the minimum amount of personal data needed to fulfil the purpose should be collected/processed; and storage limitation (Art 5(1)(f) - once no longer needed, any personal data should either be deleted or anonymized).

In the context of the SPEAR data collected from Use Cases 1-4 for the purpose of developing the FRF, this means the partners that collect the data should not disclose this to other project partners (and a fortiori not outside the project), unless the other partner also has a clear need for the data to fulfil a designated project task. It means too, in respect of specific IP addresses collected (associated with a given technical device, which may allow inferences about persons 'behind' the device), that the collecting partner should review how long those addresses are needed in order to fulfil the project tasks. If, e.g. it is possible to rely on the overall network patterns alone (not involving further use of the real addresses), then these should be discarded and replaced by a random code for the device. Optimally there should then be no means to re-link this new code to the old IP address (anonymization): here, the data would no longer be personal data under the GDPR. However, as a 'second best' approach, such a link could be retained, if justified by the underlying research purpose (e.g. in a project, it may be important to leave open the possibility of re-checking results; or perhaps the identity of a specific device in the overall network is germane for understanding a security threat). In such cases, the method of secure pseudonymisation may be applied, where a file is kept that links the original device address to the random code, but the file is stored securely elsewhere and only made available to authorized persons in pre-defined circumstances.

The GDPR for its part consistently encourages the use of pseudonymisation as a data protection safeguard, which it defines in Article 4(5) as: "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*". As is implicit in this definition, pseudonymized data (unlike the case of anonymized data – where no link is kept) remains personal data, and hence in processing it, the controller will remain subject to the other requirements of the GDPR.

Two further fair processing principles in Article 5 of the GDPR, which are particularly pertinent in the context of forensic data processing, are those of data accuracy (Art 5(1)(d), and confidentiality and integrity (Art 5(1)(f). According to the former, the data controller shall use every reasonable step to ensure that personal data is both accurate and up-to-date; the latter means that appropriate steps must also be taken to safeguard the data from unauthorized access and/or manipulation/tampering. As will be apparent, these principles are in tune with the positive aspects of collecting and preserving reliable digital forensic evidence, as discussed in Section 4.1. Accordingly, their satisfaction will in any event be a high priority for SPEAR and not pose any additional concerns. The safeguarding of data confidentiality is also closely bound up with the issue of safeguarding data subject interests, looked at in relation to the data controller's legitimate interest ground for processing. The technical security safeguards that should be utilized are spelt out in more (albeit consciously technology-neutral) detail under Article 32 of the GDPR, which states:

> "*Taking 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 controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymisation and encryption of personal data;*
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
> (d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*."

4.2.3 Further relevant GDPR compliance requirements

In addition to the above requirements on data controllers to ensure that processing has a lawful basis and occurs in accordance with the fair processing principles, there are further responsibilities in the GDPR, especially in the context of higher risk processing operations (i.e. ones where fundamental interests of the data subjects may be affected) in terms of demonstrating accountability and transparency. This includes the need under Article 30 to maintain a thorough record of all processing activities, including names and contact details of the controller (and where applicable), the joint controller; the purpose of processing, the categories of data processed, and the categories of recipients to whom the data is disclosed. This provision aims at enhancing the transparency and accountability of processing (under Article 5(2)), but also the achievement of data integrity in a positive sense (i.e. the ability to trace the operations performed on the data so as to check that it remains accurate and untampered with). In the context of the SPEAR FRF, the full logging of processing operations will be ensured, also as a positive requirement (discussed in section 4.1) to ensure that the evidence delivered by the framework is properly reliable and authentic

Also significant here is the need, under Article 35 (1) of the GDPR to carry out a data protection impact assessment (DPIA) where data processing is likely to result in a high risk to the rights and freedoms of natural persons. As discussed in Deliverable D2.1 a DPIA is required inter alia where data processing involves a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, or there is systematic monitoring of a publicly accessible area on a large scale (art.35 (3)). Where the outcome of the DPIA suggests that there are high residual risks to data subject interests, even after the controller has utilized risk mitigation strategies, the controller should then consult with its data protection authority under Article 36 GDPR prior to commencing any processing. As discussed in Section 3.2.3, the supervisory authorities in different EU member states have competence to produce rules of procedure in their own territories, which may differ, and further concretise the processing operations for which they expect a DPIA to be performed and the form it may take.

In SPEAR it is planned that a data protection impact assessment shall be carried out within Work package 4 as the work develops, and (as DPIA is not a once-for-all procedure but should be re-performed as the data processing context updates) the situation as regards risks posed by the system to data subject interests regularly reviewed. This will take account of the concrete implications of forensic data use (where personal data is at issue) for subject interests as these crystalize as the use cases mature. An aspect of the assessment will be to consider appropriate arrangements for enabling the exercise of data subject rights (under Chapter III of the GDPR) if applicable. This approach, as well as the following the privacy requirements from Deliverable D2.1, should contribute to the development by the partners of a legally and ethically sound cyber-security system that is readily implementable by end-users (in the project exploitation phase) in conformity with the rules of the GDPR.

5. Conclusions

This deliverable has described the results of the analysis of the forensics investigation law and regulatory frameworks for defining the forensics strategies in SPEAR project. The analysis was focused on the challenges as well as laws, guidelines and standards relevant for the development of the SPEAR Forensic Readiness Framework (FRF), which will provide technical solution and assistance in the field of forensic readiness of smart grids.

As discussed, the FRF aims to offer solutions and forensic tools (including of a proactive nature, as with honeypots) that gather network-based evidence for cyber investigation, as well as provide insights as to how smart grids can be made forensics-ready. A key aspect relates to the collection and securing of network traffic data that may subsequently be useful for evidential purposes, which, as discussed raises two main forms of legal compliance issues. The first is the need for the data to meet generally acceptable standards of evidential reliability and cogency (so as to be usable in subsequent criminal investigation and possible judicial proceedings); the second concerns the need for processing of such data, where it qualifies as personal data, to satisfy the requirements of applicable data protection law.

In considering these matters, the analysis has proceeded in three main parts. In the first of these (in Chapter 2), there was a detailed presentation of the four SPEAR Use Cases and the nature of the forensic data that will be gathered in each. In the second part, Chapter 3 offered a survey at a generic level of the key legal instruments and good practice guidance (with a particular emphasis on those applicable in Europe) that relate to the appropriate handling of digital forensic data. In Chapter 4, these strands of analysis were then combined, in deriving and discussing the key implications of the laws and standards for the data processing in the SPEAR FRF. In this way, the report aims to provide an ongoing template and point of reference for forensic data handling and management strategies in SPEAR.

References

[1] I. Kotsiuba, "Blockchain Evolution: from Bitcoin to Forensic in Smart Grids," in *IEEE Big Data 2018 - The 2nd International Workshop on Big Data Analytic for Cyber Crime Investigation and Prevention*, Seattle, 2018.

[2] P. Roberts, "The Forensic Challenge," *Frontiers L. China ,* vol. 13, no. 1, pp. 43-66, 2018.

[3] D. Sule, "Importance of Forensic Readiness," *ISACA Journal,* vol. 1, 2014.

[4] A. Iqbal, M. Ekstedt and H. Alobaidli, "Digital Forensic Readiness in Critical Infrastructures: A Case of Substation Automation in the Power Sector," in *International Conference on Digital Forensics and Cyber Crime*, 2017.

[5] ISO/IEC, *27037:2012.*

[6] M. Biasiotti, J. Mifsud Bonnici, J. Cannataci and F. Turchi, Eds., Handling and Exchanging Electronic Evidence Across Europe, Switzerland: Springer, 2018.

[7] ISACA, Overview of Digital Forensics, 2015.

[8] ENISA, Introduction to Network Forensics (Final version 1), January 2019.

[9] ENISA, Forensic analysis Network Incident Response Handbook, Document for Teachers, ENISA, 2016.

[10] Council of Europe, Electronic Evidence Guide A Basic Guide for Police Officers, Prosecutors and Judges (version 2.0), CoE, 2014.

[11] SWGDE, SWGDE Best Practices for Digital Evidence Collection (Version: 1.0), July 2018.

[12] NIST, Guide to Integrating Forensic Techniques into Incident Response, NIST, 2006.

[13] N. Duncan and T. Hutchinson, "Defining and Describing What We Do: Doctrinal Legal Research," *Deakin Law Review,* vol. 17, no. 1, p. 101, 2017.

[14] *Inter alia according to the terms of the NIS Directive, insofar as applicable to the relevant SPEAR user.*

[15] Modbus TCP/IP protocol specification. Available at: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[16] Profinet security guideline. Available at: https://us.profinet.com/documentation/profinet-security-guideline/

[17] Blynk IoT platform. Available at: https://blynk.io/

[18] IEC 61850:2019, Communication networks and systems for power utility automation. Available at: https://webstore.iec.ch/publication/6028

[19] IEC 62351, Power systems management and associated information exchange - Data and communications security. Available at: https://webstore.iec.ch/publication/6912

[20] T104 protocol profile. Available: https://www.schneider-electric.com/en/download/document/PACiS_T10x/.

[21] Network Time Protocol (NTP). Available: http://www.ntp.org/ .

[22] Authentication Options of NTP. Available: http://doc.ntp.org/4.1.0/authopt.htm .

[23] RFC 4253: The Secure Shell (SSH) Transport Layer Protocol. Available: https://tools.ietf.org/html/rfc4253.

[24] The Syslog Protocol. Available: https://tools.ietf.org/html/rfc5424 .

[25] Remote Authentication Dial In User Service (RADIUS). Available: https://tools.ietf.org/html/rfc2865 .

[26] Transport Layer Security (TLS) Encryption for RADIUS. Available: https://tools.ietf.org/html/rfc6614 .

[27] Server Message Block (SMB). Available: https://www.samba.org/cifs/docs/what-is-smb.html .

[28] Unitronics Communication with the Vision™ PLC. Available: https://unitronicsplc.com/Download/SoftwareUtilities/Unitronics%20PCOM%20Protocol.pdf .

[29] BACnet™ - A Data Communication Protocol for Building Automation and Control Networks. Available: https://www.bacnetinternational.org/page/BACnetStandard .

[30] Article 1 of the Cybercrime Convention defines computer system as any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

[31] R. Montasari and R. Hill, "Next-Generation Digital Forensics: Challenges and Future Paradigms," in *IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 2019.

[32] A. Phillips, *An Investigation of Digital Forensic Concepts in an International Environment: The U.S., South Africa, and Namibia,* (A Dissertation Presented to the Faculty of the University of Alaska Fairbanks).

[33] H. L. Ho, "The Legal Concept of Evidence," Stanford Encyclopedia of Philosophy, 2015.

[34] ENISA, "Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary," ENISA, 2018.

[35] I. Walden, " Forensic Investigations in Cyberspace for Civil Proceedings," *Int'l Rev. L. Computers & Tech,* vol. 18, p. 257, 2004.

[36] *Coca-Cola v. BT plc,* [1999] FSR 518.

[37] *Totalise plc v. Motley Fool and Interactive Investor,* (2001) 4 EMLR 750.

[38] J. Meese, "The Use of Illegally Obtained Evidence in Belgium," *Digital Evidence and Electronic Signature Law Review,* vol. 10, 2013.

[39] *Court of Justice of European Union, Judgment of 8 April 2014 (Digital Rights Ireland, Joined Cases C-293/12 and C-594/12)*.

[40] See the Regulation of Investigatory Powers Act 2000, s 1(2); s 6.

[42] *See the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, SI No. 2699.*

[42] I. Walden and A. Flanagan, " Honeypots: A Sticky Legal Landscape," *Rutgers Computer & Tech. L.J. 317.* , vol. 29, p. 317, 2003.

[43] ERA, "Electronic Evidence Best Practice Guide." Available: http://www.era-comm.eu/life_cycle_of_the_e_evidence_in_criminal_proceedings/e_tool/story_html5.html.

[44] *Note that in the area of international commercial arbitration, the UN Model Law on International Commercial Arbitration provides some rules on evidence for such arbitration. See the UNCITRAL Model Law on International Commercial Arbitration 1985 with amen.*

[45] ECHR, Art 8(2).

[46] T. Pöysti, *Judgment in the Case of K.U. V Finland: The European Court of Human Rights Requires Access to Communications Data to Identify the Sender to Enable Effective Criminal Prosecution in Serious Violations of Private Life.*

[47] Council of Europe, "Modernisation of the Data Protection “Convention 108". Available: https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet.

[48] N. Forgó, C. Hawellek, F. Knoke and J. Stocklas, "Privacy Protection in Exchanging Electronic Evidence in Europe," in M. Biasiotti et al (eds) *Handling and Exchanging Electronic Evidence Across Europe*, Springer, 2018.

[49] Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings, (Adopted by the Committee of Ministers on 30 January 2019), 2019.

[50] Euopean Commission, "E-evidence - cross-border access to electronic evidence." Available: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

[51] *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detectio.*

[52] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).*

[53] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal,* 2018 COM(2018) 225 final.

[54] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73..*

[55] S. Mason, Electronic evidence Disclosure, Discovery & Admissibility: LexisNexis Butterworths, 2007.

[56] F. Insa, "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study," *J. of Digital Forensic Practice ,* vol. 4, p. 285, 2007.

[57] M. Kusak, "Mutual admissibility of evidence and the European investigation order: aspirations lost in reality," *ERA Forum,* vol. 19, no. 3, 2019.

[58] *State Gazette, edition 47 of June 13, 2017; in force since June 13, 2017.*

[59] A. Tsvetkova, "Electronic evidence in Bulgaria – one step further, one step back," *Digital Evidence and Electronic Signature Law Review,* vol. 15, 2018.

[60] Signaturit (blog), "Electronic evidence and its admissibility in court," 2017. [Online]. Available: https://blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court.

[61] P. Bazin, "An Outline of the French law on Digital Evidence," *Digital Evidence and Electronic Signature Law Review,* vol. 5, p. 179, 2008.

62 A. Kaissis, ‘Exclusion of Illegally Obtained Evidence in Greek Civil and Penal Proceeding – An Outline’. Available: http://www.digestaonline.gr/pdfs/Digesta%202015/kaissis.pdf

[63] M. Barel, *Honeypot, un “pot pourri” juridique,* Presentation, SSTIC Symposium, 2004.

[64] https://www.cnil.fr/.

[65] ENISA, *Digital forensics Toolset, Document for students,* September 2013.

[66] S. Davidoff and J. Ham, Network Forensics, Pearson Education, Inc, 2012.

[67] OLAF, *Guidelines on Digital Forensic Procedures for OLAF Staff,* 15 February 2016.

[68] *Regulation (EU, EURATOM) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament.*

[69] H. Jahankhani, et al., Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger, Switzerland: Springer, 2019.

[70] P. Sokol, J. Misek and M. Husak, "Honeypots and honeynets: issues of privacy," *EURASIP J. on Info. Security,* vol. 4, 2017.

[71] A. Cormack, "Incident Response: Protecting Individual Rights under the General Data Protection Regulation," *SCRIPTed,* vol. 13, no. 3, 2016.

[72] Court of Justice of European Union, Judgment of 5 June 2018 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein C-210/16).