Chapter 10

Integrated Cyber-Physical Security Approach for Healthcare Sector

By Fabrizio Bertone, Francesco Lubrano, Marco Gavelli, Olivier Terzo, Elisabetta Biasin, Erik Kamenjasevic, Samantha Dauguet-Demailly, David Lancelin, Silvia Andernello, Francesco Tresso, Luca Viarengo and George Suciu

DOI: 10.1561/9781680836875.ch10

Published in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures* by John Soldatos, James Philpot and Gabriele Giunta (eds.). 2020. ISBN 978-1-68083-686-8. E-ISBN 978-1-68083-687-5.

Suggested citation: Fabrizio Bertone *et al.* 2020. "Integrated Cyber-physical Security Approach for Healthcare Sector" in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Edited by John Soldatos, James Philpot and Gabriele Giunta. pp. 179–192. Now Publishers. DOI: 10.1561/9781680836875.ch10.

now
the essence of knowledge

10.1 Introduction

Modern societies are strongly dependent on the continuous function of Critical Infrastructures (CI) that ensure the supply of crucial goods and services such as power, Information and Communication Technologies, or drinking water. Critical Infrastructures are essential for the maintenance of vital societal functions, such as health, safety, security, economic or social well-being of people, etcetera. These aspects are also relevant with regard to the healthcare sector, where any interruption, damage, or unavailability of healthcare services may provoke economic and non-economic damages for individuals, organizations, States, and society as a whole.

The healthcare sector is among the most critical sectors in Critical Infrastructure Protection (CIP). Healthcare services considered "critical" are, for instance, emergency healthcare; hospital care (inpatient & outpatient); the supply of pharmaceuticals, vaccines, blood, medical supplies; and infection/epidemic control,

to name but a few. The disruption of one of these critical healthcare services could imply several damages for society. This happened, for instance, after the Wannacry ransomware attack on the National Healthcare Services (NHS), in the UK (Ghafur *et al.*, 2010). According to NHS England, the ransomware affected at least 80 out of 236 trusts across England, because they were infected by the ransomware or turned off their devices or systems as a precaution. Furthermore, 603 primary care and other NHS organizations were infected, including 595 GP practices. Thousands of appointments and operations were cancelled, and in five areas, patients had to travel further to reach accident and emergency departments.

Having recognized the increasing role of CIP, the EU legislator and majority of the EU Member States have adopted national strategies to increase the level of protection of critical infrastructures in the EU. Concerning CIP, in the last few years, many of the Member States adopted national CIP strategies and consider healthcare as one of the sectors requiring protection.

Nevertheless, to protect Critical Infrastructures such as a hospital is a huge and very complex task that requires particular attention and knowledge of defense and prevention strategies, as well as of vulnerabilities and potential attacks that may occur.

Critical Infrastructures such as hospitals are constantly threatened by different kinds of potential attackers with different resources available. Some could be simply motivated by visibility. Others could be driven by profit gain (Sultan *et al.*, 2018; Tonutti, 2016). The last few decades have also seen an increase of state-sponsored attacks, which can be motivated by espionage, retaliation, intimidation or as a stealth way to create disruption in case of escalating conflicts (Geers *et al.*, 2013).

Dangerous threats are also presented by increasing terrorist activities in recent years. While, traditionally, terrorist attacks have mostly targeted the physical world, cyberattacks are getting more and more popular, for financing purposes, to collect intelligence information or to cause disruption. When expertise is not available internally, other people can be persuaded to do the job without knowing the real objective (Mitnick and Simon, 2010).

Nowadays, physical and cyber systems are more and more interconnected, in some cases being so integrated to be indivisible. From a security point of view, this greatly enhances the attack surface and the possibility for remote actors to reach their goals. Moreover, physical intrusions are still possible and currently used by criminals.

Let us consider the motivation for a generic attacker to access confidential information stored in local servers inside a hospital. This could be achieved by various means and exploiting different levels of physical and cyber intrusions.

A more "traditional" attack would be to enter the hospital's premises and collect the desired information manually. An evolved remote attacker would rather look

for a chain of vulnerabilities in the "cyber" services exposed by the hospital and get the data from a completely different country. In the middle, there are many different mixes of physical and cyber steps that can allow the accomplishment of the same goal. Social engineering techniques could be used to trick hospital staff in order to gain access to the systems (Medlin *et al.*, 2008). Alternatively, a USB drive infected with malware could be given as a gift to a doctor during a conference (De Falco, 2012; Cluley, 2010).

It is therefore clear that physical and cyber threats should be considered, analyzed, and treated together, as cyber-physical threats. An integrated approach that considers both physical and cyber worlds is therefore required.

This chapter presents the description of threats, potential incidents, and issues regarding the protection of the critical infrastructures like hospitals, and it presents the first results of the SAFECARE project, describing the internal architecture of the whole system.

10.2 Safecare Approach

The idea behind the SAFECARE project is to respond to the growing demand for an integrated cyber-physical security solution for Critical Infrastructures, in particular hospitals. The challenge is to bring together the most advanced technologies from the physical and cyber security spheres, to achieve a global optimum for systemic security and for the management of combined cyber and physical threats and incidents, their interconnections and potential cascading effects. Indeed, the main objective of the SAFECARE project is to increase the protection and resilience of Healthcare facilities and services, allowing for a better response in case of emergencies. This is done using a holistic approach that considers the physical and cyber worlds in a single integrated system.

In addition, innovative services enable first responders and other relevant actors to get real-time updated information about the availability of healthcare services. This is useful both in case of incidents inside the facility itself, so that the information about unavailable services is easily accessible, and in case of large-scale emergencies such as earthquakes that can require the involvement of many facilities and an efficient routing of patients.

Within the SAFECARE project, a global architecture schema that includes all the physical, cyber, and cyber-physical module has been designed. This architecture can be broken down into 3 parts, as shown in Figure 10.1:

- Physical security solutions
- Cybersecurity solutions
- Integrated cyber-physical security solutions

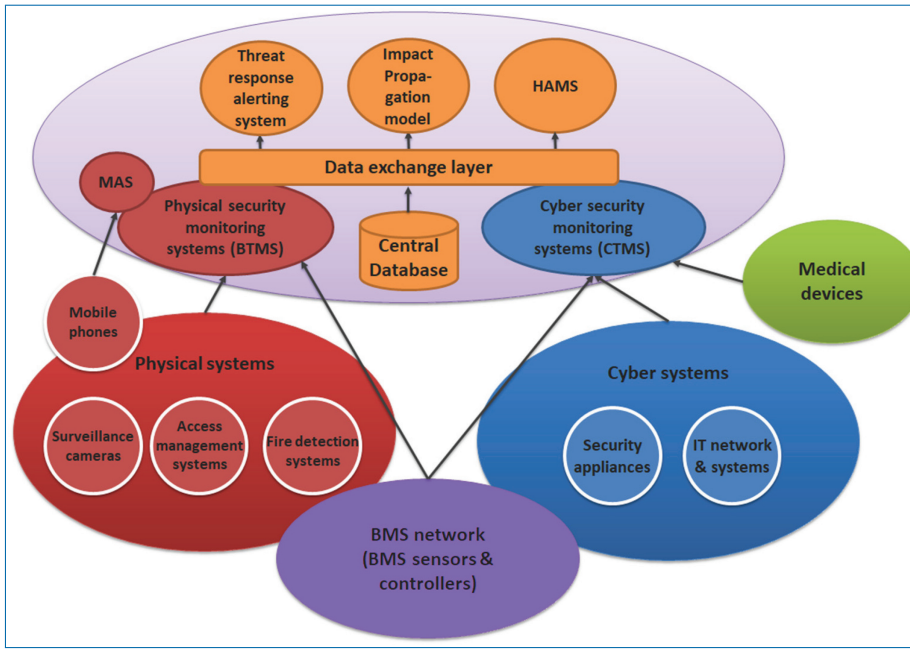

Figure 10.1. SAFECARE global architecture.

The physical and cybersecurity solutions consist of smart modules and efficient integrated technologies to, respectively, improve physical security and cybersecurity.

More specifically, physical security solutions embed integrated intelligent video monitoring and interconnect building monitoring systems as well as management systems. Meanwhile, cybersecurity solutions consist of cyber monitoring systems as well as threat detection systems related to Information Technology (IT), Building Management Systems (BMS), and e-health systems.

Both physical and cybersecurity monitoring tools are interconnected thanks to the integrated cyber-physical security solutions. They consist of intelligent modules whose role is to integrate different data sources and better take into account the combination of physical and cybersecurity threats.

In order to fulfill their role, each solution ensemble is composed of several dedicated systems.

The physical security solutions rely on:

- The Suspicious Behavior Detection System;
- The Intrusion and Fire Detection System;
- The Data Collection System;
- The Mobile Alerting System;
- The Building Threat Monitoring System.

The Building Threat Monitoring System (BTMS) is the aggregation point for physical security and makes the link between physical systems and the rest of the architecture. The Mobile Alerting System (MAS) is intended for local security operators, providing them with a quick way to report physical security events and visualize contextual information.

The cybersecurity solutions rely on:

- The IT Threat Detection System;
- The BMS Threat Detection System;
- The Advanced File Analysis System;
- The E-health Devices Security Analytics;
- The Cyber Threat Monitoring System.

Just like the BTMS, the Cyber Threat Monitoring System (CTMS) connects the cyber systems to the rest of the architecture and is the central point for cybersecurity.

Finally, the integrated cyber-physical security solutions rely on:

- The Data eXchange Layer;
- The Impact Propagation and Decision Support Model;
- The Threat Response and Alert System;
- The Hospital Availability Management System;
- The E-health Security Risk Management Model.

The Data eXchange Layer (DXL) enables communication between all of the SAFECARE subsystems. It works in pairs with the central database which stores static and dynamic data characterizing the whole system. The Impact Propagation and Decision Support Model (IPDSM), the Threat Response and Alert System (TRAS), along with the Hospital Availability Management System (HAMS) are three decision-making modules. They respectively enable inferring cascading impacts of physical and/or cybersecurity incidents, alerting internal and external practitioners (or any other appropriate defined response) upon reception of an "impact" message from the IPDSM, and providing information about health services availability.

10.2.1 Intercommunication Layer and Central Database

In order to cope with such a combined approach for the management of cyber and physical security, the SAFECARE project implements a central database and a common data exchange layer to connect the different modules of the SAFECARE platform.

Dentral Database

The SAFECARE Central Database is a single, unique repository that stores multiple types of data needed for the other modules in the platform. In particular, two different categories of data have been identified and modeled in the database:

- Static data, all the information related to assets, facilities, buildings, and services inside the hospital. Furthermore, this category includes interconnections and relations among the assets.
- Dynamic data, all the information that is generated by SAFECARE modules, such as incidents, impacts, and all the other responses/messages. Relations among incidents, impacts, etc. are also represented in the database and can be used for further analysis.

Data eXchange Layer

The Data eXchange Layer constitutes the core of the communication layer in the SAFECARE architecture. It allows all the other modules to communicate with each other in near real time and provides relevant interfaces to extract data stored in the database. Five types of dynamic-data messages are defined:

- Incident: message generated by the monitoring tools; it reports information related to the incident, it is validated by human operators, and it triggers decision-making modules.
- Impact: reports the potential impacts after an incident occurs allowing prevention of potential cascading effects.
- Threat response: provides a predefined reaction plan to mitigate the effects of incidents and improve time to response.
- Notification: exchange the communication between Threat Response and Alerting System and Mobile Alerting System.
- Availability: reports the updated availability of assets involved in the incident.

10.2.2 Cyber and Physical Security Solutions

In order to detect possible incidents, some monitoring systems are required. This section describes the set of tools that are integrated in SAFECARE for this kind of job, logically subdivided between physical and cybersecurity.

Building Threat Monitoring System

The Building Threat Monitoring System is the module in charge of monitoring the physical assets. BTMS is an event-based server that tracks physical events coming from different subsystems, such as: the Suspicious Behavior Detection System, that

analyzes the video surveillance detecting irregular movements or behavior such as loitering or tailgating; the Intrusion and Fire Detection System, that is connected to the access control system and to the fire alarm system of the hospital; the Data Collection System, that collects data from many different type of sensors and controllers; and the Mobile Alerting System. The BTMS is the central point for communicating physical incidents, which are alerts that have been judged to require a security response by operators in charge.

Finally, the BTMS is also responsible for receiving and relaying the incident handling responses elaborated by the Impact Propagation and Decision Support Model.

Mobile Alerting System

Smartphones and tablets are powerful network-connected devices, constantly available and low cost; therefore, they are perfect tools for widespread use by human operators.

Through the MAS, coupled with the mobile app specifically developed in SAFECARE, a building security officer via a smartphone has the ability to quickly report specific categories of security threats or alerts (system failure, natural hazard, terrorist attack, etc.), as depicted in Figure 10.2(left). On the other side, automatic alerts generated by detection systems can be validated or cancelled by the operator as can be seen in Figure 10.2(right), where a false fire alarm is shown.

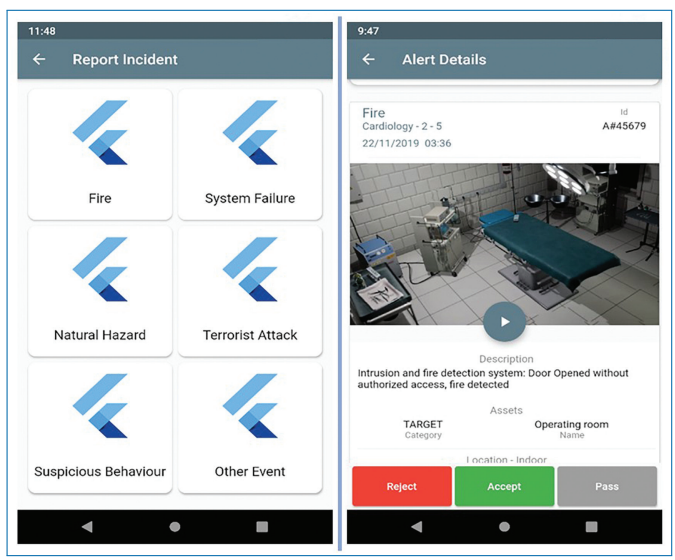

Figure 10.2. Incident reporting (left) and alert validation (right).

Cyber Threat Monitoring System

The objective of the Cyber Threat Monitoring System is to collect and centralize security events from the cyber threat detection systems, organize the information, and provide user-friendly interfaces to SOC[1] operators so that they can visualize the threats and have an overview of the potentially impacted assets.

The CTMS receives security events from the following systems: the IT Threat Detection System (ITDS) that monitors the IT network and receives log messages from the different components in order to detect threats targeting the IT infrastructures; the BMS Threat Detection System (BMSTDS) that analyzes the Operational Technologies (OT) protocols used in building automation systems (such as SCADA systems and PLC controllers); the advanced file analysis system that performs in-depth analysis of files extracted by the ITDS or the BMSTDS, thus allowing malware detection; the e-health devices security analytics that monitors medical devices by collecting their log messages and rely on an e-health security risk management model to identify any related risk.

Rules are implemented within the CTMS to automatically generate alerts from the received security events. The CTMS is the entry point for SOC operators to monitor in real time all incoming alerts regarding cyber threats as it centralizes them. After a first analysis phase, the SOC operators must confirm the alerts as either incidents or false-positive alerts. From there, the CTMS enables tracking of incidents and coordination of incident responses.

Finally, the CTMS receives potential impacts, which are computed from both physical and cyber incidents by the Impact Propagation and Decision Support Model, in order to provide SOC operators with a clear understanding of potential impacted assets and services.

10.2.3 Integrated Cyber-physical Security Solutions and Decision Support

This section provides a brief description of the SAFECARE subsystems that handle incidents that generate potential impact and cascading effects, alerting relevant recipients following predefined reaction plans and providing updated information related to the hospital status.

Impact Propagation and Decision Support Model

The ability to simulate the propagation of impacts caused by incidents and to mitigate risk is the cornerstone of the SAFECARE project. The module in

1. Security Operation Centre.

charge of these functionalities is the Impact Propagation and Decision Support Model.

The objectives of the IPDSM are:

- Combine physical and cyber incidents that occur on assets
- Infer cascading effects as impacts that could potentially affect the same or related assets
- Alert other modules about the potential impacts and severity.

In order to reason about incidents and their potential impacts, the IPDSM needs to know detailed information about physical and cyber assets and their relations. This information is collected in a custom ontology defined for the project. Following incidents, the IPDSM simulates a set of potential impacts on directly or indirectly involved assets. This is done by employing a set of rules derived by domain knowledge.

Threat Response and Alert System

The Threat Response and Alert System is a specific module devoted to alerting relevant recipients by providing information about incidents, potential impacts and sharing the predefined reaction plan, according to incident type and severity. It is activated by an "impact" message received from the IPDSM through the DXL. Once triggered, the module runs the corresponding predefined response plan and alerts internal and external practitioners via different media (SMS, emails, phone calls,…) and possibly also by using the MAS.

Hospital Availability Management System

The Hospital Availability Management System service aims to improve the resilience of health services and the communication of availability information among hospital staff and first responders. The HAMS is an integral part of the incident management process in SAFECARE. Based on incidents that are received from monitoring modules, it updates the availability of assets involved, considering the incident nature and the asset category. Once the impacts are reported, HAMS can examine them, updating the availability of assets that are involved (even indirectly) in the incident. Furthermore, HAMS provides a web interface with which users can check the status of the hospital and eventually manually update resources/availability status. Finally, HAMS provides an interface to export hospital status/information compliant with the EDXL-HAVE standard.[2]

2. http://docs.oasis-open.org/emergency/edxl-have/v2.0/edxl-have-v2.0.html

10.3 Ensuring Security, Privacy, and Data Protection within the EU Legal Requirements

Security and confidentiality are key factors when it comes to privacy and data protection. In that regard, healthcare infrastructures process on a daily basis personal health-related data of vulnerable individuals (i.e., patients), due to the nature of the services they provide. These kinds of activities are likely to result in a high risk, especially when they are performed on a large scale. If a healthcare infrastructure falls victim to an attack and a security incident occurs, appropriate steps should be taken. To do so, it is important to follow procedures determined by the relevant legal frameworks on incident reporting and notification.

The paragraphs that follow provide a brief overview of the applicable EU security, privacy, and data protection legal requirements that may be considered when dealing with reporting and notification of incidents.

10.3.1 Security of Networks and Information Systems

Network and information system security is a matter that has been regulated at European level in 2016 with the NIS Directive. This legislative instrument has provided a minimum set of rules ("harmonization") with the aim of achieving a common level of security resilience across the European Union. Every Member State has to transpose the Directive via national legislation. The NIS Directive requires entities providing services considered "essential" (i.e., "Operators of Essential Services" or "OES"—e.g., healthcare providers such as hospitals and private clinics) to ensure the security of their network and information systems and to adopt a risk-based approach.[3] OES must put in place technical and organizational measures appropriate to the risk posed to their networks and information systems. Among these, OES/healthcare providers should enact measures aimed at preventing, detecting, and handling incidents[4] and at mitigating their impact.

(Security) Incident: prevention, detection and notification under the NIS Directive

The NIS Directive has established the duty for operators to notify, without undue delay, to the competent authorities or Computer Security Incident Response Teams

3. See art. 5(2) NIS Directive for the definition and criteria of identification of OES, which have to be identified by the Member States.

4. Incidents are defined by the NIS Directive as "any event having an actual adverse effect on the security of network and information systems" (art. 4(1)(7)).

(CSIRTs) incidents having a significant impact[5] to the continuity of the essential services they provide. This requirement implies that OES/healthcare providers must set up measures to detect incidents as they have to be prepared to gather key information on incidents to be notified to the competent authorities. Furthermore, OES/healthcare providers should notify incidents *as soon as they can.* As cybersecurity incidents are dynamic and the situation can change rapidly, operators should first send an immediate alert notification to the national competent authority and/or CSIRTs in order to allow them, for instance, to offer support concerning the handling of the incidents or to assess the potential impact for essential services, individuals, society, economy, etc. An incident notification may happen via different means, such as a phone call, a plain email, a web service, an online paper. Procedures regarding modalities of incident reporting and the information that has to be provided (which may concern the nature of the incident, the impact of the incident, operational information such as time or status, etc.) may vary between Member States, as they must be determined by each MS individually.

10.3.2 Security of Personal Data

Integration of security architecture in hospital's infrastructure in order to prevent security incidents from happening entails the application of EU privacy and data protection laws (i.e., GDPR). Unlike the NIS Directive, the GDPR is directly applicable in all EU Member States. Healthcare organizations, healthcare professionals, and healthcare staff are bound by the requirements of the GDPR. The Regulation requires all persons and legal entities (e.g., healthcare providers) acting as controllers[6] to abide by the key principles of data protection laws and shall be responsible for and be able to demonstrate compliance with the law. With regard to security, the integrity and confidentiality principles require from the healthcare providers to process personal data securely. This shall include protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage; and it must imply the use of appropriate technical and organizational measures according to the risk inherent to the processing.

5. Parameters to determine the "significance" of the impact of an incident are listed under art. 14 NIS Directive, i.e.: (a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident. The NIS Coordination Group provided further guidance in this regard. See: Reference document on Incident Notification for Operators of Essential Services (February 2018); Guidelines on notification of Operators of Essential Services incidents (May 2018).

6. The 'controller' is "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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" (art 4(1)(7) GDPR).

Personal data breaches: prevention, detection and notification under the GDPR

The GDPR also requires healthcare infrastructures, when acting as controllers, to notify the supervisory authority in case a personal data breach[7] occurs. The concept of "personal data breach" is close to the NIS Directive concept of "incident" analyzed above. However, it differs significantly in scope: the former concerns personal data only, whereas the latter concerns any kind of security incidents. In other words, every personal data breach is a security incident, but not every security incident is necessarily a personal data breach.

As the Article 29 Data Protection Working Party puts it, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner. Personal data breaches must be notified to competent authorities without undue delay, and no later than 72 hours after becoming aware of it. The notification should describe the nature of the personal data breach including the categories and approximate number of data subjects concerned as well as the categories and approximate number of personal data records concerned. Data breaches must also be notified to data subjects when the breach is likely to result in a high risk for their rights and freedoms.

10.3.3 Relevance of the NIS and Privacy and Data Protection Requirements within the SAFECARE Framework

The solutions presented within the SAFECARE architecture are aimed at establishing monitoring mechanisms and internal incident detection mechanisms. By monitoring and preventing incidents, these solutions may thus represent a security measure with which healthcare providers may manage the risks posed to security of their network and information systems, including to the risk posed to the processing of patients' data concerning health. By doing so, healthcare providers may be facilitated in their process of compliance with prevention, detection, and notification requirements set by the NIS Directive and the GDPR.

10.4 Conclusions

The threats that target critical infrastructures, in particular the healthcare sector, are multiple and manifold. The actors that can act against critical infrastructure, their

7. A personal data beach consists in "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data" (art. 4(1)(12) GDPR).

motivations, and means of operating can also be varied and involve either physical and cyber assets, or a combination of them. These reasons explain the motivation behind the need for an integrated cyber-physical security solution.

The SAFECARE project conceived an integrated cyber-physical security approach and designed an architecture that combines together different monitoring and management tools, each considering a specific aspect of the global solution. Assets, vulnerabilities, threats, incidents, and impacts are all considered together with their dependencies, forming a shared intelligence that greatly enhances the value of each single piece of data. This approach allows us to extract much more information and uncover possible menaces previously unseen.

Finally, an important aspect to consider while implementing an organization's security plan is the compliance with relevant legislation. For this reason, security, privacy, and data protection requirements have been analyzed from a legal point of view, giving a brief overview of the relevant legislation concerning SAFECARE framework.

Acknowledgments

The SAFECARE project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no. 787002.

References

Cluley, G. (2010, May 21). *IBM distributes USB malware cocktail at AusCERT security conference*. Retrieved from Naked Security: https://nakedsecurity.sophos.com/2010/05/21/ibm-distributes-usb-malware-cocktail-auscert-security-conference/

De Falco, M. (2012). *Stuxnet Facts Report: A Technical and Strategic Analysis*. Tallin: NATO Cooperative Cyber Defense Centre of Excellence.

Geers, K., Kindlund, D., Moran, N., and Rachwald, R. (2013). *WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*. FireEye.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., and Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine*.

Medlin, B. D., Cazier, J. A., and Foulk, D. P. (2008). Analyzing the Vulnerability of U.S. Hospitals to Social Engineering Attacks: How Many of Your Employees Would Share Their Password? *International Journal of Information Security and Privacy (IJISP)*, 71–83.

Mitnick, K. D. and Simon, W. L. (2005). When Terrorists Come Calling. In K. D. Mitnick, and W. L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (pp. 23–47). John Wiley & Sons.

Sultan, H., Khalique, A., Tanweer, S., and Alam, S. I. (2018). A Survey on Ransomeware: Evolution, Growth, and Impact. *International Journal of Advanced Research in Computer Science*.

Tonutti, S. (2016, September 16). *Genetic Data Theft as a new type of Biocrime: legal and social aspects of genetic privacy*. Retrieved from Privacy Genetica: http://www.privacygenetica.it/2016/09/genetic-data-theft-as-a-new-type-of-biocrime-legal-and-social-aspects-of-genetic-privacy/