Cyber security beyond the Industry 4.0 era. A short review on a few technological promises

Preprint · July 2019

DOI: 10.13140/RG.2.2.25394.56002

1 author:

Antonio Clim
Bucharest Academy of Economic Studies
26 PUBLICATIONS **45** CITATIONS

SEE PROFILE

Cyber security beyond the Industry 4.0 era. A short review on a few technological promises

Antonio CLIM[1]
[1]The Bucharest University of Economic Studies
antonio.clim@csie.ase.ro

The global development industries progress towards meeting the ever evolving contemporary and future demands. This transformative evolution introduced phenomena such as Industry 4.0 and 5.0 which are facilitated by both information and operational technologies: collaborative robotics, IoT, AI. Their integration into a hyper-connected system facilitates the production of goods and services. In addition, these industries are characterized by automation, as well as by unmatched levels of data exchange throughout the value chain. Cyber security risks are crucial as the prevalence of these information and operation technologies has changed the appearance of cyber threats. Addressing the premises and realities of cyber security in Industries 4.0 and 5.0 is crucial. Risk mitigation strategies provided by various organizations are crucial for lowering risks. Given the loopholes and vulnerabilities generated by interconnections, cyber security is vital for the advancement of digital industrial transformation.
Keywords: *collaborative robots (cobots), IPv6 Low power Wireless Personal Area Networks (6LoWPAN), Sigma routing metric, Routing Protocol for LLN (RPL), ContikiOS, cyber-physical production systems (CPPSs), Destination-Oriented Directed Acyclic Graph (DODAG)*

1 Introduction

Technological developments and advancements are under a rapid pace and as a result, they play critical roles in various aspects of our lives. The technical changes, as well as socio-economic impact, are some of the critical drivers for the Industrial revolution which has implanted various technological progress. To manage such change, people will need holistic strategies which entail sustainable and innovative system solutions. Over time, the Information Communication Technology (ICT) has always been under constant evolution, and its establishment in the various processes of production is changing the conventional industry thus creating a contemporary level of organizational development [1]. For the sake of creating the advantages of such technologies which are meant to enhance the global competitive market, it is critical to have a new framework like the one discussed across the globe. The fourth industrial revolution (Industry 4.0) is a description used for the application of smart devices which can communicate along the value chain autonomously. As a result, in such a system, the machine will apply self-configuration, self-optimization, as well as artificial intelligence to offer a better quality of products and services [2].

The development of collaborative robots (cobots) which have been working without the supervision of people in different paradigms such as driverless cars with artificial intelligence, as well as automated supermarkets, has created debates and criticism across industries [3]. The main point of contention is about the effects of extreme automation which is catalyzed by factors such as Industry 4.0, artificial intelligence, and Internet of Things (IoT) towards Big Data. Therefore, in Industry 4.0, the application of IoT which has been developed on internet connectivity, sensors in animate and inanimate elements and the artificial intelligence through cobots have made sense of the Big Data. Therefore, this sense of automating the industry has led to the development of the fifth industrial revolution (Industry 5.0) which is mainly attributed by the association of machines and man hence resulted in a great collaboration in the form of cognitive computing that has been equipped to work next to human intelligence [4] as we can see in Fig. 1.

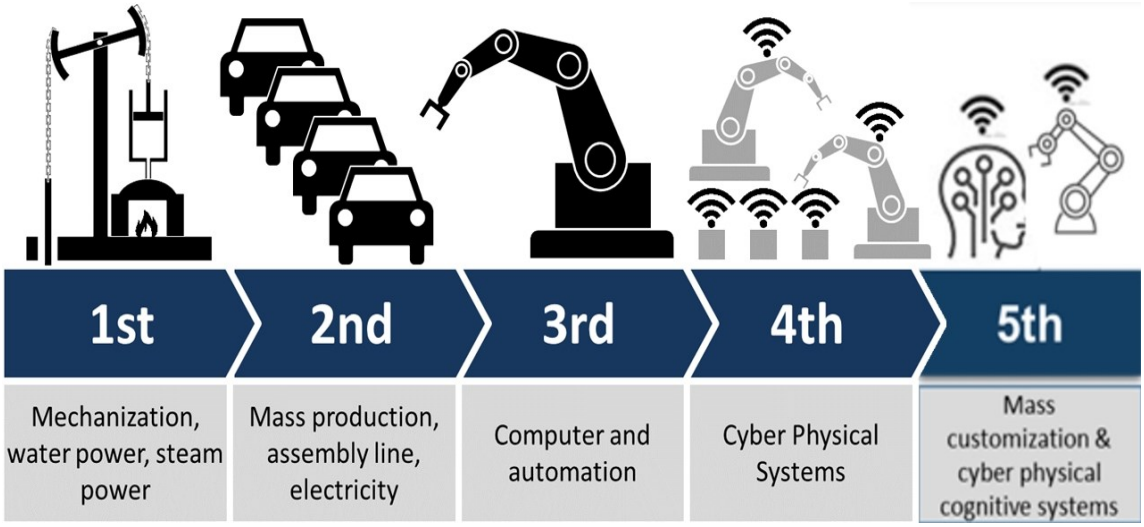

Fig. 1. Industrial revolutions [5]

Therefore, it is worth noting that in this fifth industrial revolution, the cobots, robots, as well as artificial intelligence will be the driving factors thus playing significant roles in this industry. However, despite its opportunities and capabilities, the industry will still need the human ability in customizing and personalizing the system.

Majority of the sectors which have implemented the concepts of Industry 4.0 and Industry 5.0 can be attributed by the development of significant value whereby big data is captured, stored, and mined and as a result, there are numerous opportunities developed from this across different industries such as government services [6] and even healthcare [7]. Therefore, the industrial revolutions which led to the development of ICT and other forms of digital technology caused big data to become the contemporary oil in the technology world considering how numerous advantages can be created out of big data. Consequently, the importance and impact of big data are one of the main reasons why organizations are investing a significative percent of their budgets on cyber security and privacy issues. For instance, as big data is stored and recorded, more than basic privacy conscious access control guidelines are required to be enforced such that the big data can only be used for their required functions. However, it is worth to consider how data is shared and linked through different organization and sectors because the issue of security and privacy will be highly considered [3]. Therefore, due to such aspects, the cyber security in the fourth and fifth industrial revolution has become vital since most sectors have digitized and automated their operations and this has posted various forms of vulnerabilities that can significantly cripple the system.

Both industries 4.0 and 5.0 have become effective but in the course of their development, there are various operational risks which have tagged along, and it is an issue for the connected smart industries and the digital supply networks [8]. The interdependence in these industries which drive operations as well as set pace for the digital development and advancement means that cyber security shall be the central issue of concern. That is because, in case of a cyber-attack, the effects can be extended to the extent that the industrial value chain may fail to mitigate on time because they are not ready for such risks [9]. Therefore, in this age of the Industry 4.0 on its way to 5.0, it is vital to address the cyber risks by well-developed cyber security strategies which have to be vigilant, secure, and persistent with full integration into the IT and organizational strategies. Therefore, this discussion seeks to evaluate some of the cyber security issues that affect Industry 4.0 and 5.0 in a reflection of some of the promises and realities the sector holds, in any case, there is the need for upgrades or addressing the cyber risk factors.

2 Characterizing and measuring maliciousness

Some of the prospective metrics for human maliciousness within the cyber realm is one of the initial times when the cyber security researchers have tried to gain a holistic perspective whereby humans have been considered as the malicious perpetrators in the cyber paradigm. Therefore, as a way of quantifying the cyber threats, it is essential to quantify the insider threat, expertise, as well as the economic motive in reflection to human maliciousness as one of the main risk factors for cyber security [10]. However, it is worth mentioning that there is little research done surrounding the levels of human maliciousness within the cyber paradigm such that the maliciousness within humans can be reflected from different levels such as the micro level, meso level, and the macro level. Ultimately, every factor here is a potential threat to cyber security [11]. Therefore, based on this grouping, it can be deduced that an individual can act maliciously because of their personality in as much as his or her behaviour can be influenced by the interaction he or she has with other people. The intergroup aggression is a frequent contributor for the motive of an individual person to conduct himself in a malicious manner in such a way similar to cultural biases whereby the perception of an individual regarding cyberattack is guided, and as a result, it would influence the person to conduct themselves in a specific manner [12]. Therefore, considering this characterization, it is imperative to note that maliciousness is viewed as a sociotechnical problem and in turn, it would be influential in ascertaining the optimum standards which can be applied in the process of integration of the human factors into the issues regarding the evaluation of cyber security risks [13]. Therefore, in cyber security, the thoughts, as well as the behaviour of an individual, are important factors towards malicious code in exploiting some of the vulnerabilities in technology throughout the modern industries.

Some of the promises in this area are that it is difficult to group maliciousness as well as to come up with an index for maliciousness which can be applied in modelling various human factors and behaviours through a standardized psychological evaluation [14]. However, these malicious behaviours will not, and they cannot be displayed openly during such tests, but their manifestation can be stimulated by using a gaming environment whereby the outcome will not be the real attribution of a person acting at a malicious level of a cyber-attack [15]. When an individual is genuinely malicious, they are likely to overthrow any form of testing which is focused on grouping the maliciousness and this means that maliciousness can be evaluated through natural assessment of the observable language based on rational and spontaneous communication that is developed for the sake of other purposes such as web pages and blogs [12]. Therefore, the development of an ontology focused on the grouping as well as the flowchart issued with creating and grouping relationship between a person's personality and their cultural attributes since both of them have the capacity of influencing the behaviour of an individual hence their degree of maliciousness [16]. For future, it would be essential to apply the ontology which will help to reveal some of the factors which can cause the cyber-associated maliciousness, and this research can also focus on grouping the influence of different metrics at a given time.

3 Forecast of Global Data Traffic promises of 5G and beyond

Over the past years, the world has experienced significant growth in the mobile data traffic, and it is forecasted that people will be experiencing an increase up to 23-fold as of 2021 when compared to the global internet traffic in 2005. Therefore, it is predicted that the general mobile data will reach five zettabytes (ZB) per month [17] (see table 1, below).

Characteristics	5G	6G
Individual data rate	1 Gbps	100 Gbps
DL data rate	20 Gbps	>1000 Gbps
U-plane latency	0.5 ms	< 0.1 ms

C-plane latency	10 ms	< 1 ms
Mobility	Up to 500 km/h	Up to 1000 km/h
DL spectral efficiency	30 bps/Hz	100 bps/Hz
Operating frequency	3 - 300 GHz	Up to 1000 GHz

Table 1. Table KPI Comparison between 5G and 6G [17]

The fifth generation (5G) is the latest form in mobile technology which has been coupled with massive machine-type communication as well as the internet of things among other factors. Such developments have shown that in 10 years, the 5G will attain its maximum limits hence giving way for the sixth generation (6G) that will be developed to meet the needs and demands in the mobile technology sector during that time. In addition, as the 5G is on the verge of attaining the deployment phase currently, the discussion regarding 6G is taking shape, but it is still early to discuss the aspects of 6G as much as it holds immense promises [17] (see the fig.2).

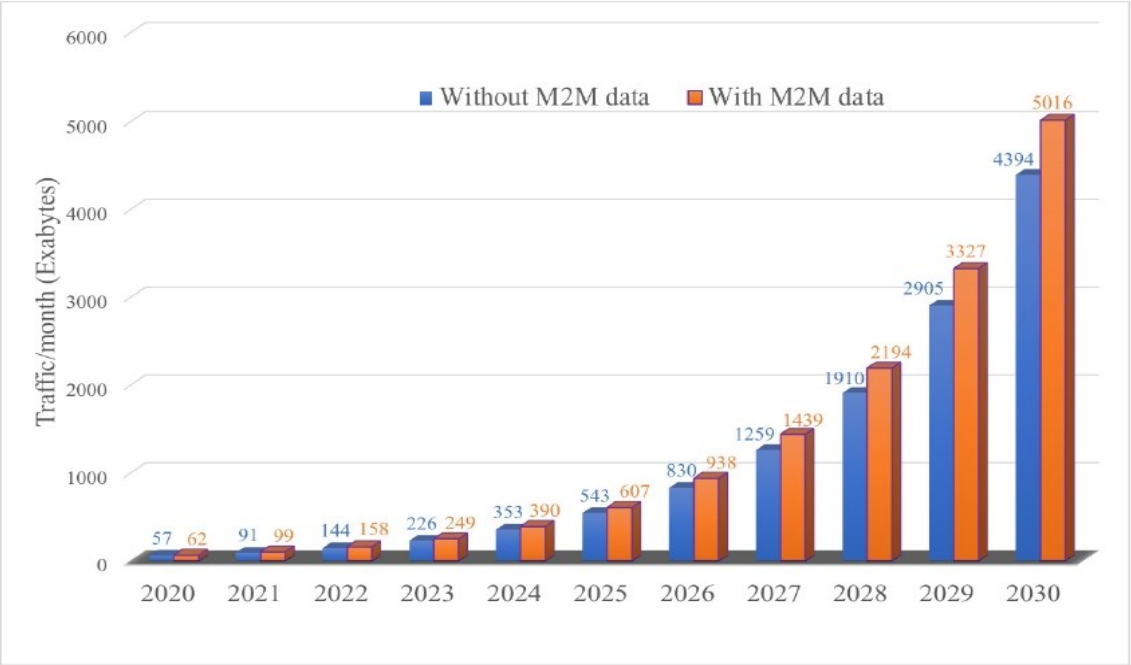

Fig. 2. Forecast of the Global Mobile Data [17]

As a result, with such promises in place, it is worth noting that in the coming years, everything around us will be intelligent hence developing more concept such as the aspect of having Internet of Everything which will be characterized by a significant amount of information and data. Other technological aspects such as AI will be integral in the 6G digitalization because there is immense actionable data as well as progress towards computation capacities.

4 Protocol structure of 6LoWPAN devices

The network layer in the protocol devices among the IoT is usually supported by (IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) hence making the IPv6 compressed and adapted to the properties Low-Rate Wireless Personal Area Networks (LR-WPANs) properties. One essential function of adapting the IPv6 to its usability within the LR-WPAN is for compression of both IPv6 headers as well as the UDP header as they are crucial during compression [18]. In scenarios whereby the WPAN is networked it should have the capacity of being transmitting the IPv6 packets between the non-directly accessible devices which belong to various WPAN throughout the multiple transit devices. Considering that the transmission of an IPv6 packet entailed in the MAC frame occurs on the link-layer in different hops through transit devices that are explicitly used as forwarders whereby one speaks about a multi-hop

communication on the link layer [19]. Therefore, the support of multi-hop communication will allow the two devices which come from different WPANs to communicate with one another through a transit device. Therefore, in such form of communication, the sender is the originator whereas the recipient is the final destination. In cases whereby the communication devices have been installed across different WPANs and as a result, the multi-hop communication occurs, it is imperative to specify the particular place where the WPAN devices belong. The information regarding this is only in the IPv6 addresses and in turn, the IPv6 header has compression in the multi-hop communication such that the IPv6 address will not be present in the compressed IPv6 header thus the need to be transmitted in a particular manner. Therefore, the 6LoWPAN describes the aspect of adapting the Internet Protocol IPv6 to the LR-WPAN based on the IEEE standards [18]. In this case, the most critical aspect of the adaptation of the IPv6 for application in the LR-WPAN will be the compression of IPv6 packet as well as the fragmentation of the bigger ones. As a result, the technical development relevant to the 6LoWPAN is coordinated through Working Group Glo, an IPv6 over Networks of Resource-constrained Nodes.

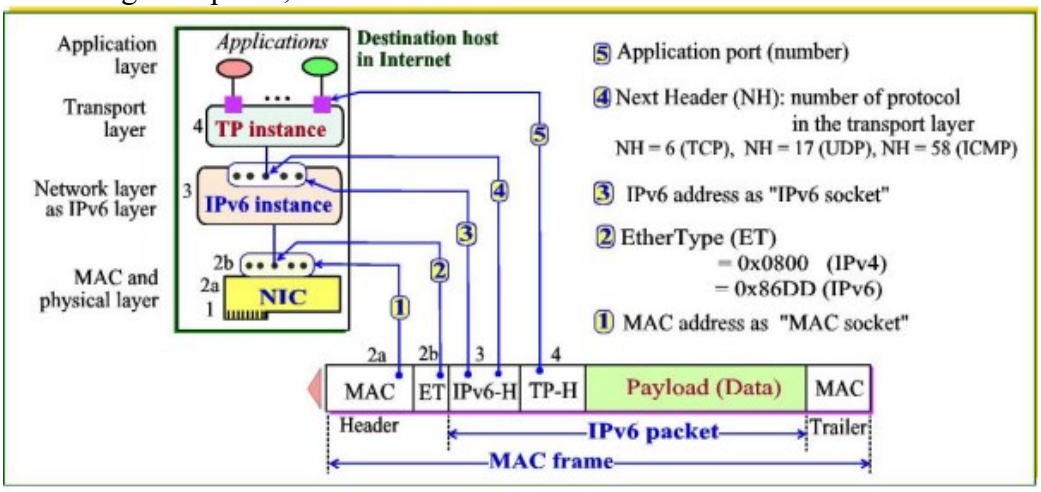

Fig. 3. Visual interpretation of the host address [18]

5 RPL protocol's Sigma routing metric

Considering that the development and advancement of technology are always growing and it guarantees the circulation of smart technology, there are more devices and their numbers will keep on growing to have an internet connection. As a result, this has caused the growth of the Internet of Things as well as the Low Power and Lossy Networks (LLN) [20]. For the IoT, it is an aspect whereby every device can be connected to the internet thus allowing people to have access at their convenience as long as there is an internet connection. Therefore, the IoT is based on the application of wireless sensor network and in turn, it was used to the concept of smart cities thus enabling them to come up with various technological solutions which can solve different challenges faced in a particular industry [21]. In the recent past, there has been a growing interest in research as well as experiments surrounding the wireless sensor networks more so in the IPv6 for the consumption of low power and high rates of packet loss [22]. Therefore, the wireless network community has been researching new routing protocols which can be suitable in different cases, but majority of these protocols need energy and Quality of Services (QoS) whereby they have been using aggressive techniques and standards for battery autonomy, the network lifetime, the link quality, as well as the QoS the users get. Consequently, in our society today, there is an increasing need for quick access to different kinds of information that is offered by the internet hence the need to stress on LLN with link state quality.

The main challenge of RPL within LLN is the issue of security considering how several vulnerabilities of sensor networks tend to make their transition into the IoT more so RPL such

as HELLO Flood, Clone ID, and Sinkhole which take place through intruder nodes. Therefore, it is important to be careful because the majority of the IoT devices could be having vulnerable operating systems to other forms of attack such as Android [23]. Therefore, the majority of the industries such as Microchip, Atmel, and Cisco are using the tested RPL for their products hence getting positive outcomes [24]. These companies have made RPL available for the public; hence the reason why it is easy to conduct tests in real IoT situations with the RPL protocol. Moreover, these manufacturers have risked and utilized ContikiOS to be the operating system for their devices inclusive of the RPL protocol since there is also an implementation of RPL among the open source operating systems such as Linux. Nonetheless, it is crucial to consider that the implementation of RPL in ContikiOS has offered more opportunity for improvement [20]. This implementation has issues, and as a result, it is not wholly based on the explanation given in the RFC 6550 hence the reason most organizations believe that there are various issues which have to be tested and improved in order to develop the RPL in the IoT to its full capacity.

Across such networks, it is challenging to have the route. Hence the reason why most researches and global standardization organization have focused on this matter by having a direct lead on the design of routing protocol IPv6 for LLN known as IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) that has been standardized by IETF hence presenting itself as the central part in the LLN [25]. The RPL is based on distance vector, and it is made up of two forms of nodes in an RPL network which are the sink or receiver nodes which gather information across the network, the issuer node or the origin which gathers data from sensors in order to send them to the sink node. Moreover, the RPL applies the concept of Destination-Oriented Directed Acyclic Graph (DODAG) in defining its topology. The DODAG is developed in a downward construction from the sink node by using DIO messages which have information such as the root node identifier as well as the objective function which is applicable during the selection of the parent of each node. Therefore, it is worth mentioning that the LLN network has had an immense development as well as the capacity to be used in IoT hence justifying the attention they have had from various manufacturers who have invested in various technologies which facilitate the association between various devices, nodes, within the data link level [25]. As a result, these technologies leverage the highest advantage of IPv6 address considering that each node has its IP address hence asserting that the LLN will be scalable rapidly thus making the RPL protocol to be the main piece of development.

6 Risk scenarios

Some of the common risk scenarios in an industrial setting include a vast range of cyber attacks such as when an attacker installs programs that are malicious to the system and as a result manages to block every form of logistics and production operations. The productions, as well as the capacity application, are usually scrutinized thus allowing the application and system data to be controlled. In such a case, the worst-case scenario will involve a misdirected machine which can result in physical damages throughout its vicinity [26]. Another case scenario is when the commands for the industrial robots are sent through an implanted system that is linked with a programmed logic controller which is connected with the internet. As a result, in such a situation, the attacker can be able to install his or her data packets which have the capacity of sabotaging the production line of a given industry or the entire organization's IT infrastructure as well as read various system and application data. The third scenario is in the social engineering sector whereby the attackers will take advantage of the human attributes like trust, helpfulness, fear, and curiosity in compelling the employee such that they can gain entry or access into the organization's data by evading various security contingencies or installing malicious applications on their devices [27]. Overall, their objective is to have an undisturbed time while they go unnoticed into the network of the company.

Therefore, cyber security will pose a risk in industrial organizations and as much as it is still connected with the classic network and computer security point of view. There are various features which can be affected such as the sharing of data through a Digital Supply Network (DSN) which correlates with increased access to data and information for more stakeholders as well as vendor's agreement and payment within a large market [28]. Moreover, some of the new cyber issues have been developed through connected production. Moreover, some of the manipulated and misused requests for extemporary production lines can cause loss of finance, diminished quality of a product, as well as the safety of the industry's workers. As a result, the targets within a smart industry will mainly focus on the presence as well as the integrity of the physical processes instead of information confidentiality as it is with the conventional cyber risks. Therefore, in the age of Industry 4.0 and Industry 5.0 has gone beyond the manufacturing and supply network and it is at the product section [29]. Consequently, as the product continues to have an increased connection, sometimes to one another whereas in other times to the manufacturer as well as the supply network hence making the cyber risk not to end once the product has been sold.

When objects are connected, they will pose more risk level. Since some of the IoT devices have immense cyber risks, and as a result, the security implications within the compromised device would entail damage to facility or equipment and cause downtime for production hence resulting in disastrous failure of equipment and even in extreme cases, it would result in loss of life [30]. Moreover, there are cases where capital is lost, and in turn, it shows that the damages of such cyber attacks are not only limited to case remediation and production downtime and as a result it can span beyond the litigation expenses, fines, as well as loss of revenue from the damages a brand undergoes during an attack [31]. The IoT devices which have been characterized to be producing some of the most important and sensitive cases within an industry are usually the most susceptible devices which are found within a network since it will be attracting interests from various hackers and their respective cyberattacks. As a result, it is imperative for industries to have contingency plans and integrate the basic strategies which can safeguard their devices. It is important to note that the overall nature of cyber risks within the industries usually depend on specific portfolio within the organization hence the need to have sufficient action from the associated automated decision-making aspects [32]. Nonetheless, since various rules and controls regulate industrial production, cyber risks should also remain a major concern for the regulators.

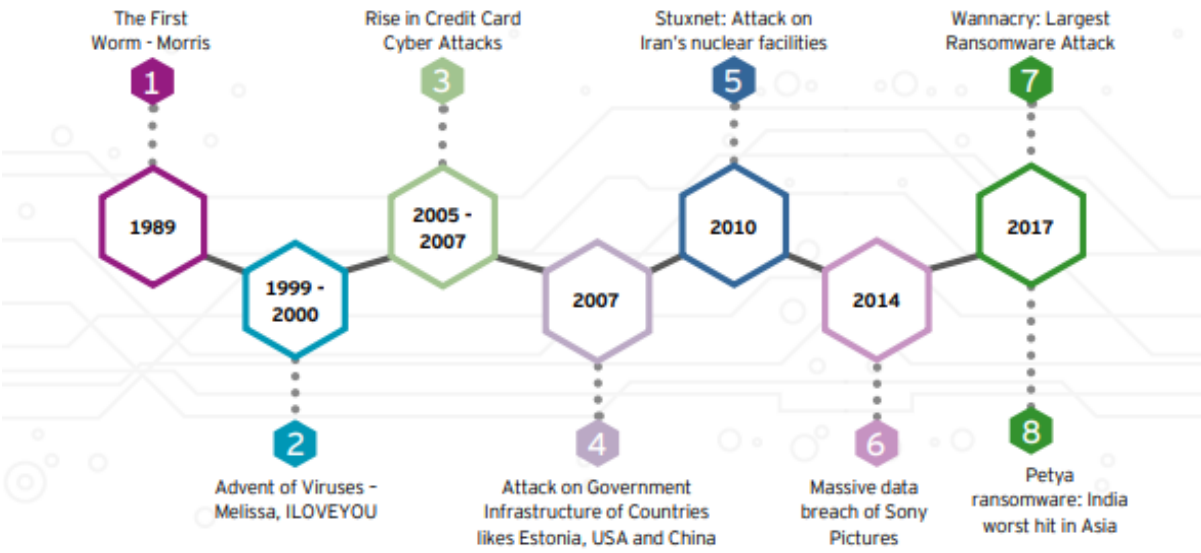

Fig. 4. History of Cyberattacks [33]

7 The future works in Cyber security

The cyber domain is a multifaceted sector considering how it has amalgamated different professions by being relevant in almost every industry since it entails various aspects such as the process of networking online devices together as well as creating a platform which gives people the chance to interact with these devices and in the long it reveals how these devices have influenced different components of their lives [34]. Therefore, it is worth mentioning that the cyber paradigm is crucial as it has managed to influence almost every aspect of the contemporary life such as healthcare, powering homes, transportation and other million things people do in their day to day lives [35]. As time goes by, the number of connected devices and their usage will be rising, and as a result of this, the convolution of cyberinfrastructure will exponentially increase. However, as these numbers increase, another major problem associated with the issue is that more vulnerable devices will emerge from this phenomenon hence the need to have a cyber security workforce which will underpin the developing cyberinfrastructure hence protecting the networks [36]. Consequently, with the inception of cyber security and how this issue is pivotal in maintaining the integrity of the cyberspace for many industries, there has been a growing need and demand for the development of various cyber security workforces and the pertinent framework which can offer some of the crucial roles of the cyber workforce.

8 Conclusion

The architects of the conventional cyber security entail security mechanisms which will offer services such as authenticity, access control, confidentiality, non-repudiation, as well as integrity. Therefore, having these mechanisms in place will be critical in preventing attack and intrusion into a particular network or computer. However, in the contemporary industries whereby the modern internet is taking over in an overarching fashion, the landscape of these modern industries is attributed by attacks which can be characterized to be continually changing, voluminous, persistent, highly sophisticated and super fast. Therefore, having such attributes in a cyber threat shall increase the challenge on various preventive measures. In today's world, the Industry 4.0 and Industry 5.0 are the defining factors in almost every aspect people indulge in today such as automation of systems through cloud computing, cognitive computing, the Internet of things, as well as cyber-physical systems [37] [38].

Moreover, Industry 5.0 is characterized by adding unmatched and synchronous advancement into the digital space with the introduction of robotics, machine learning, artificial intelligence, virtual and augmented reality, nanotechnology, wearable technology, quantum computing, biotechnology, and additive manufacturing. Both Industry 4.0 and 5.0 have been crucial in development but there are various operational risks which have developed as a result, and it is an issue for the connected smart industries and the digital supply networks. The association in these industries which drive operations and set the pace for digital development means that cyber security will be the central issue of concern. This is because in case of a cyber attack, the effects can be extended to the extent that the industrial value chain may fail to mitigate the issue on time since they are not ready for such risks. Therefore, in this age of the Industry 4.0 and 5.0, it is crucial to address the cyber risks by well-developed cyber security strategies which have to be vigilant, secure, and persistent with full integration into the IT and organizational strategies. Therefore, security and safety when someone is using the internet and other digital technologies are some of the critical aspects which have an immense concern or majority of the industries which have digitized their operations. This is because the combination between usability and cyber security are related hence the need to have a secured platform whereby the activities and objectives of a given industry cannot be affected by some of the contemporary cyber threats.

References

[1] P. B. Santos, F. Charrua-Santos and T. M. Lima, "Industry 4.0: An Overview," in *Proceedings of the World Congress on Engineering 2018 Vol II*, London, UK, 2018.

[2] B. C. Ervural and B. Ervural, "Overview of Cyber Security in the Industry 4.0 Era," in *Industry 4.0: Managing The Digital Transformation*, Cham, Switzerland, Springer, Cham, 2018, pp. 267-284.

[3] O. S. Kamel and N. Hegazi, "A Proposed Model of IoT Security Management System Based on A study of Internet of Things (IoT) Security," *International Journal of Scientific and Engineering Research,* vol. 9, no. 9, pp. 1227-1244, 2018.

[4] V. Özdemir and N. Hekim, "Birth of Industry 5.0: Making Sense of Big Data with Artificial Intelligence, "The Internet of Things" and Next-Generation Technology Policy," *OMICS.,* vol. 22, no. 1, pp. 65-76, 2018.

[5] C. Roser, "https://www.allaboutlean.com/industry-4-0/," December 2015. [Online]. Available: https://www.allaboutlean.com/industry-4-0/industry-4-0-2/. [Accessed March 2019].

[6] A. Toma, R. Constantinescu and R. Zota, "Enhancing Administrative Services through Document Models," in *The Proceedings of the 5th international conference Knowledge Management: Projects, Systems and Technologies*, Bucharest, 2010.

[7] G. Tinică, V. Bostan and V. Grosu, "The dynamics of public expenses in healthcare and demographic evolution in Italy and Romania," *Revista Romana de Bioetica [Romanian Journal of Bioethics],* vol. 6, no. 3, pp. 56-63, July – September 2008.

[8] P. Sanmartin, A. Rojas, L. Fernandez, K. Avila, D. Jabba and S. Valle, "Sigma Routing Metric for RPL Protocol," *Sensors,* vol. 18, no. 4, p. 1277, 2018.

[9] R. Waslo, T. Lewis, R. Hajj and R. Carton, "Industry 4.0 and cybersecurity: Managing risk in an age of connected production," 21 Mar 2017. [Online]. Available: https://www2.deloitte.com/insights/us/en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html.

[10] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy," *Journal of Advanced Research,* vol. 5, no. 4, pp. 491-97, 2014.

[11] Z. M. King, D. Henshel, L. Flora, M. Cains, B. Hoffman and C. Sample, "Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment," *Frontiers in Psychology,* 05 Feb. 2018.

[12] G. L. Brase, E. Vasserman and W. H. Hsu, "Do Different Mental Models Influence Cybersecurity Behavior? Evaluations via Statistical Reasoning Performance," *Frontiers in Psychology,* vol. 8, no. 1929, November 2017.

[13] G. A. Fine, "Group culture and the interaction order: local sociology on the meso-level," *Annual Review of Sociology,* vol. 38, p. 159–179, 2012.

[14] J. Fluck, "Why do students bully? An analysis of motives behind violence in schools," *Youth Sociology,* vol. 49, p. 1–21, 2014.

[15] Z. DeSmit, A. U. Kulkani and C. Wernz, "Enhancing Cyber-Physical Security in Manufacturing through Game-Theoretic Analysis," *Cyber-Physical Systems,* 2018.

[16] S. Gil, A. Kott and A. L. Barabási, "A genetic epidemiology approach to cyber-security," *Scientific Reports,* vol. 4, p. 5659, 2014.

[17] F. Tariq, M. R. Khandaker, K. Wong, M. Imran, M. Bennis and M. Debbah, ", M., Bennis, M., & Debbah, M. (2019). A Speculative Study on 6G. CoRR, abs/1902.06700.," *IEEE Communications Magazine,* vol. XX, no. X, pp. 1-7, 2019.

[18] A. Badach, "Protocol structure of 6LoWPAN devices," September 2017. [Online]. Available: https://www.researchgate.net/publication/320003101_Protocol_structure_of_6LoWPAN_devices.

[19] T. Fredriksson and N. Ljungberg , "Security in low power wireless networks: Evaluating and mitigating routing attacks in a reactive, on demand ad-hoc routing protocol," 2017.

[20] W. Xiao, J. Liu, N. Jiang and H. Shi, "An optimization of the object function for routing protocol of low-power and lossy networks," in *Proceedings of the 2014 2nd International Conference on Systems and Informatics (ICSAI)*, Shanghai, China, 2014.

[21] J. P. J. Peixoto and D. G. Costa, "Wireless visual sensor networks for smart city applications: A relevance-based approach for multiple sinks mobility," *Future Generation Computer System,* vol. 76, p. 51–62, 2017.

[22] L.-M. Ang, K. P. Seng, A. M. Zungeru and G. K. Ijemaru, "Big Sensor Data Systems for Smart Cities," *IEEE Internet of Things Journal,* vol. 4, no. 5, pp. 1259 - 1271, October 2017.

[23] Hellman, F. and Hellmann, P., "Implications of vulnerable internetconnected smart home devices," 2018.

[24] J. Park, K. Kim H. and Kim, K., "An Algorithm for Timely Transmission of Solicitation Messages in RPL for Energy-Efficient Node Mobility," *Sensors (Basel),* vol. 17, no. 4, p. E899, 2017.

[25] H. Kim, J. Ko, D. Culler and J. Paek, "Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey," *IEEE Communications Surveys & Tutorials,* vol. 19, no. 4, pp. 2502 - 2525, 2017.

[26] V. Fernandez-Anez, G. Velazquez, F. Perez-Prada and A. Monzon, "Smart City Projects Assessment Matrix: Connecting Challenges and Actions in the Mediterranean Region," *Journal of Urban Technology,* 2018.

[27] L. Urciuoli, T. Mannisto, J. Hintsa and T. Khan, "Supply Chain Cyber Security - Potential Threats," *Information & Security: An International Journal,* vol. 29, pp. 51-68, 2013.

[28] P. Liddell, G. Archibald and S. Pyke, "Digital Supply Chain - the hype and the risks," 19 February 2018. [Online]. Available: https://assets.kpmg/content/dam/kpmg/au/pdf/2018/digital-supply-chain-hype-and-risks.pdf.

[29] J. Boyens, "Integrating Cybersecurity into Supply Chain Risk Management," RSA Conference 2016, San Francisco, 2016.

[30] F. Schluter, K. Diedrich and M. Guller, "Analyzing the Impact of Digitalization on Supply Chain Risk Management," in *26th IPSERA Conference*, Budapest/Balatonfured, 2017.

[31] E. Park, P. A. del Pobil and S. Kwon, "The Role of Internet of Things (IoT) in Smart Cities: Technology Roadmap-oriented Approaches," *Sustainability,* vol. 10, no. 5, pp. 1-13, 2018.

[32] M. L. Gyorffi, "Digitising Industry (Industry 4.0) and Cybersecurity," *European Parliament: Industry, Research And Energy (ITRE),* p. 12, November 2017.

[33] Ernst & Young, "Cybersecurity for Industry 4.0: Cybersecurity implications for government, industry and homeland security," 31 Aug 2018. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-for-industry-4-0/$File/ey-cybersecurity-for-industry-4-0.pdf. [Accessed February - April 2019].

[34] J. Dawson and R. Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance," *Frontiers in Psychology,* 2018.

[35] Z. Li and M. Shahidehpour, "Deployment of cybersecurity for managing traffic efficiency and safety in smart cities," *The Electricity Journal,* 2017.

[36] N. Buchler, C. G. La Fleur, B. Hoffman, P. Rajivan, L. Marusich and L. Lightner, "Cyber Teaming and Role Specialization in a Cyber Security Defense Competition," *Frontiers in Psychology,* vol. 9, pp. 21-33, November 2018.

[37] R. D. ZOTA and I. A. PETRE, "An Overview of the Most Important Reference Architectures for Cloud Computing," *Informatica Economică,* vol. 18, no. 4, pp. 26-39, 2014.

[38] M. DOINEA and P. POCATILU, "Security of Heterogeneous Content in Cloud Based Library Information Systems Using an Ontology Based Approach," *Informatica Economică,* vol. 18, no. 4, pp. 101-110, 2014.

[39] M. Kantarcioglu and E. Ferrari, "Frontiers in Big Data," 14 Feb. 1019. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fdata.2019.00001/full.

Antonio CLIM has graduated the Faculty of Food Science and Engineering at the University of Galati in 1996. In 2017 he has been admitted as Ph.D. candidate at the Bucharest University of Economic Studies in the field of Economic Informatics. His research interests include Business Informatics, Computer Networks and Smart Cities. Currently he is Teaching Assistant at Faculty of Cybernetics, Statistics and Economic Informatics from the Academy of Economic Studies. His work focuses on the security and analysis of machine-learning applications for health services.