Cybersecurity Top Findings & Key Takeaways

Authors:

Marco Anisetti, *Università degli studi di Milano*

Claudio Ardagna, *Università degli studi di Milano*

Marco Cremonini, *Università degli studi di Milano*

Ernesto Damiani, *Università degli studi di Milano*

Jadran Sessa, *Università degli studi di Milano*

Paolo de Lutis, *Telecom Italia*

Cybersecurity impacts every ICT domain. In the following we consider the CONCORDIA taxonomy of domains:

- **Device/IoT-Centric Security**: Internet of Things (IoT) can be defined as *"the networked interconnection of everyday objects, equipped with ubiquitous intelligence"*[1]. IoT, edge computing, and smart devices are changing the environment in many ways, including smart transportation, sustainable mobility, smart cities, e-health, smart vehicles, and UAVs, just to name the few. The exponential growth of connected devices (from minuscule sensors to bigger machines), which, according to Intel[2] are expected to reach 200 billion by 2020, is revolutionizing current IT systems. The existence of billions of resource-constrained devices connected to the Internet introduces fundamental risks that can threaten users' life and personal sphere.
- **Network-Centric Security**: Traditional network environments are characterized by well-defined perimeters and trusted domains. Networks have been initially designed to create internal segments separated from the external world by using a fixed perimeter. The internal network was deemed trustworthy, whereas the external was considered potentially hostile. Perimeter devices, such as firewalls and intrusion detection systems, have been the traditional technologies used to secure the network.
- **System-Centric Security**: The notion of system is often used as a synonym of Operating System (OS), or in general, software that enables applications to take advantage of the computation connectivity and storage capabilities of the hardware. OSs were a preferred target of a number of disruptive attacks in the past (e.g., Code Red exploiting IIS buffer overflow, Sasser attacking the Local Security Authority Subsystem Service, Snakso Linux server rootkit) owing mainly to their complexity, centrality, and role in certain crucial security features, such as authentication. Nonetheless, they will have an essential role even in the future due to the fact that OSs are increasingly immersed in a more complex environment (e.g., mobile devices, virtualized systems), where their vulnerabilities can be either exacerbated or mitigated and they can become a commodity for applications (e.g., containerization of applications).
- **Data-Centric Security**: The ability of sharing, managing, discriminating, and accessing data quickly and remotely are at the basis of the digital revolution that started several decades ago. The role of data in today's technology is even more important, having entered the so-called, data-driven economy. Data management and inference based on them are fundamental for any enterprise, from micro to large. Moreover, data management allows enterprises to stay competitive in the evolving global market. The data domain observed important changes at all layers of an IT chain: i) data layer: from data to big data, ii) database layer: from SQL to NoSQL, iii) platform layer: from the data warehouse and DBMS to Big Data platforms, iv) analytics layer: from data mining to machine learning and artificial intelligence. For instance, data mining focuses on discovering unknown patterns and relationships in large data sets, while machine learning aims to discover patterns in data, by learning patterns parameters directly from data.
- **Application-Centric Security**: Application is denoted as a program or group of programs designed for end-users. There are numerous examples of applications used in everyday life, including word processing, spreadsheet, accounting, web browser, email client, file viewer applications among many others. Applications can be either bundled with the OS or published separately as proprietary or open-source. Current IT systems are heavily based on applications/services composed at run time.
- **User-Centric Security**: The term users refers to human users of information technologies in a professional context. In general, users may have the double role of perpetrator of a threat (e.g., a threat is carried out by human actions) or victims (e.g., individuals are the asset targeted by a threat). There is not a clear-cut answer, especially considering that users as perpetrators of security violations are necessarily considered in other domains too, and several semi-automated attack vectors, such as botnets, are operated by humans. Furthermore, humans are responsible for all kinds of cybercrimes, in the end, even social bots used in frauds have been designed by humans and provide illicit benefits to some humans. For most security incidents, the consequences are likely to impact humans (systems experiencing downtime, malicious applications, compromised IoT networks).

Key Takeaways

The following summarizes the most important findings, as a key takeaway, emerging from the threat landscape.

- **Endemic persistent threats.** Crosscutting traditional threats, like software bugs, malware, and DoS, which span all over the ICT domains, from OS to networking and applications, are becoming persistent and endemic. Even old vulnerabilities can revive in the context of a new domain not enough to consider security as the first-class requirements. Even advanced architectures must be designed to face security threats, like in the case of 5G services, virtualized operating systems, and layered systems, where a number of countermeasures are used to limit their impact(e.g., sandboxing, isolation). Persistent threats are increasingly exploiting new possibilities given by new assets, platforms, and application domains. For instance, DoS is evolving towards targeting mobile devices and sensors, by speeding up battery consumption, instead of inducing service failures. Mobile devices are becoming a suitable target vector due, for instance, to poor security skills of the users. For instance, stealthy multimedia files can be used to carry out the attack, unrecognized by inexperienced users, instead of more traditional DoS flooding techniques[3]. *Interested domains:* All.
- **Balance security and domain-specific constraints.** Not all the domains can adopt the same security countermeasures to deal with cybersecurity risks. There is the need to find a good trade-off between the security level to be achieved, also, as set forth by the associated legal and economic requirements. On one hand, the economic impacts of cybersecurity on the different actors and stakeholders can have important consequences. The assessment of cybersecurity efficiency in terms of economic investments in cyber ecosystems becomes fundamental to analyze security from a strictly economic point of view, considering that often critically important systems or components have their investments in related security activities neglected. For instance, in IoT, there is an ongoing discussion on the adoption of lightweight cryptography for embedded devices in order to find a balance between security and cost constraints.[4] Such reduced cryptography protection quality is not feasible in other domains, where security breaches and data leakages are likely to have severe impacts and a number of persistent threats still exist. The European Regulatory framework provides the basis to respond to cybersecurity threats, also, by allowing in the longer terms the related capacity building across sectors. However, the rapid development of current architectures and infrastructures render it challenging for existing regulations to remain effective for newly introduced regulations to be sufficiently future proof. Nevertheless, the European Regulators have been taking prompt action by amending existing regulations as, for instance, the ePrivacy Directive and by announcing initiatives such as the announcement by the European Commission of new legislation focusing on artificial intelligence. *Interested domains:* All.
- **Relation between security and safety.** ICT is more and more permeating every sector and impacts, people, everyday life. It is nowadays clear that there is an increasing connection between cybersecurity and safety, and this will be more and more exacerbated in the future. The impact of IoT cybersecurity on safety, for instance, is crucial and current trends in the adoption of IoT in critical environments such as automotive and UAVs will increase it tremendously. Another scenario where safety is connected with IoT security is health. There is increasing adoption of IoT devices in hospitals and at the same time very low awareness about the security impact of having critical devices connected to the Internet. In this scenario, there is also a critical privacy concern to be addressed since in most cases hospital infrastructures, even if certified for HIPAA, are not ready to host IoT ecosystems that most of the times share the same networking segment as the rest of the hospital system. *Interested domains:* Device/IoT, System.
- **Physical access and insider threats.** Having physical access to assets is a serious insider-related threat and often permits to easily bypass security protections (e.g., in the IoT domain). In general, insider threats are difficult to mitigate, both when access to critical information with high privileges is granted by software components, and when access is granted to humans/employees. In the latter case, there is the additional difficulty of predicting human behavior and intentions. For the future, it is a common belief that these threats might become even more insidious, especially when human-based (Netwrix 2018 Cloud Security Report indicates that 58% of companies attribute security breaches to insiders). This trend will be further exacerbated in the IoT context thanks to the distributed nature that makes it easier to hide insider activities. A huge effort will be put in the future to identify anomalous human behavior in conjunction with insider threats. *Interested domains:* Device/IoT, System.
- **User profiling.** The need for profiling users has a long history in ICT and was grounded on the need for control. It emerges more concretely when linked to business profits. Profiling is also one of the preliminary stages to carry out a cyber-attack and to gain an advantage. The profiling capabilities (e.g., using social engineering) will be more and more exploited in the future for attack preparation and for targeted spam campaigns. The success of smart home IoT devices is enlarging the perimeter exploitable for profiling purposes. Alexa and Google home, to name the ones with the largest user base, are fully connected and powerful devices having as one of their main goals to profile the users. They are also perceived as ubiquitous devices, and this lowers the transparency of the interaction with them, increasing the risk due to low awareness. This type of device is also connected to a powerful AI that will constitute in the future a new target for an attacker having the objective to lead the IoT to take a wrong decision (e.g., to not recognize a specific face as the one of a criminal). *Interested domains:* Device/IoT, System, User.
- **Diffusion of Ultra-Wideband networks.** The network is obviously the primary attack vector. The more the network is powerful, the more the attack vector is critical. With the adoption of 5G, network slicing will offer differentiated services over the whole network, opening the possibility to provide networking infrastructure as a service. New threats will be introduced from the adoption of network slicing in the context of verticals. IoT threats are related to data leakage between multiple virtual environments or slices, bad slice isolation that can result in security resources exhaustion in other slices. Low latency of 5G could allow better coordination among zombies in a DDoS attack scenario and to exploit protocol leakages connected to performances. In the context of IoT, the capillary diffusion enabled by 5G will allow, for instance, an attacker to focus on a specific area covered by a slice, where a large number of compromised devices can interfere with the cellular connectivity leading to a new generation of better localized DDoS. *Interested domains:* Device/IoT, Network.
- **Decentralization and computation capability at the edge.** Edge computing is migrating functionality to the edge and with them also security concerns. Some of these concerns shift from a powerful and protected environment to a less powerful and less protected one. This shift needs to be carried out very carefully to provide functionalities without impacting the security features. Edge computing is adopted in many contexts including new incoming ultra-wideband networking services. For instance, the access network domain will be impacted by the support of Mobile Edge Computing (MEC) that provides enhanced functionality at the edge of the network. Some sensitive functions currently performed in the physically and logically separated core are likely to be moved closer to the edge of the network, requiring relevant security controls to be moved too. *Interested domains:* Network, Application.
- **Increased software and services embedded in networking.** Nowadays, the software is increasingly permeating networking, bringing more functionalities and flexibility, but also enlarging attack surfaces. Software-Defined Networks (SDN) and Network Functions Virtualisation (NFV) technologies are moving the traditional network architecture built on specialized hardware and software to virtualized network functions. The consequence is increased exposure to third-party suppliers and the importance of robust patch management procedures. 5G will be based on this ecosystem of networking services. Any software vulnerability will become more significant in this context. In the report about the EU coordinated risk assessment of the cybersecurity of 5G networks,[5] published on 9 October 2019, core network functions of the 5G network are underlined as critical because affecting the overall network security compromise the confidentiality, availability, and integrity of all network services. Also, management systems and supporting services are considered critical assets since they control important network elements and can, therefore, be used to conduct malicious activity, such as sabotage and espionage. Moreover, the loss of availability or integrity of these systems and services can disrupt a significant portion of 5G network functionalities. *Interested domains:* Network.
- **Artificial Intelligence as a booster of cybersecurity attacks.** The adoption of Artificial Intelligence and Machine Learning techniques can substantially expand the attack surface of every domain, permitting to discover vulnerabilities both in software components and in business process logic[6]. Artificial intelligence and machine learning techniques are at the basis of many business decisions and the success of the inferences based on them can result in a huge (economic) value. For these same reasons, they become targets of attacks by cybercriminals. On one side, data poisoning becomes a huge driver towards more complex attacks. On the other side, model poisoning aims to poison the source of training data in order to fake the learning algorithm in considering a malicious behavior as a normal one. In this context, adversarial machine learning had a huge boost and become a hot research topic, while computation architectures, such as Big data platforms, are enabling these threats on a large scale. An example of how powerful the AI is becoming thanks to the amount of data currently available and the computation capability of the distributed architecture is the current increasing trend of the deepfake.[7] Differently from the past, attackers are targeting a person's reputation to gain an advantage and to play a scam (e.g., artificial intelligence-generated voice deepfake). *Interested domains:* System, Data, User.
- **Social Media and Social Networks Threats.** Social media and social networks represent another source of emerging cybersecurity threats for the user-centered domain. The rise of social bots, that is, automatic software agents disguised as humans, is widely debated, for example in connection with the adoption of Artificial Intelligence methods able to replace humans interacting over social media. However, social bots might become a problem for cybersecurity too, for example in the case of phishing [8], for the spread of disinformation [9][10], or political propaganda[11]. In general, social bots for social media[12] and Artificial Intelligence for social media[13] are considered as both a remarkable opportunity and possibly an insidious threat for people, in both cases a challenge for future systems, organizations, and institutions[15]. *Interested domains:* System, Data, User.
- **Layered and Virtualized Systems.** Current systems are based on several layer. Several layers often including a virtualization layer. In layered systems, the security of the upper layers relies on the security of the lower ones, forming a chain where each layer can be the weakest one. The trend is to increase the level of sharing and the density of multitenancy, exacerbating the impact of most of the threats. In addition, weaknesses of traditional systems based on specific OSs will be inherited as well in the context of each layer. Specific threats for the layer protection mechanisms are evolving starting from virtualization and containment escape to cross-layer hijacking. In general, containment, isolation, and sandboxing mechanisms will expose vulnerabilities in the future and their exploitation are normally associated with a very high-risk score. *Interested domains:* System, Network.
- **Misconfigurations of security mechanisms and lack of transparency.** Given the complex multi-layer nature of current architectures, misconfigurations and in general issues due to the lack of transparency are largely considered as among those with the most severe impact. According to CSA, misconfigurations and inadequate controls will become increasingly problematic especially in cloud environments, as well as weaknesses in authentication, lack-of-control, and visibility, while more traditional threats to confidentiality based on malicious code are becoming less important for cloud and virtualization. *Interested domains:* System.
- **Business process compromise.** BPC traditional threats are becoming more and more diffuse nowadays for business processes implemented in the cloud. This is possible also due to the advanced AI capabilities of an attacker to improve BPC-based attacks. Such attacks are able, for instance, to exploit behavioral information via shadow IT, which is increasing due to the plethora of services that are becoming part of the daily activities of employees. The current lack of countermeasures capable to mitigate this behavioral-oriented threat should be addressed in the future. *Interested domains:* System, Network.
- **Human errors.** One notable trend is that human interactions with machines, and in particular the proportion of workers whose place of work is strongly intertwined with IT technologies, has increased fast in the last decade, as clearly analyzed by the European Agency for Safety and Health at Work[16]. A human mistake is more likely than in the past possibly causing failures in machine-controlled processes, a broad category that includes cybersecurity incidents. The reason is in the more frequent presence of human-machine interfaces in business processes as well as in the increasing complexity of digital-physical interactions in workplaces. Often, it could turn out to be mostly (i) a problem of business procedures, (ii) employees under the pressure of a tight schedule or with conflicting requirements between security and productivity, or (iii) even a consolidated usage of a technology, not aligned with original specification, that the company has tolerated (or promoted) along many years.[17] Healthcare is a sector that presents sensible user-centered threats and is often mentioned as one mostly endangered by emerging cybersecurity threats[18]. Not only healthcare personal information of patients is leaked or mismanaged, a type of security incident that hardly could be called "emerging"[19], but also medical devices are considered at risk and increasingly exposed to cybersecurity threats[20]. *Interested domains:* All.
- **Skill shortage and configuration errors.** Today, single and not-expert users are directly involved in complex business processes and can influence them. Configuration errors are therefore increasing as never seen before, introducing a huge amount of new opportunities for cybercriminals to affect the CIA (Confidentiality, Integrity, Availability) properties of systems and users. For instance, security misconfigurations such as wrong access policies, weak passwords, unpatched systems, and the like, make the overall environment unsecure. Personal data of the users can be stolen and sold on the black market. Entire systems can be hijacked and remotely controlled, while specific sensors/devices put offline by exhausting their resources. A portion of the whole system can be compromised to launch more complex attacks (e.g., Mirai botnet). This complexity is even exacerbated when the architecture requires interdisciplinary competences in order to be used like in the case of Big Data architecture. The privacy implications of Big data processing are connected with the computation architecture, as well as with the algorithms, models, and learning possibilities. The increase in system and platform complexity does not find a counterpart in the skills and competences, resulting in important lack of data scientists able to properly manage such new technologies. Human errors in system configurations are still at the forefront of the issues driving new and old attacks. *Interested domains:* All.
- **Data breaches.** The fundamental role assumed by data in every aspect of our life makes attacks that aim to data breach and leak increasing.[21] In this context, traditional attacks like phishing and (D)DoS are reviving a new boost and mainly target the CIA triad of data. Given the potentially huge revenue for attackers stealing data, targeted phishing attacks and malware have been presented in the last few years. For example, phishing attacks are not aiming at big numbers of compromised users, but rather they target rich individuals, people with access to financial accounts or sensitive business data, or even public authorities that handle PII related data.[21] As another example, malware mostly targets data and in particular unauthorized data wiping, modification, access. They count 30% of all data breaches incidents.[22] Moreover, the EU General Data Protection Regulation (GDPR) that became applicable as of May 2018 introduced a series of novelties, including the mandatory reporting of data breaches to the competent authorities, provided that certain requirements are met. Today, a data breach or leakage can become a new weapon in the cybercriminal hands, which will increase the number of extortion attacks with the threat of GDPR penalties deriving from data disclosure. Note that the reporting of security incidents to competent authorities is, also, dictated under then Directive on the Security of the Networks and Information Systems (NIS Directive) that was to be transposed to the national legal orders of the Member States by May 2018. *Interested domains:* All.
- **Applications and software everywhere.** As applications are spreading at all layers of ICT systems, attacks targeting them are spreading as well. Malware attacks continue to rule the roost, particularly targeting cloud (and IoT) applications. Ransomware is still strong in this area and difficult to challenge by national law enforcement agencies alone. Mobile malware is growing exponentially since 2017, following the increase in the use of mobile systems, such as mobile banking that is overtaking online banking.[23] In this context, it is quite likely that the growth and development of mobile malware targeting users and applications will be observed. *Interested domains:* Application.
- **Complexity of the application deployment environment.** Traditionally, the application deployment environment is considered quite stable. It is handled as a landing platform for application development. Nowadays, the complexity and dynamics of the surrounding environment are changing this scenario. The increase in platform complexity and the proliferation of many (third-party) libraries open the door to new attacks (e.g., privilege escalation, hijacking, code execution) that threaten not only the platform itself but also the users relying on it. *Interested domains:* Application.
- **Service miniaturization.** The advent of microservice architecture has increased the revenue for enterprises and supported new businesses, at the same time neglecting non-functional properties such as security and privacy. This scenario represents one of the most important challenges to be faced in the next years. The miniaturization of services but also of devices (IoT sensors), as well as the pervasive and continuous involvement of humans in the functioning loop, have resulted in an environment with an unprecedented level of risk. *Interested domains:* Application, Device/IoT, System.
- **Cyber-physical systems as enablers of next-generation attacks to users.** Cyber-physical systems have brought changes to several aspects of daily life, like in electrical power grids, oil and natural gas distribution, transportation systems, health-care devices, household appliances, and many more. They clearly could show a relevant user-centered component, either for their development and maintenance, or the consequences of their operation. As often is the case with emerging technologies, they are often riddled with security vulnerabilities that could easily become threats to users and individuals[24]. *Interested domains:* Human, Device/IoT, System.

The following list represents an overview of the identified key takeaways and their corresponding domains:

- **Endemic persistent threats**: All.
- **Balance security and domain-specific constraints**: All.
- **Relation between security and safety**: All.
- **Physical access and insider threats**: Device/IoT, System.
- **User profiling**: Device/IoT, System, User.
- **Diffusion of Ultra-Wideband networks**: Device/IoT, Network.
- **Decentralization and computation capability at the edge**: Network, Application.
- **Increased software and services embedded in networking**: Network.
- **Artificial Intelligence as a booster of cybersecurity attacks**: System, Data, User.
- **Social Media and Social Networks Threats**: System, Data, User.
- **Layered and Virtualized Systems**: System, Network.
- **Misconfigurations of security mechanisms and lack of transparency**: System.
- **Business process compromise**: System, Network.
- **Human errors**: All.
- **Skill shortage and configuration errors**: All.
- **Data breaches**: All.
- **Applications and software everywhere**: Application.
- **Complexity of the application deployment environment**: Application.
- **Service miniaturization**: Application, Device/IoT, System.
- **Cyber-physical systems as enablers of next-generation attacks to users**: Human, Device/IoT, System.

---

[1] *F. Xia, L. T. Yang, L. Wang e A. Vinel, «Internet of Things,» International Journal of Communication Systems 25 (September 2012), vol. 9, pp. 1101-1102, 2012.*

[2] *A guide to Internet of Things Infographic* https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

[3] *P. Bhat e K. Dutta, «A Survey on Various Threats and Current State of Security in Android Platform,» ACM Computing Surveys, vol. 52, pp. 1-35, February 2019.*

[4] *The Debate Over How to Encrypt the Internet of Things* https://www.wired.com/story/lightweight-encryption-internet-of-things/amp

[5] *EU-wide coordinated risk assessment of 5G networks security* https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[6] *S. Hussain, O. Chowdhury, S. Mehnaz e E. Bertino, «LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE,» Network and Distributed Systems Security (NDSS) Symposium 2018, February 2018.*

[7] *A Voice Deepfake Was Used To Scam A CEO Out Of $243,000* https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#114964a22241

[8] *M. Shafahi, L. Kempers e H. Afsarmanesh, «Phishing through social bots on Twitter,» n 2016 IEEE International Conference on Big Data (Big Data), 2016.*

[9] *C. Shao, G. L. Ciampaglia, O. Varol, A. Flammini e F. Menczer, «The spread of fake news by social bots,» pp. 96-104, 2017.*

[10] *C. Shao, G. L. Ciampaglia, O. Varol, A. Flammini, F. Menczer e K.-C. Yang, «The spread of low-credibility content by social bots,» Nature Communications, vol. 9, n. 1, p. 4787, 2018.*

[11] *A. Bessi e E. Ferrara, «Social bots distort the 2016 U.S. Presidential election online discussion,» First Monday, vol. 21, n. 11-7, 2016.*

[12] *F. Brachten, M. Mirbabaie, S. Stieglitz, O. Berger, S. Bludau e K. Schrickel, «Threat or Opportunity? – Examining Social Bots in Social Media Crisis Communication».*

[13] *A. Nowak, P. Lukowicz e P. Horodecki, «Assessing Artificial Intelligence for Humanity: Will AI be the Our Biggest Ever Advance ? or the Biggest Threat [Opinion],» IEEE Technology and Society Magazine, vol. 37, n. 4, pp. 26-34, 2018.*

[14] *Y. Duan, J. Edwards e Y. Dwivedi, «Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda,» International Journal of Information Management, vol. 48, pp. 63-71, 2019.*

[15] *D. Helbing, B. Frey, E. Hafen, J. van den Hoven, G. Gigerenzer, R. Zicari, A. Zwitter e Y. Hofstetter, «Will Democracy Survive Big Data and Artificial Intelligence?,» In Towards Digital Enlightenment, pp. 73-98, 2019.*

[16] *E. Flaspöler, A. Hauke, P. Pappachan, D. Reinert, B. T., N. Henke e R. O. D. Beeck, «The human machine interface as an emerging risk,» EU-OSHA (European Agency for Safety and Health at Work), Luxembourg, 2009.*

[17] *C. Ciborra, «The Labyrinths of Information: Challenging the Wisdom of Systems,» OUP, Oxford, 2002.*

[18] *C. Kruse, B. Frederick, T. Jacobson e D. K. Monticone, «Cybersecurity in healthcare: A systematic review of modern threats and trends,» Technology and Health Care, vol. 25, n. 1, pp. 1-10, 2017.*

[19] *H. Kupwade Patil e R. Seshadri, «Big Data Security and Privacy Issues in Healthcare,» n 2014 IEEE International Congress on Big Data, pp. 762-765, 2014.*

[20] *J. Sametinger e J. W. Rozenblit, «Security Challenges for Medical Devices,» Communications of the ACM, vol. 58, n. 4, pp. 75-82, 2015.*

[21] *WP2018 O.1.2.1 – ENISA Threat Landscape 2018* https://www.enisa.europa.eu/publications/enisa-threat-landscape-report

[22] *2018 Verizon Data Breach Investigations Report,* https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report

[23] *Europol, Internet Organised Crime Threat Assessment (IOCTA), Strategic, policy and tactical updates on the fight against cybercrime* https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

[24] *A. Humayed, J. Lin, F. Li e B. Luo, «Cyber-Physical Systems Security — A Survey,» IEEE Internet of Things Journal, vol. 4, n. 6, pp. 1802-1831, 2017.*