20 Years of Scientific Evolution of Cyber Security: a Science Mapping

Leonardo Bertolin Furstenau[1], Michele Kremer Sott[1], Andrio Jonas Ouriques Homrich[2] and Liane Mahlmann Kipper[3]
[1]Master student of Graduate Program in Industrial Systems and Processes
[2]Undergraduate student of Production Engineering
[3]Professor of Graduate Program in Industrial Systems and Processes
University of Santa Cruz do Sul (UNISC)
Santa Cruz do Sul – BRAZIL
leonardofurstenau@mx2.unisc.br, micheleksott@mx2.unisc.br, andrio@mx2.unisc.br, liane@unisc.br

Abdul Aziz Al Abri
Professor of Advanced Cyber Security Academy
Advanced Cyber security Academy
Muscat – OMAN
abdulaziz.alabri@aca.om

Theodoro Flores Cardoso
Undergraduate student of Automation and Control Engineering
Pontifical Catholic University of Rio Grande do Sul (PUCRS)
Porto Alegre – BRAZIL
cardoso.theodoro@gmail.com

José Ricardo López-Robles
Management Engineering PhD
University of the Basque Country
Bilbao – SPAIN
ricardolopezrobles@outlook.com

Manuel J. Cobo
Professor at the Dept. of Computer Science and Engineering
University of Cadiz
Cadiz – SPAIN
manueljesus.cobo@uca.es

Abstract
The technologies of industry 4.0 such as big data brings challenges since companies will have to deal with a large amount of data that will help to anticipate and solve problems in development, flexibility and organizational efficiency. On the other hand, companies need to create defenses strategies, also known as “cyber security” in order to deal with the cyber-attacks. The objective of this study is to perform a science mapping in the field of study of cyber security in order to discover current topics, authors in the field and create a map of the area of study, identify productive themes with great scientific impact and point challenges, perspectives and suggestion for future works. To perform this science mapping, the SciMAT (Science Mapping Analysis Software Tool) was used. Besides, the VOSviewer was used to analyze co-authorship between countries and authors. The scientific evolution presented 17 clusters whereby the most representative themes are: 'challenges', 'framework' and ‘intrusion detection’. The analysis of the network of the cluster

'challenges' showed the most challenges that researchers are trying to solve such as: ‘privacy’, ‘smart grid’, ‘internet of thing’, ‘systems’, ‘smart cities’, and ‘cloud computing’.

Keywords
Cyber security, Data security, Industry 4.0, SciMAT, Science Mapping.

1. Introduction

Cyber security is a concept related to computer engineering focused on ensure the privacy, confidentiality, and integrity of data transmitted or stored on internal networks or on the Internet itself (Babiceanu and Seker 2016). This concept is becoming gradually more important as the complexity of integration between physical and cyber dimensions increase, providing opportunities for hackers to take advantage of remote management of systems for adverse purposes (Mo et al. 2011), whose attacks have become increasingly common and sophisticated, arousing the concern of wide range of agents of society, like individuals, businesses and governments (Liu and Yu 2011; Babiceanu and Seker 2016). The concept can be understood as the protection of the cyber environment, as well as the physical dimensions of information technology that support it and the users whose information, data, and interests may be vulnerable to cyber-attacks (Von Solms and Van Niekern 2012). Thus, it becomes a relevant topic as society demands security in its information infrastructure to contain system vulnerabilities, which may compromise social and national welfare in situations of cyber terrorism, system sabotage, information warfare and natural disasters that endanger the infrastructure which support society (Ten et al. 2010; Jang-Jaccard and Nepal 2014; López-Robles et al. 2018; López-Robles et al. 2019a). The industry 4.0 technologies such as big data, cloud computing, internet of things will allow the automation of processes and data exchange (Furstenau and Kipper 2018), but the cyber-physical systems are susceptible to security threats in the same way, where the ability to extract and generate information from networks can be severely affected by these vulnerabilities, which, coupled with the scarcity of skilled professionals in the field, undermine the viability and integrity of smart factories (Atat et al. 2018; Cobo et al. 2018; Kipper et al. 2019; López-Robles et al. 2019b).

In an increasingly technology-dependent society, the number of cyber-attacks grows as much as the need for information. In 2012 cyber-attacks cost $ 114 billion a year, and could reach $ 385 billion if we consider the time companies spend trying to recover (Jang-Jaccard and Nepal 2014). According to the Symantec Cybercrime Report (2019) in 2018 enterprise ransomware infections had a 12% increase over the previous year, while 55% of incoming emails were classified as spam and one in 36 devices used in organizations are at high risk, showing that these remain as problems for organizations. Concern is increasing since industry 4.0 smart products and services are estimated to be $ 310 billion by 2023 (Kumar and Iyer 2019), with billions of smart sensors and more than 50 billion devices connected by 2020, which could double every two years (Brenner 2018).

The bibliometric analysis performed by Kipper et al. (2019) pointed out the evolution of themes inherent in the industry 4.0, as well the the state of the art, the main challenges and perspectives for future research in the field, showing that cyber security is one of the main challenges to implement industry 4.0 technologies in companies. Authors such as Nayak et al. (2016), Liao et al. (2017), Ben-Daya et al. (2017), Wang and Wang (2018) and Gu et al. (2019) also suggest more investigation in the field. Therefore, a science mapping in the field of cyber security is still needed. The objective of this study is to perform a science mapping in the field of study of cyber security in order to discover current topics, authors in the field and create a map of the field of study, identifying productive themes with great scientific impact and point challenges, perspectives and suggestion for future works.

2. Materials and methods

The materials and methods used in this study will be presented as follows. The criteria for conducting the research, as well as the scientific mapping procedures are described below. First of all, we selected the Web of Science database to perform this science mapping. The term used was “cyber security” OR “cybersecurity” OR “cyber-security” and the retrieve of data was on 11/13/2019. For the period, it was defined from 1999 to 2019, since the first paper that discusses about cyber security is Chang et al. (1999). We selected just articles and reviews as a filter of documents. To perform this bibliometric analysis we used the SciMAT software developed by Cobo et al. (2012) wich can perform all the key elements of a science mapping (data retrieval, preprocessing, network extraction, normalization, mapping, analysis, visualization, and interpretation) (Cobo et al. 2011). 2631 documents were exported from Web of Science, after we performed a preprocessing step to ensure quality results by excluding duplications of documents. Also, the word “cyber security” was excluded since the authors wanted to search for new and hidden keywords in the field of study. Besides, misspelled words were corrected. We splited the research into three subperiods (1999 – 2004; 2005 – 2010; 2011 – 2019). Finally, the keywords representing the same concept such as 'Internet of Things' and 'IoT' were grouped. A reduction of data was performed due the large amount of documents in second and third subperiod. The workflow of the science mapping performed in this study can be seen in Figure 1 (for more

information see Cobo et al. 2012; Kipper et al. 2019). Besides, this science mapping was supported by VOSviewer developed by Waltman and Van Eck (2012) in order to create the co-authorship network.

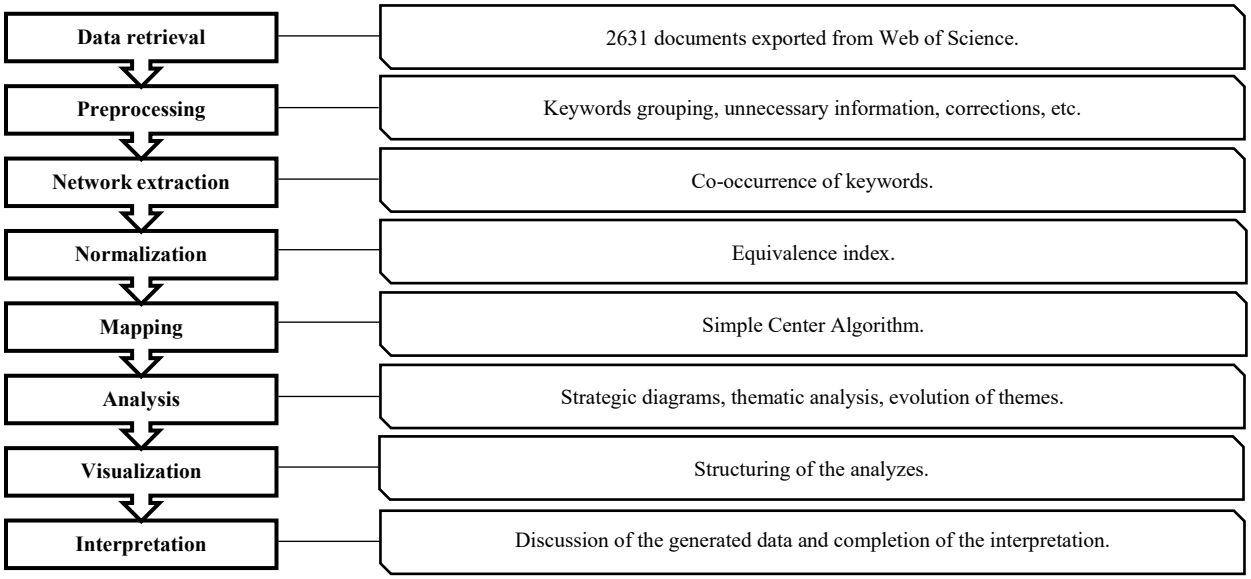


Figure 1. Workflow of science mapping (Source: Adapted from Cobo et al. 2012).

3. Analysis of data and discussions

Regarding the number of publications over time (1999 – 2019), there is a low number of publications of articles related to cyber security between 1999 and 2011 (Figure 2), but there is a significant increase from 2011, reaching 630 publications in 2018. This phenomenon can be explained by the emergence of industry 4.0, since cyber security is one of the pillars of the fourth industrial revolution (Kagermann et al. 2013; Liao et al. 2017; Kipper et al. 2019). However, there is a decline in 2019, which is justified as consequence of the period of this study (until 11/13/2019).

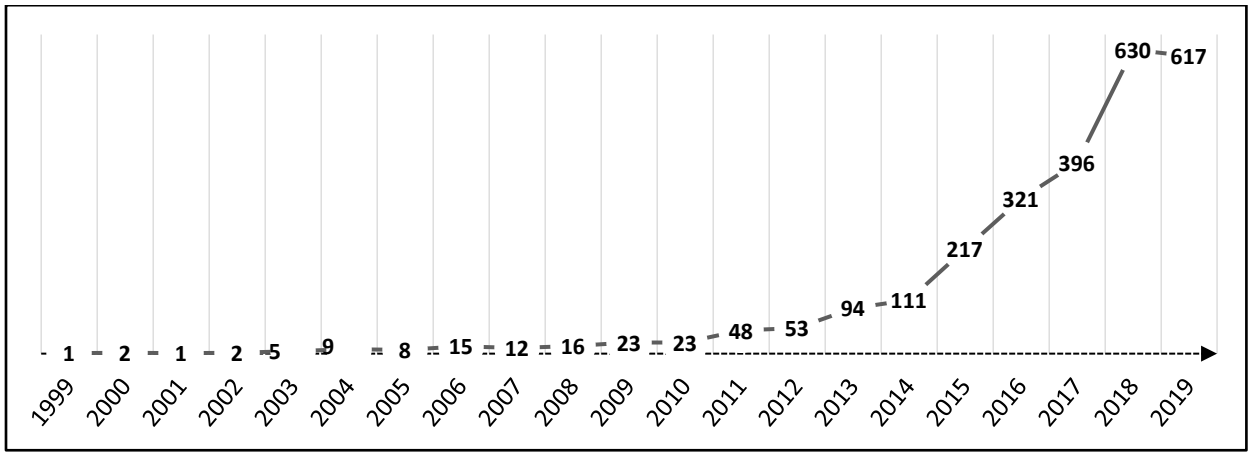
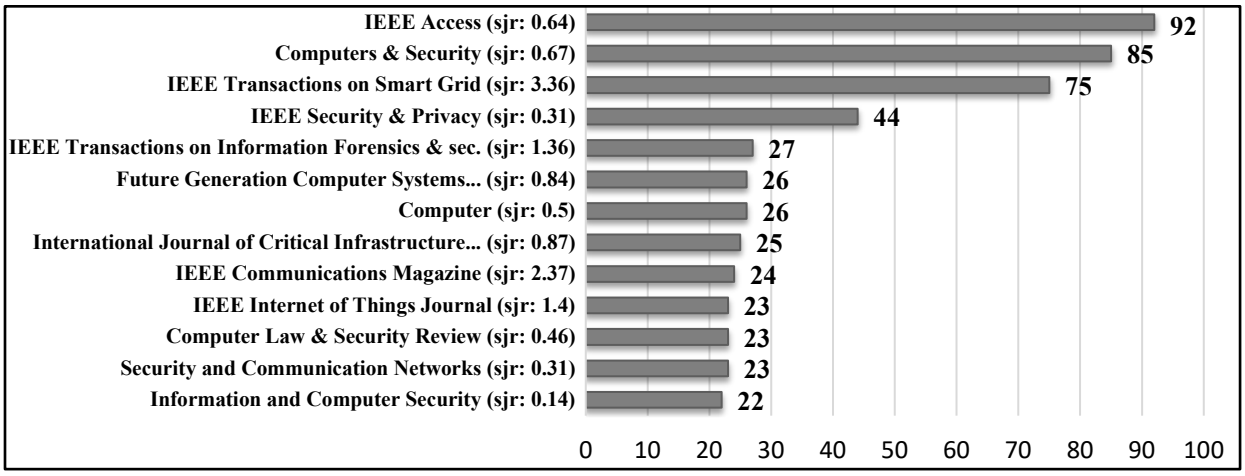


Figure 2. Number of publications over time (1999 – 2019).

Figure 3 shows the journals that publish studies relating cyber security. The IEEE Access is the journal that has the largest number of publications, followed by Computers & Security, however the journal with the highest SCImago Journal Rank (SJR) is IEEE Transactions on Information Forensics with 3.36. The SJR indicates the journal's scientific impact factor (Falagas et al. 2008). Publications in such journals, whose scientific impacts (SJR) are high, demonstrate the importance and necessity of studies related to the theme.

Figure 3. Journal that publish studies to cyber security (Source: SCImago and SciMAT).



For the analysis of authors network we used the software VOSviewer developed by Waltman and Van Eck (2012). It is possible to observe that there are 5 main groups of researchers in the field of cyber security (Figure 4). The countries with largest number of publications is the USA, followed by the People's Republic of China, these countries also have a strong relationship in publications and partnership in the field of cyber security.

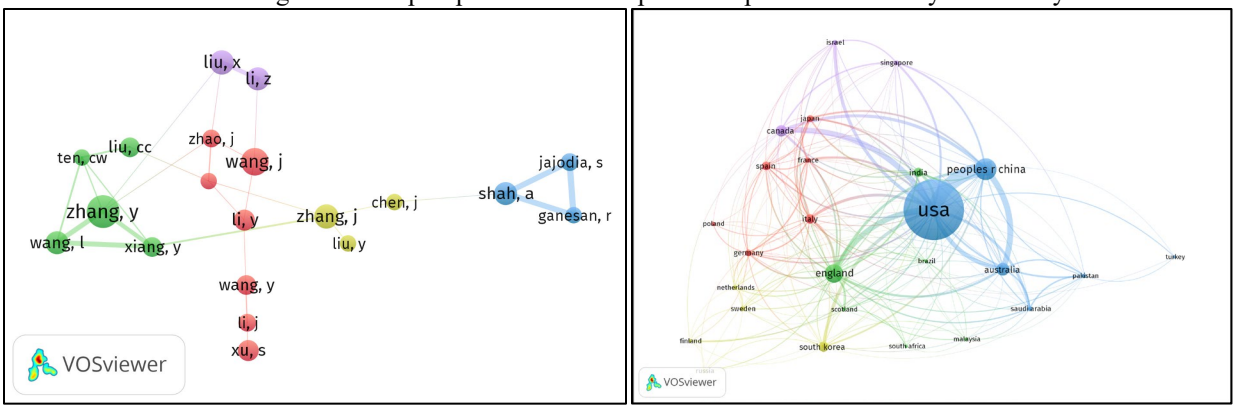


Figure 4. Co-authorship network of authors and countries on cyber security.

4. Analysis and discussion of the strategic diagrams

Cyber security first appeared in the literature in 1999, when Chang et al. (1999) developed a methodology for statistical with network and host security, in order to protect networks, computers and intellectual properties of the organization. Later, Martin (2001) presents the vulnerabilities and consequences of the lack of security in system networks, as well as the concern of organizations in the search for methods and technologies that help in the security of their data. Between 1999 and 2004 few documents were found addressing cyber security. The 'intrusion-detection' theme in first subperiod (Figure 5) is characterized as a motor theme, with high density and strong centrality, being discussed by Lam and Chiueh (2004) when dealing with the implementation of a hijacking attack identification system. The themes 'internet' and 'risk-analysis' are also discussed in this subperiod, but with less centrality and density.

In the second subperiod (2005 – 2010) new clusters related to cyber security emerged and gained momentum, mainly linked to information technology security (IT-Security), which is characterized as a highly dense and central cluster. In this scenario, Ericsson (2007) addresses security in electricity companies, especially regarding awareness

and management. After, the author discusses framework development, risk assessment and technologies for electric utilities (Ericsson 2009), cyber security and communication system for development of a smart grid infrastructure (Ericsson 2010). Discussions involving information technology also guide other clusters of this subperiod. The clusters 'systems' and 'network' for instance bring work related to frameworks for modeling security measures (Pudar et al. 2009; Ten et al. 2010).

In the third subperiod (2011 – 2019) the subject presented a considerable increase of documents in the area, and new clusters emerged representing new research relations. In this subperiod, cyber security once focused on firewalls, intrusion detection, and other organizational property protections is undergoing a major transformation with the implementation of internet of things, sensors, and distributed systems, among other technologies that have gained momentum with the coming of industry 4.0 (Culot et al. 2019). Thus, cyber security becomes indispensable in businesses that integrate technologies through the internet (Lin and Bergmann 2016; Georgescu et al. 2019), applying guidelines, policies, risk management and the use of tools and technologies to protect the cyber environment of organizations (Lykou et al. 2019). In this subperiod the cluster 'challenges' stands out for its high density and strong centrality with the largest number of associated documents. The papers address different challenges in this scenario, such as smart cities (Gharaibeh et al. 2017), smart grids (Leszczyna 2018; Ferrag et al. 2018), internet of things (Aman et al. 2018), among others. Other clusters such as 'intrusion-detection', 'framework' and 'impact' also have a high degree of development and a great impact on the research field.

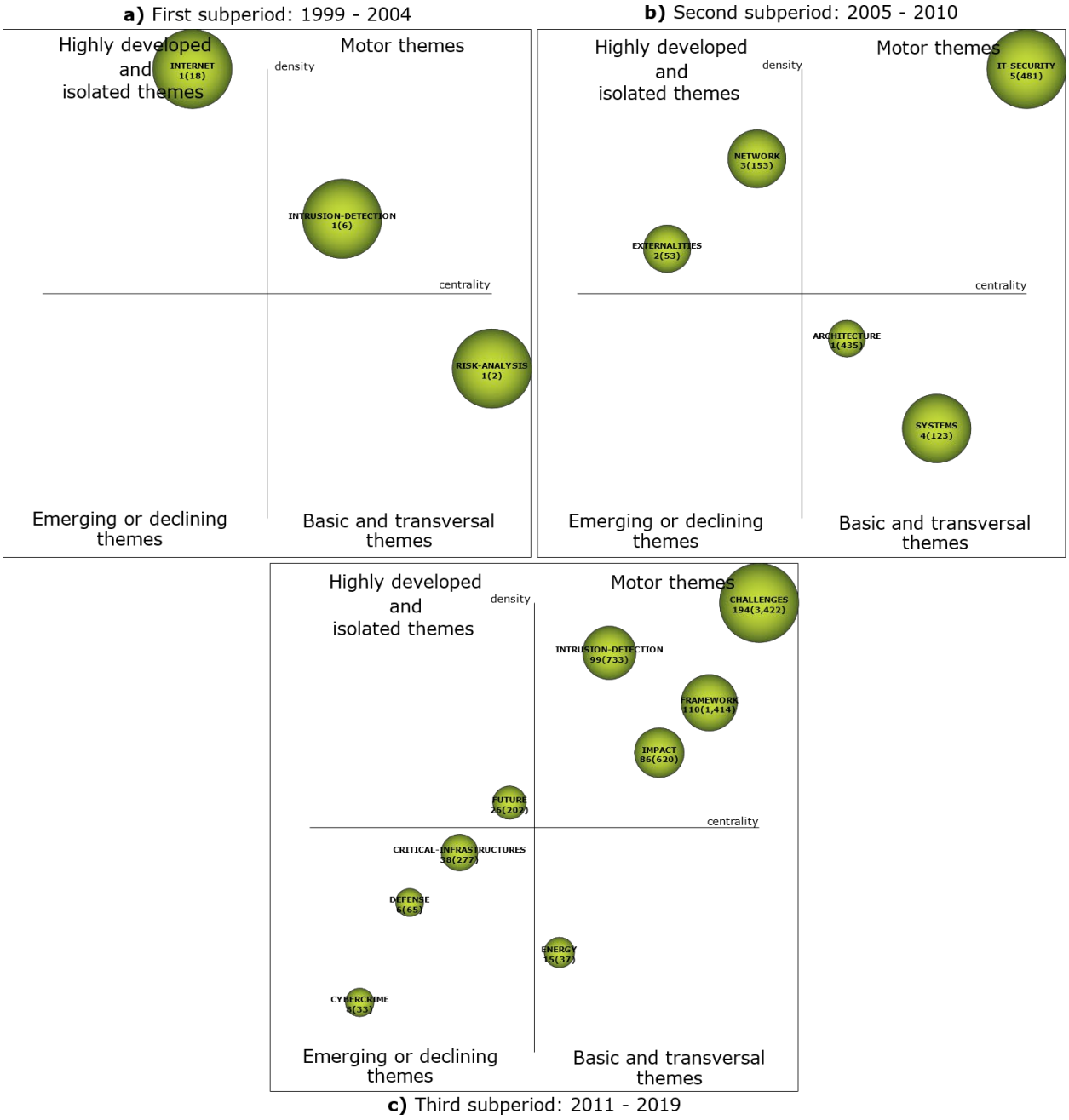


Figure 5. Strategic diagrams (1999 – 2019) (Source: SciMAT).

5. Analysis of thematic areas

Figure 6 presents the thematic evolution of the field of study of cyber security. The size of the clusters is proportional to the number of associated documents. The first subperiod (1999 – 2004) is characterized by the emergence of clusters such as 'internet', 'intrusion detection' and 'risk analysis'. These themes present the beginning of researchers' concern with planning for data security management in large networks (Chang et al. 1999), mainly because organizations have failed to create barriers in their networks and systems (Martin 2001). Therefore, risk analysis, as well as new method to identify threats and vulnerabilities performed by saboteurs, terrorists and other criminals (Baybutt 2003) started being developed.

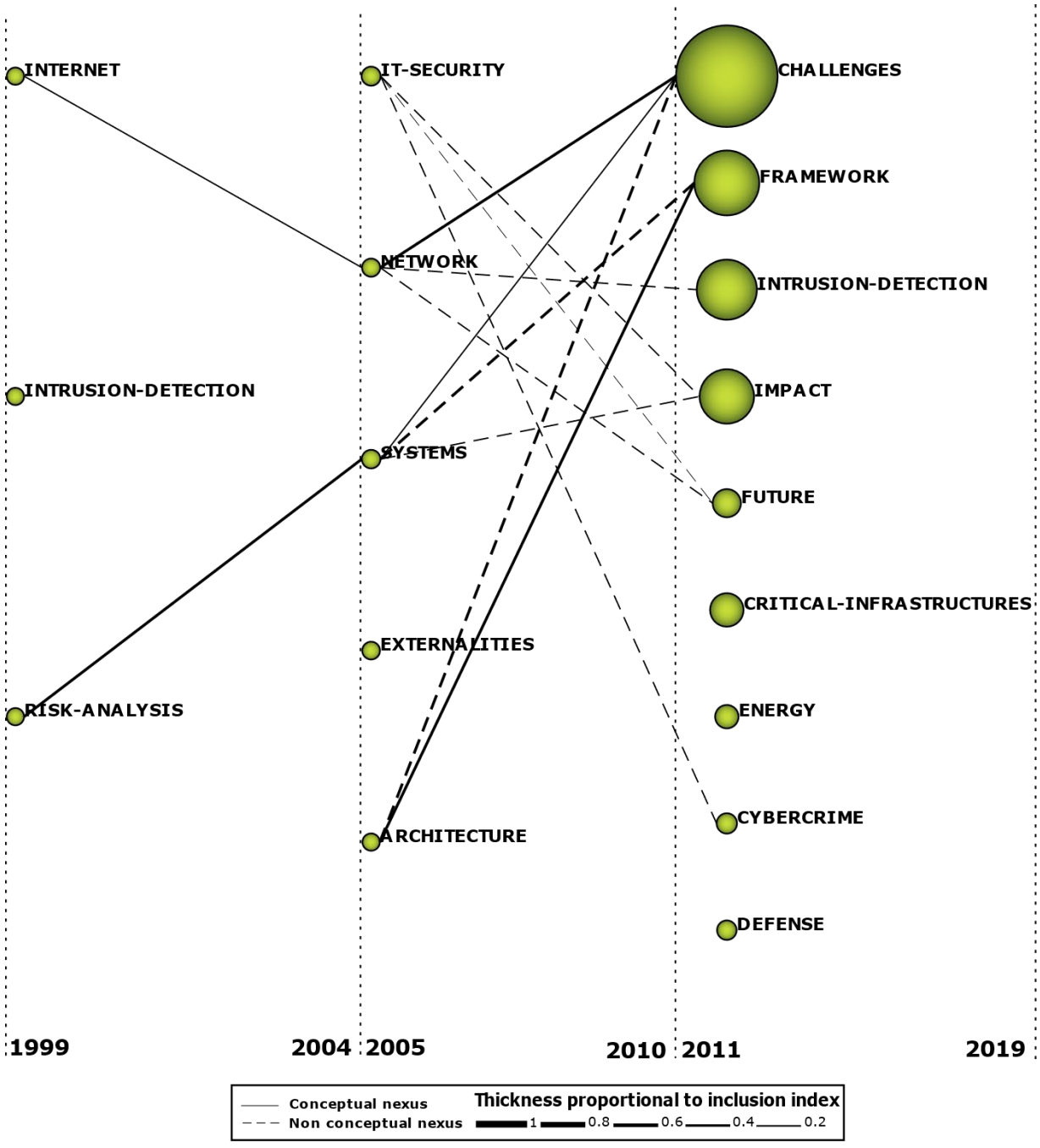


Figure 6. Thematic areas (Source: SciMAT).

The second and third subperiod shows the higher co-occurrence of clusters such as 'internet', 'network' and 'challenges', 'risk analysis', systems' and 'challenges'. This relationship shows the transition to a new era of challenges in the field of cyber security, mainly due the emergence of the concept of industry 4.0 created by the German government (High Tech Strategy). Through a deep investigation of the cluster 'challenges' (Figure 7) it is possible to identify the main challenges related to other technologies and concepts of industry 4.0 such as cloud computing, internet of things, smart grid, wireless sensors network. Moreover, systems and privacy presents as big challenges, since companies are worried about the implementation of technologies of industry 4.0 such as cyber-physical systems, since a cyber-attack in this system can cause a high impact and damages in companies such as loss

of data, incorrect production of parts, as well as risks to equipment and collaborators (Yu et al. 2017; Khalid et al. 2018; Kipper et al. 2019).

The co-occurrence of the clusters 'architecture' and 'framework' highlights the efforts of researchers to develop new architectures and frameworks in order to deal with attacks on electricity distribution infrastructure networks (Chen et al. 2016; Oughton et al. 2019), analysis of largescale critical infrastructure systems (Ficco et al. 2017), framework that defends national databases and detects cyber-attacks (Awan 2017), medical device cybersecurity framework (Alvarenga and Tanev 2017), among others. These studies show the variety of fields suffering with cyber-attacks due the interconnectedness of systems and devices.

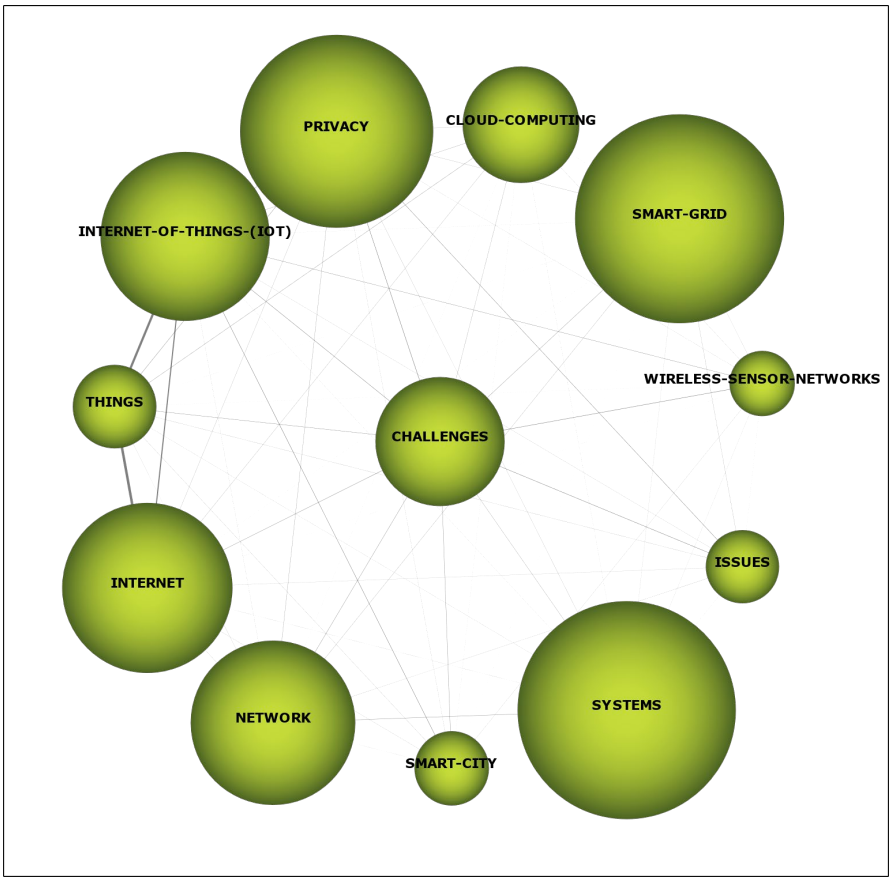


Figure 7. Network of the cluster 'challenges' (2011 – 2019) (Source: SciMAT).

6. Conclusion

The cyber security focus on cyber-attack prevention. Even the cyber security has improved over the years, the cyber-attack growth as well and cyber security became a challenge to all organizations and nations. The reason behind this that the attacker became smarter and the technology available for everyone. There is an interconnection of different infrastructures such as banking and finance, electric power, transportation, emergency services, oil and gas, water supply, among others. The effect of one sector could lead to a failure in another. The invader may attack the supply chain in order to achieve the goal, which can be an individual or organization. The effect of the attack could impact the human life. Therefore, all organizations should practice the cyber resilience (cyber security plus cyber defense) to ensure the business continuity. The cyber resilience can be deployed through different capabilities started by cyber threat intelligence.

The aim of this study was to perform a science mapping of 20 years of studies of cyber security with the support of SciMAT and VOSviewer software. Through this research we identified current topics, authors in the field, co-authorship of researchers, as well as the development of a map of the field of study, identifying productive themes with great scientific impact, highlighting challenges, perspectives and suggestions for future works. The number of publications is increasing considerably every year. The countries that publish the largest amount of documents about

cyber security are the USA and China. The scientific evolution presented 17 clusters whereby the most representative themes are: 'challenges', 'framework' and 'intrusion detection'. The analysis of the network of the cluster 'challenges' showed the most challenges that researchers are trying to solve such as: 'privacy', 'smart grid', 'internet of thing', 'systems', 'smart cities', and 'cloud computing'. This research is limited to analyzing only the Web of Science database. Besides, some studies may have been ignored, since the work linked to the most important clusters, which are characterized as motor themes in the strategic diagrams, with the purpose of reducing the bias of the researchers on the chosen works. Only documents articles and reviews in English were also used, although other documents may present relevant topics and research. Further works can be developed by analyzing databases such as Scopus, Science Direct, among others. Future works can be performed in order to strengthen research networks between countries mainly in creation of partnership with the USA and China, since these are the countries that have most substantial amount of publications and researchers dealing with cyber security in order to develop new theories and frameworks, so that companies can create better defense strategies for cyber-attacks, and as a consequence support the implementation of industry 4.0.

Acknowledgments

We acknowledges the support by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES) - Finance Code 001, Ministry of Manpower - Advanced Cyber Security Academy - Oman Sultanate and CONACYT - Consejo Nacional de Ciencia y Tecnología (Mexico) and DGRI-Dirección General de Relaciones Exteriores – México to carry out this study.

References

Aman, M. N., Sikdar, B., Chua, K. C., and Ali, A., Low Power Data Integrity in IoT Systems, *IEEE Internet of Things Journal*, *5*(4), 3102-3113, 2018.

Atat, R., Liu, L., Wu, J., Li, G., Ye, C., and Yang, Y., Big data meet cyber-physical systems: A panoramic survey, *IEEE Access*, *6*, 73603-73636, 2018.

Awan, J. H., Memon, S., Pathan, S. M., Usman, M., Khan, R. A., Abbasi, S., ... and Hussain, Z., A user friendly security framework for the protection of confidential information, *Int. J. Comput. Sci. Netw. Secur*, *17*(04), 215-223, 2017.

Babiceanu, R. F., and Seker, R., Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook, *Computers in Industry*, *81*, 128-137, 2016.

Baybutt, P., Cyber security vulnerability analysis: An asset-based approach, *Process Safety Progress*, *22*(4), 220-228, 2003.

Ben-Daya, M., Hassini, E., and Bahroun, Z., Internet of things and supply chain management: a literature review, *International Journal of Production Research*, *57*(15-16), 4719-4742, 2019.

Brenner, B., Transformative Sustainable Business Models in the Light of the Digital Imperative—A Global Business Economics Perspective, *Sustainability*, *10*(12), 4428, 2018.

Chang, E. S., Jain, A. K., Slade, D. M., and Tsao, S. L., Managing cyber security vulnerabilities in large networks. *Bell Labs technical journal*, *4*(4), 252-272, 1999.

Chen, Y., Hong, J., and Liu, C. C., Modeling of intrusion and defense for assessment of cyber security at power substations, *IEEE Transactions on Smart Grid*, *9*(4), 2541-2552, 2016.

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., and Herrera, F. (2011). Science Mapping Software Tools: Review, Analysis, and Cooperative Study Among Tools. *Journal of the American Society for Information Science and Technology*, 62(7), 1382-1402. https://doi.org/10.1002/asi.21525

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., and Herrera, F., SciMAT: A new science mapping analysis software tool, *Journal of the American Society for Information Science and Technology*, *63*(8), 1609-1630, 2012.

Cobo, M. J., Jürgens, B., Herrero-Solana, V., Martínez, M. A., and Herrera-Viedma, E. (2018). Industry 4.0: a perspective based on bibliometric analysis. *Procedia computer science*, 139, 364-371.

Culot, G., Fattori, F., Podrecca, M., and Sartor, M., Addressing Industry 4.0 Cybersecurity Challenges, *IEEE Engineering Management Review*, *47*(3), 79-86, 2019.

Ericsson, G. N., Cyber security and power system communication—essential parts of a smart grid infrastructure, *IEEE Transactions on Power Delivery*, *25*(3), 1501-1507, 2010.

Ericsson, G. N., Information security for electric power utilities (EPUs)—CIGRE developments on frameworks, risk assessment, and technology, *IEEE Transactions on Power Delivery*, *24*(3), 1174-1181, 2009.

Ericsson, G. N., Toward a framework for managing information security for an electric power utility—CIGRÉ experiences, *IEEE transactions on power delivery*, *22*(3), 1461-1469, 2007.

Falagas, M. E., Kouranos, V. D., Arencibia-Jorge, R., and Karageorgopoulos, D. E., Comparison of SCImago journal rank indicator with journal impact factor, *The FASEB journal*, *22*(8), 2623-2628, 2008.

Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., and Shu, L., A systematic review of data protection and privacy preservation schemes for smart grid communications, *Sustainable cities and society*, *38*, 806-835, 2018.

Ficco, M., Choraś, M., and Kozik, R., Simulation platform for cyber-security and vulnerability analysis of critical infrastructures, *Journal of computational science*, *22*, 179-186, 2017.

Furstenau, L. B., and Kipper, L. M. (2018). Produção enxuta e indústria 4.0 com foco na demanda do cliente: desafios e oportunidades para o desenvolvimento de pesquisas aplicadas. *Seminário de Iniciação Científica*, 199. https://doi.org/10.14488/enegep2018_tn_wic_258_478_35887

Georgescu, T. M., Iancu, B., and Zurini, M., Named-Entity-Recognition-Based Automated System for Diagnosing Cybersecurity Situations in IoT Networks, *Sensors*, *19*(15), 3380, 2019.

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., and Al-Fuqaha, A., Smart cities: A survey on data management, security, and enabling technologies, *IEEE Communications Surveys & Tutorials*, *19*(4), 2456-2501, 2017.

Gu, F., Guo, J., Hall, P., and Gu, X., An integrated architecture for implementing extended producer responsibility in the context of Industry 4.0, *International Journal of Production Research*, *57*(5), 1458-1477, 2019.

Internet Security Threats Report, Volume 24 - Symantec, http://www.symantec.com/threatreport/, last accessed: November 2019.

Jang-Jaccard, J., and Nepal, S., A survey of emerging threats in cybersecurity, *Journal of Computer and System Sciences*, *80*(5), 973-993, 2014.

Kagermann, H., Helbig, J., Hellinger, A., and Wahlster, W., Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry, *Final Report of the Industrie 4.0 Working Group*, Forschungsunion, 2013.

Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K. D., and Pannek, J., Security framework for industrial collaborative robotic cyber-physical systems, *Computers in Industry*, *97*, 132-145, 2018.

Kipper, L. M., Furstenau, L. B., Hoppe, D., Frozza, R., and Iespen, S., Scopus scientific mapping production in industry 4.0 (2011–2018): a bibliometric analysis, *International Journal of Production Research*, 1-24, 2019.

Kumar, A. S., and Iyer, E., An industrial IoT in engireering and manufacturing industries – benefits and challenges, International Journal of Mechanical and Production Engineering Research and Dvelopment (IJMPERD), v. 9, n 2, p. 151-160, 2019.

Lam, L. C., and Chiueh, T. C., Automatic extraction of accurate application-specific sandboxing policy, In *International Workshop on Recent Advances in Intrusion Detection* (pp. 1-20). Springer, Berlin, Heidelberg, 2004.

Leszczyna, R., Standards on cyber security assessment of smart grid, *International Journal of Critical Infrastructure Protection*, *22*, 70-89, 2018.

Liao, Y., Deschamps, F., Loures, E. D. F. R., and Ramos, L. F. P., Past, present and future of Industry 4.0-a systematic literature review and research agenda proposal, *International journal of production research*, *55*(12), 3609-3629, 2017.

Lin, H., and Bergmann, N., IoT privacy and security challenges for smart home environments, *Information*, *7*(3), 44, 2016.

Liu, P., and Yu, M., Damage assessment and repair in attack resilient distributed database systems, *Computer Standards & Interfaces*, *33*(1), 96-107, 2011.

López-Robles, J. R., Otegi-Olaso, J. R., Gamboa-Rosales, N. K., Gamboa-Rosales, H., and Cobo, M. J. (2018). 60 Years of Business Intelligence: A Bibliometric Review from 1958 to 2017.

Paper presented at the New Trends in Intelligent Software Methodologies, *Tools and Techniques: Proceedings of the 17th International Conference SoMeT_18*.

López-Robles, J. R., Otegi-Olaso, J. R., Porto-Gómez, I., and Cobo, M. J. (2019a). 30 years of intelligence models in management and business: A bibliometric review. *International Journal of Information Management,* 48, 22-38. https://doi.org/10.1016/j.ijinfomgt.2019.01.013

López-Robles, J. R., Rodríguez-Salvador, M., Gamboa-Rosales, N. K., Ramirez-Rosales, S., and Cobo, M. J. (2019b). The last five years of Big Data Research in Economics, Econometrics and Finance: Identification and conceptual analysis. *Procedia computer science*, 162, 729-736. https://doi.org/10.1016/j.procs.2019.12.044

Lykou, G., Anagnostopoulou, A., and Gritzalis, D., Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls, *Sensors*, *19*(1), 19, 2019.

Martin, R. A., Managing vulnerabilities in networked systems, *Computer*, *34*(11), 32-38, 2001.

Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., and Sinopoli, B., Cyber–physical security of a smart grid infrastructure, *Proceedings of the IEEE*, *100*(1), 195-209, 2011.

Nayak, A., Reyes Levalle, R., Lee, S., and Nof, S. Y., Resource sharing in cyber-physical systems: modelling framework and case studies, *International Journal of Production Research*, *54*(23), 6969-6983, 2016.

Oughton, E. J., Ralph, D., Pant, R., Leverett, E., Copic, J., Thacker, S., ... and Hall, J. W., Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks, *Risk Analysis*, 2019.

Pudar, S., Manimaran, G., and Liu, C. C., PENET: A practical method and tool for integrated modeling of security attacks and countermeasures, *Computers & Security*, *28*(8), 754-771, 2009.

Ten, C. W., Manimaran, G., and Liu, C. C., Cybersecurity for critical infrastructures: Attack and defense modeling, *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *40*(4), 853-865, 2010.

Von Solms, R., and Van Niekerk, J., From information security to cyber security, *computers & security*, *38*, 97-102, 2013.

Waltman, L., and Van Eck, N. J., A new methodology for constructing a publication-level classification system of science, *Journal of the American Society for Information Science and Technology*, *63*(12), 2378-2392, 2012.

Wang, X. V., and Wang, L., Digital twin-based WEEE recycling, recovery and remanufacturing in the background of Industry 4.0, *International Journal of Production Research*, *57*(12), 3892-3902, 2019.

Yu, Z., Zhou, L., Ma, Z., and El-Meligy, M. A., Trustworthiness modeling and analysis of cyber-physical manufacturing systems, *IEEE Access*, *5*, 26076-26085, 2017.

Biographies

Leonardo Bertolin Furstenau is Graduated in Production Engineering at University of Santa Cruz do Sul (UNISC), Brazil, and currently a Master's student in Graduate Program in Industrial Systems and Processes. He has experiences in production planning and control, process management and CNC (Computerized Numeric Command) machine programming, as well as consultancies focused on management strategies for small enterprises. Nowadays Leonardo Furstenau does research in Lean Production, Industry 4.0, Bibliometrics and Science Mapping and works on Interactive Laboratory of Creativity at TecnoUnisc (UNISC's Technological Park, Research & Development). His most recent publication is 'Scopus scientific mapping production in industry 4.0 (2011–2018): a bibliometric analysis'.

Michele Kremer Sott is graduated in Business Administration at University of Santa Cruz do Sul (UNISC), Brazil, and currently a master's student in Graduate Program in Industrial Systems and Processes. She has an MBA in Business Management, MBE in Production Engineering, and experience in management systems, information and communication technology. Nowadays, she works on Interactive Laboratory of Creativity at TecnoUnisc (UNISC's Technological Park, Research & Development) and does research in Industry 4.0, Lean Production, Science Mapping and Process Modelling and Management.

Andrio Homrich is an undergraduate Production Engineering student at the University of Santa Cruz do Sul (UNISC). During graduation has engaged in operations management research projects in the areas of process optimization, simulation, lean manufacturing, and intelligent manufacturing. Has experience in scientific research due junior researcher experiences at Interactive Creativity Laboratory, where has developed research regarding knowledge management tools for creativity and innovation in organizations. Currently, finishing the project course, whose theme refers to the identification of soft skills for the development of industry 4.0 in production engineering education, and collaborating with research groups related to cyber-physical systems, industry 4.0 and Big Data.

Liane Mahlmann Kipper is full Professor at the University of Santa Cruz do Sul (UNISC) and Coordinator of the Master in Industrial Systems and Processes from 2013 to 2015. She works in the Graduate Program in Systems and Industrial Processes in the areas of knowledge management, innovation and creativity, and in process management and research methods and techniques developing activities mainly on the following topics: process improvement, lean systems, innovation, creativity, product development and knowledge protection; and in process and technology management for process optimization and improvement. Has experience in Physics, focusing on Mechanics, Thermal Sciences, Optics and Experimental Physics. From 1995 until 2009 she worked with university management, especially in the research and postgraduate areas. Currently working with undergraduate courses in the technological area of UNISC and with the Master in Industrial Systems and Processes in the areas of process management and knowledge management.

Abdul Aziz Al Abri is a professor in Advanced Cybersecurity Academy. Has Master in Computer Forensics at University of South Wales in 2018. He was head of computer service section in Nizwa college of technology 2005-2013. Nowadays, Abdul Aziz gives training and classes about Cyber Security at Advanced Cybersecurity Academy for professionals of government, as well for undergraduates.

Theodoro Flores Cardoso is a senior undergraduate student in Automation and Control Engineering at Pontifical Catholic University of Rio Grande do Sul (PUCRS). He is a former WorldSkills competitor awarded with the medallion of excellence. Nowadays, besides being an expert in Mobile Robotics with over five years of experience, Theodoro is also the founder and CEO at SkillsHub, a global company that provides effective training solutions for WorldSkills, the world's largest vocational skills competition.

José Ricardo López-Robles received the Bachelor's degree in Industrial Engineering from the Monterrey Institute of Technology and Higher Education (Mexico, 2007), Master's degree in Project Management from the University of the Basque Country (Spain, 2010), Master's degree in Business Administration from the ENEB Business School (Spain, 2017) and Management Engineering Ph.D. from the University of the Basque Country (Spain, 2019). Finally, he is the recipient of the Ibero-American Award "Veta de Plata 2016" in the category "Science and Technology".

Manuel J. Cobo is a professor at the Dept. of Computer Science and Engineering, University of Cádiz, Spain, since 2011. His research focuses on Bibliometric, Science Mapping Analysis, Social Network, Artificial Intelligence, Data Mining and Information Science and he has authored more than 50 peer reviewed papers where he applies these tools on computer science, animal science, business, marketing, social work, transportation, etc. He and his team developed the open access software SciMAT for science mapping.