SECURITY EVALUATION OF INDUSTRY 4.0: UNDERSTANDING INDUSTRY 4.0 ON THE BASIS OF CRIME, BIG DATA, INTERNET OF THING (IoT) AND CYBER PHYSICAL SYSTEMS

Emre Cihan ATEŞ[*], Erkan BOSTANCI[**] , Mehmet Serdar GÜZEL[***]

Abstract

In the past, we all witnessed that the production facilities were shifted to the countries with low employment costs due to the increasing labour costs around the world. Today, especially with the revolution of industry 4.0 initiated under the leadership of the developed countries on the basis of technology, industrial competition is tried to be provided within the framework of productivity and quality by reducing the cost of workmanship. The Industry 4.0 revolution is also defined as intelligent self-coordinating factories almost independently of people.

The entry of Industry 4.0 into our lives is expected to revolutionize many sectors especially information technologies, communication and education. In this context, the subject of crime is also a candidate to be one of the areas of change because the profitable gain structure of the Industry 4.0 environment is expected to be one of the factors that motivate criminals to take action in this field. Therefore, the industrial revolutions were aimed to be examined in terms of security, internet of things and big data with this study conducted.

In the analysis performed, it is clear that Industry 4.0, which aims at production maximization, will cause security problems with its current situation. With Industry 4.0, these security issues have become more specific problems and the concept of automation has added new paradigms to security issues and increased the possibility of being a victim of cyber threats. Currently, our industry is between Industry 2.0 and Industry 3.0. Within this scope, it is essential to enhance the technical background of the security teams in order to prevent the crimes that may occur in the future. It is expected that the most appropriate action type of security teams is the security-focused defence understanding. Regarding this understanding, a proactive attitude should be exhibited and it is necessary to use effective methods against cybercriminals. In today's world where the technology changes rapidly, it should be considered that a statical defence understanding cannot be accepted but security teams should adopt a dynamic cybercrime intervention policy in order to fight against new threats.

Keywords: *Industry 4.0, Crime, Internet of Thing (IoT), Security, Big Data, Artificial Intelligence, Cyber-physical Systems.*

[*] Gendarmerie Lieutenant, Lecturer, Gendarmerie and Coast Guard Academy, Turkey, emre_cihan_ates@hotmail.com, ORCID ID: https://orcid.org/0000-0001-9550-4532

[**] Assoc. Prof. Dr., Ankara University, Faculty of Engineering, Turkey, erkan.bostanci@ankara.edu.tr, ORCID ID: https://orcid.org/0000-0001-8547-7569

[***] Assoc. Prof. Dr., Ankara University, Faculty of Engineering, Turkey, mguzel@ankara.edu.tr, ORCID ID: https://orcid.org/0000-0002-3408-0083

Makale Geliş Tarihi: 28.10.2019 Makale Kabul Tarihi: 02.01.2020

ENDÜSTRİ 4.0'IN GÜVENLİK DEĞERLENDİRİLMESİ: ENDÜSTRİ 4.0'I SUÇ, BÜYÜK VERİ, NESNELERİN İNTERNETİ VE SİBER FİZİKSEL SİSTEMLER TEMELİNDE ANLAMAK

Öz

Dünya üzerinde işgücü maliyetlerinin artmasıyla birlikte üretim tesislerinin işçilik maliyeti düşük olan ülkelere kaydırıldığına geçmiş zamanlarda hepimiz şahit olduk. Günümüzde özellikle, teknoloji temelinde gelişmiş ülkeler öncülüğünde başlatılan endüstri 4.0 devrimiyle birlikte, söz konusu işçilik maliyeti düşürülerek üretkenlik ve kalite çerçevesinde endüstriyel rekabet sağlanmaya çalışılmaktadır. Endüstri 4.0 devrimi, neredeyse insanlardan bağımsız olarak kendi kendini koordine eden akıllı fabrikalar olarak da tanımlanmaktadır.

Endüstri 4.0'ın hayatımıza girmesiyle birlikte; bilgi teknolojileri, iletişim ve eğitim başta olmak üzere birçok sektörel alanda devrim yaşanması beklenmektedir. Bu kapsamda, suç alanı da söz konusu değişim alanlarından biri olmaya aday konumdadır. Çünkü Endüstri 4.0'ın ortaya çıkaracağı kârlı kazanç yapısı, suçluları da bu alanda harekete geçmeye motive eden unsurların başında gelmesi beklenmektedir. Yapılan bu çalışma ile Endüstri 4.0'ı anlayarak, mevcut endüstriyel devrimlerin; güvenlik, nesnelerin interneti ve büyük veri açısından incelenmesi amaçlanmıştır.

Yapılan incelemede, üretim maksimizasyonunu amaç edinen endüstri 4.0'ın, mevcut haliyle güvenlik sorunu doğuracağı ortadadır. Endüstri 4.0 ile birlikte, güvenlik sorunlarının çok daha spesifik hale gelmesi ve otomasyon kavramının güvenlik sorunlarına yeni paradigmalar eklemesi, genel anlamda siber tehdit mağduriyetini arttırmıştır. Halihazırda sanayimiz Endüstri 2.0 ile Endüstri 3.0 arasındadır. Bu kapsamda, gelecekte olması muhtemel suçların önlenmesi için güvenlik güçlerinin şimdiden teknik altyapılarını olgunlaştırmaları şarttır. Güvenlik güçleri için en uygun hareket tarzının, güvenlik odaklı savunma anlayışı olması beklenmektedir. Bu anlayış çerçevesinde, proaktif tutum sergileyerek; siber suçlulara karşı etkin yöntemlerin kullanılması gerekliliktir. Teknolojinin hızla değiştiği günümüzde, statik bir savunma anlayışının kabul edilemeyeceği, güvenlik güçlerinin her zaman yeni tehditlere karşı koyabilecek, dinamik bir siber suçla mücadele politikası benimsemesi gerektiği değerlendirilmektedir.

***Anahtar Kelimeler**: Endüstri 4.0, Suç, Nesnelerin İnterneti, Güvenlik, Büyük Veri, Yapay Zeka, Siber-Fiziksel Sistemler.*

INTRODUCTION

Throughout history, human beings have constantly changed their life habits. The changing items were behaviours, habits, goods, houses, etc., which were always described as better. In every progress in the life cycle of humanity, the old deeds were seen as more primitive and evil. In fact, this understanding can be explained by the saying "doing more with less." As a series of researchers aiming at this aphorism invented the machines that used water and steam power in England in the 18th century, the transition from the agriculture and handicrafts-

based economy, which can be called as primitive, to industry-based production was realized (Harley, 2018). On the basis of mechanization, the transition to industrial production spread to the whole world in time, and this was followed by the development of the so-called 1st Industrial Revolution (Industry 1.0). After 1870, mechanical productions became faster with the support of electrical energy and the period called the second industrial revolution (Industry 2.0) was entered (Klingenberg and Do Vale Antunes, 2017; Stearns, 2018). As a result of the widespread use of electronic and automation systems as of 1969, labour costs were further reduced and the third industrial revolution (Industry 3.0) emerged (Stearns, 2018).

The existence of industrial manufacturing is an absolute part of every economy. Since the evolution of industrialization, the industry has experienced quite different technological changes, aiming at profit maximization. Today's economy has begun to face a new industrial revolution triggered by political, technological, economic and social changes, which is defined as the 4th industrial revolution (Industry 4.0) (Morrar, Arman and Mousa, 2017). As shown in Figure 1, the complexity of the event increases with each time-related industrial revolution. With Industry 4.0, many new technologies that are pioneers in different disciplines will start to be used together (Klingenberg and Do Vale Antunes, 2017).

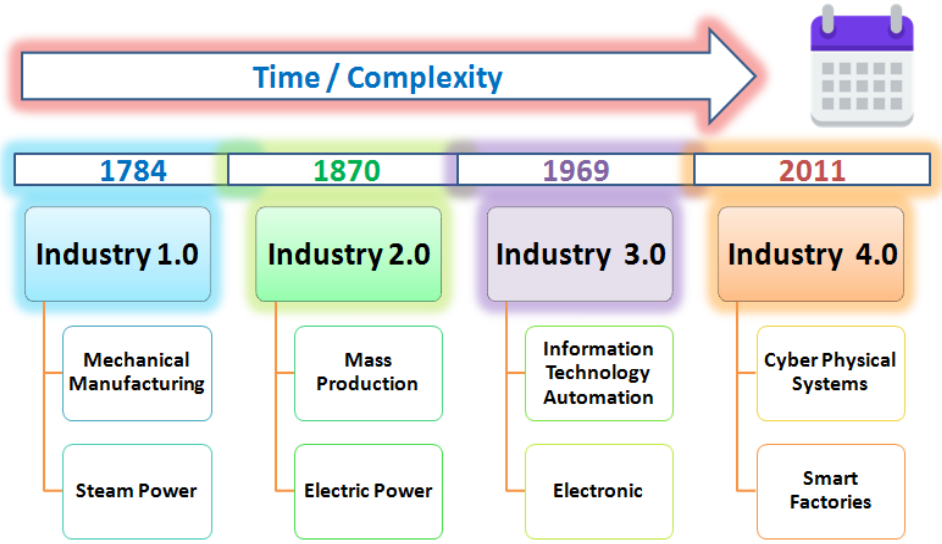

Figure-1. Time-Based Changes of Industrial Revolutions

The concept of Industry 4.0 is also defined as “smart factory" (Chen, Wan, Shu, Li, Mukherjee and Yin, 2017; Hozdić, 2015; Wang, Wan, Li and Zhang 2016) and the smart factories are expected

- To be a virtual replica of the physical world,

- Developing decentralized decision-making processes,

- All physical systems are expected to be able to communicate and cooperate with each other and people in real-time through the “Internet of Things”.

1. UNDERSTANDING INDUSTRY 4.0

The basic element in understanding Industry 4.0 is to determine why the current society and industrial order need a change. The origin of the rising paradigms of the change put forward in this context was laid in 2011. Many of the world's major economies of the past, including Germany, the USA and France, which are known for their success in industry and production, began to suffer economic defeat against China, which is the rising star of the Asian market (Wübbeke and Conrad, 2015). The low labour costs in some densely populated countries, especially China, are the main factors that render competition difficult. In addition to the existing labour costs, the fact that the age average of the world population has been increasing and the population growth rate has been decreasing gradually in many countries in the world, foremost being European countries, comprise many risk factors for industry and production for the near future (Stearns, 2018).

The first step towards changing this order that emerged was taken in 2011 at the Hannover Fair in Germany (Vogel-Heuser and Hess, 2016). The term “Industry 4.0" emerged as the strategy of decreasing competition with overseas countries and differentiating the industries of Germany and the European Union from other international markets. In this context, Germany will start to use new developments such as big data, internet of things and machine learning actively in the future productions for the sake of increasing competitive power by decreasing costs.

The main idea of Industry 4.0 is to connect cyber-physical systems (CPS), i.e. embedded actuators, sensors and microcomputer networks, to the value chain of machines (Vogel-Heuser and Hess, 2016). It is characterized by being able to restructure products by developing them digitally as well as personalized products and a well-coordinated combination of products and services (Lee, Bagheri and Kao, 2015). To put it differently, the industry 4.0 system is a centralized and

automation-oriented form of production that minimizes the difference between the real and the virtual world by using modern information technologies, thereby keeping human intervention and labour-power to a minimum (Figure 2) (Monostori et al., 2016).

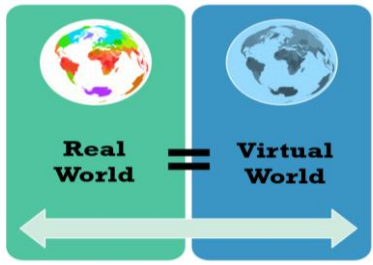

Figure-2. Reality in Cyber-Physical Systems

Cyber-physical systems (CPS) used in Industry 4.0 are likely to become one of the most important technological developments in the near future. When examined in general, these are systems in which the inputs learned by the computer are increased to maximum efficiency with machine learning and artificial intelligence and which comprise a physical environment controlled by the computer software and the software in question (Chen, 2017; Chiu, Cheng and Huang, 2017; Lee, Bagheri and Kao, 2015). The systems, as shown in Figure3, focus on (3C) computerization, inter-system communication and control of input and output (feedback loop) (Liu et al., 2017, Wan et al., 2011). Many of the systems we use today, which we call “intelligent production systems", are generally focused on the logic of continuing the same process singularly and continuously, which is also the distinguishing aspect of cyber-physical systems.

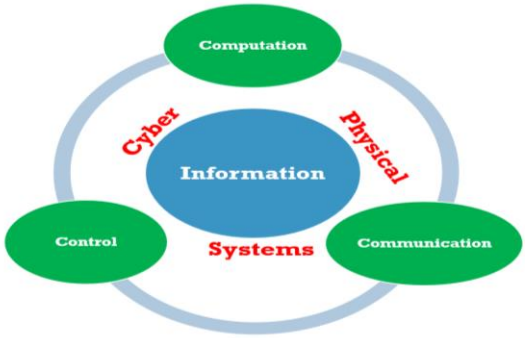

Figure-3. The Cycle of Cyber-Physical Systems (3C)

With the new cyber-physical systems put forth, the production equipment aims to improve the production process by maintaining communication with each other and employees. From this point of view, since the information processing speed of computers is much faster than the people, the aim was to get the products and the equipment that provides the production to communicate with each other (Liu et al., 2017).

In the report published by Boston Consulting Group with the title "Industry 4.0: The Future of Productivity and Growth in Manufacturing," regarding the identification of areas that Industry 4.0 will revolutionize, the nine different transformation technologies where Industry 4.0 was defined were put forth, as shown in Figure 4 (Rüßmann et al., 2015).

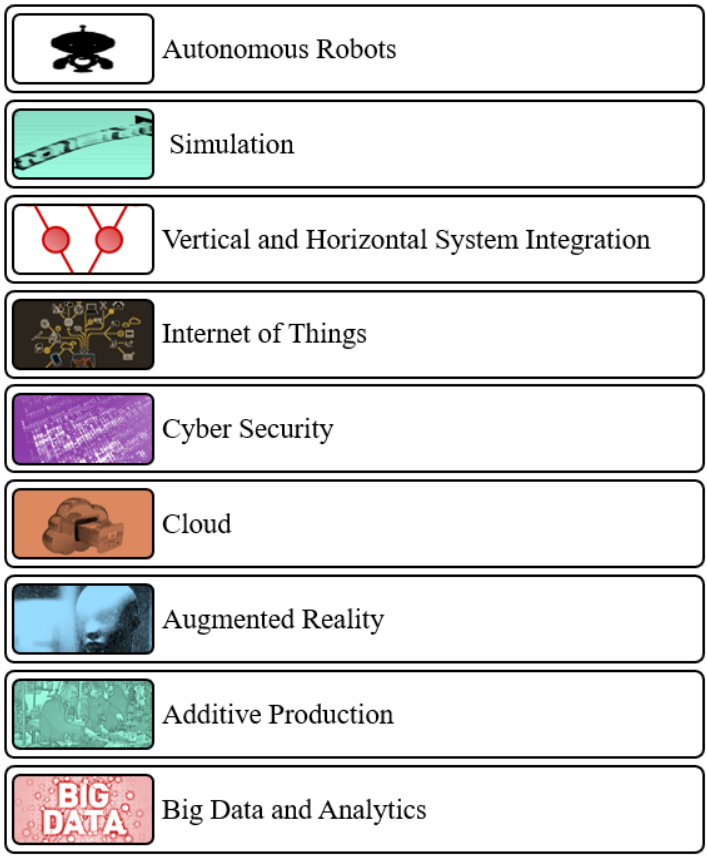

Figure-4. Nine Transforming Technology in Industry 4.0

When the transformation technologies mentioned in Figure 4 are examined, it is seen that;

- Thanks to autonomous robots, productivity will increase as the cost will decrease in the manufacturing industry. Furthermore, the robots will be able to work more autonomously and flexibly (Rüßmann et al., 2015).

- With the simulation systems, it will be possible to simulate factory, machine and products in a virtual model over real-time data. Products simulated in a virtual environment will reduce cost after testing and optimization (Schluse et al., 2018).

- Vertical and horizontal system integration is aimed with industry 4.0, and horizontal integration will establish a network connection between machines and equipment. With vertical integration, it will be possible to control different parts of the supply chain (Vaidya et al., 2018).

- With the "Internet of Things" technology, the communication of machines used in production with each other and with central control devices will be increased, and productivity will be ensured (Hozdić, 2015).

- With the concept of cybersecurity, it will be possible to protect machines and systems defined in networks within the scope of industry 4.0 against cyber attacks (Rüßmann et al., 2015; Nguyen et al., 2019).

- Cloud systems will facilitate access to all machinery and production equipment by providing data storage over the network. Their speeds will decrease down to milliseconds of reaction time, and their functionality will gradually increase (Aljawarneh, Alawneh and Jaradat, 2017).

- It will be possible to perform various services such as augmented reality-based systems, selection of parts in a warehouse and sending repair instructions to mobile devices. In addition, the creation of the replica of the physical environment in the virtual environment will reduce costs (Paelke, 2014).

- The added production will especially be used in the production of three-dimensional printers and customized products. It will be actively used to make the prototype of and produce the components in production (Rüßmann et al., 2015).

- A comprehensive evaluation by collecting data from many different sources with big data and data analytics will become the standard to support real-time decision making (Jin, Wah, Cheng and Wang, 2015).

In this study, which aims to analyze the new transformation environment that will be revealed by the concept of Industry 4.0, it is aimed to examine the concepts of the internet of things and big data, which are among the mentioned transformation areas, in terms of cybersecurity. In this context, the internet of things and big data concepts will be described in detail in the first part of the study.

1.1. Big Data and Analytics

The concept of big data is the data collection structure that emerges with the loops of event that we encounter every day and which does not make sense in the instant view (which can provide access to meaningful information through analysis). The data is meaningful only when evaluated. In other words, we can describe the data as precious metals in piles of rocks, waiting to be extracted (Yin and Kaynak, 2015).

We are in a system where almost everything we encounter in the modern age is based on data. Therefore, in order to better define the concept of big data, we should examine the 5V (Volume – Variety – Velocity – Verification - Value) rule which is accepted in the literature and defines the big data (Figure 5) (Jin et al., 2015; Mayer-Schönberger and Cukier, 2013);

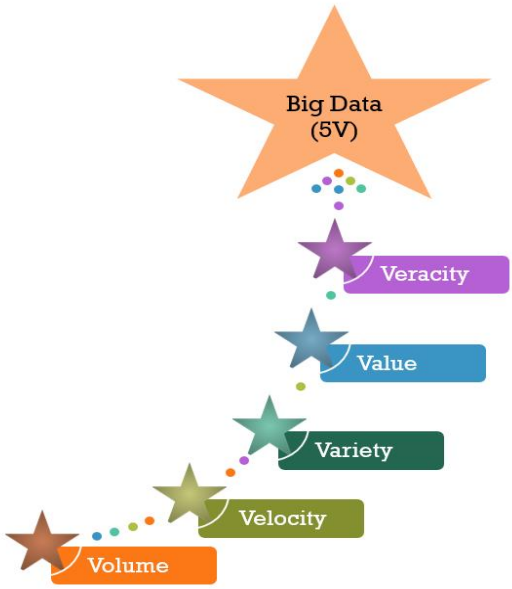

Figure-5. 5V Rule in Big Data

- Volume refers to the continuously increasing amount of data. Increase in the amount of data will make it difficult to access meaningful information from big data (Jin et al., 2015).

- Variety refers to the fact that the majority of the data constituting the big data is produced in different non-structural environments and formats. Analysis of data received from different formats and sources will also be more difficult and different from classical methods (Assunção, Calheiros, Bianchi, Netto and Buyya, 2015).

- Velocity refers to the data, the growth rate of which continuously increases. Big data is structures in which the data increases continuously.

- Verification of the data refers to the protection of the data obtained by high-level security measures and the impossibility to modify it by unauthorized interventions (Jin et al., 2015).

- Value defines the transformation of data into meaningful information by the evaluations that will be made from within the big data and its backing up decision support units (Assunção et al., 2015).

The increase in data volume together with the concept of big data leads to the problem of relativity and complexity of information. Therefore, it is becoming more and more important that accurate data that is analyzed correctly can be put forth. Big data in industrial terms are important in areas such as product and market development, operational efficiency, decision making, market demand forecasts and customer experience.

The industrial structure put forth by Industry 4.0 suggests a predictive production model (Bendel, 2015). In smart factories, machines are interconnected as a common community, and production is customer-oriented and flexible. Such a structure increases the importance of prospective forecasts. Forecasting is possible by analyzing historical data, that is, with the concept of big data. For the industry, this data is generally that which changes manufacturers' perception of value and manufacturing services and includes the production analyses of the previous years. In this decision-making process in industry 4.0, where human labour is minimized, most of the decisions will be made through artificial intelligence systems based on machine learning. Although the concept of artificial intelligence is not at the desired level today, it is considered that depending on the scientific developments to occur in this field, transformation into smarter machines will be provided in the future (Lee, Ardakani, Yang and Bagheri, 2015).

1.2. Internet of Things (IoT) Technology

The “Internet of Things” concept is a term used to refer to an object connected to any network. It can also be defined as a system that can define the physical objects that we see around us and communicate with them. As illustrated in Figure 6, in the “Internet of Things” system, the objects can connect to the network by means of the sensors they have and establish access to the system or database. The concept of the “Internet of Things” is shown as one of the greatest developments in the modern age, because an object that also has a digital identity is in contact with its environment as well as its user.

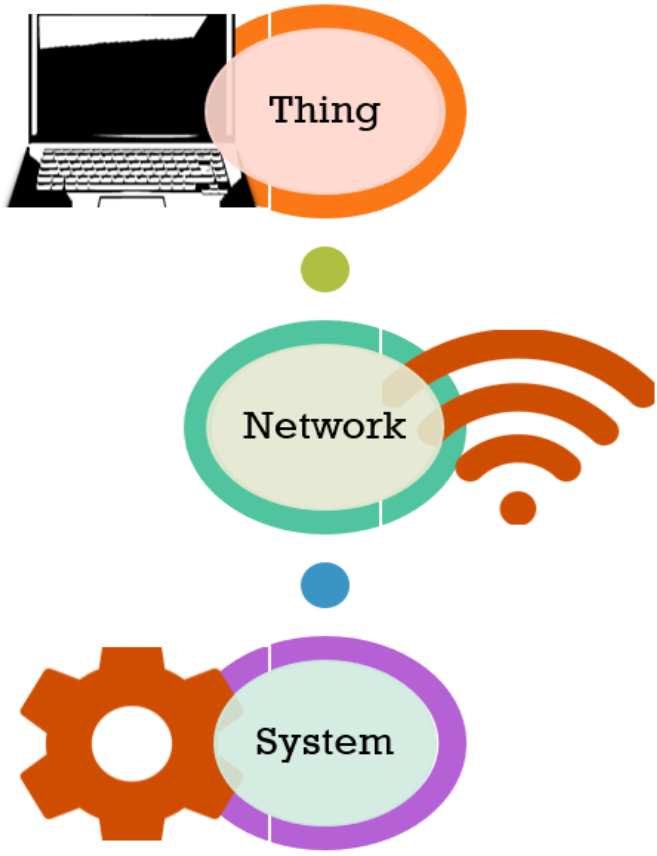

Figure-6. Internet of Things (IoT) Technology

The ability of objects to connect will bring along many positive benefits, especially in the field of production (Botta, De Donato, Persico and Pescapé, 2016; Hozdić, 2015). The following five main "Internet of Things" technologies are widely used for the distribution of network data (Lee and Lee, 2015). The Internet of things technologies in question are defined as radio frequency identification (RFID), wireless sensor networks (WSN), middleware, cloud computing and IoT application software (Hozdić, 2015).

Today we live in a world with more IoT-connected devices in number than people. Devices connected to the "Internet of Things" can communicate with each other over defined networks or cloud-based platforms. Real-time information collected through the "Internet of Things" technology may comprise many different areas, primarily health, security and commercial activities.

2. EVALUATION OF POSSIBLE CRIME AREAS ON SECURITY BASIS

In parallel with the increase in labour costs in developed countries, increasing production costs have set off humanity into a new quest. As the labour costs are high, developed countries have significantly closed the cost gap with productivity and quality in order to be able to compete with the industrial revolution led by Germany (Zhou, Liu and Zhou, 2015).

Together with industry 4.0, as social change is expected in many areas, the area of crime is also a candidate for becoming one of the areas of the social change in question. This is because the profitable earnings structure of the Industry 4.0 environment is expected to motivate criminals to take action in this area (Nguyen et al., 2019). Besides, the resulting crime environment is expected to increase the role of cybersecurity gradually. It is obvious that increasing cybersecurity measures too much will partially reduce the productivity of the factories. In this context, cost-effectiveness analysis is a must for each method to be used in the struggle against crime. The concept of Industry 4.0 will be examined from 7 different perspectives in terms of crime and security in the light of today's changing paradigms (Figure 7). In this study, the aim was to investigate the changes brought about in terms of security by Industry 4.0, which revolutionized information technologies.

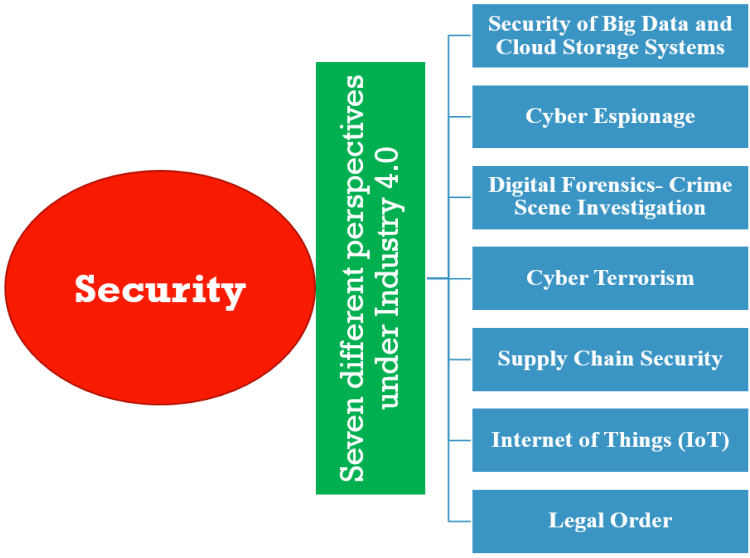

Figure-7. Security Areas in Industry 4.0

2.1. Security of Big Data and Cloud Storage Systems

Today, together with the continuous increase in the amount of data and the ability of machines to communicate with each other thanks to the Internet of Things Technology, the transition of data from singular and closed environment to cloud storage environments has become necessary (Aljawarneh et al., 2017; Yin and Kaynak, 2015). This transition brings about a series of changes in data protection habits in the field of security. Cloud-based data storage in Industry 4.0 should be “highly secure, scalable, and autonomous" (Gubbi et al., 2013).

Cloud storage systems actively use authentication methods as security. The storage areas in question, by duty, allow the processing of the data by storing big data. Cloud storage areas are the centre of the industrial production system, so only the right people should have access to the centre where the information is stored (Botta et al., 2016). Otherwise, all information can be retrieved, changed or destroyed in cyberattacks conducted by competing companies and businesses with different purposes. In this context, measures such as privileged access control, especially through flexible authentication methods, are considered to be highly effective in managing data access. As with the Internet of Things technology, the great increase in security measures leads to the disintegration of the factory's centre of gravity. In this context, it is obvious that cloud storage areas will be re-evaluated within the scope of cost-effectiveness analysis in the near future.

2.2. Cyber Espionage

The main work of cyber espionage is the capture, sabotage and unfair information acquisition of information in virtual environments, especially by malicious hackers (Wangen, 2015). Within the scope of Industry 4.0, information that the manufacturing sector defines as a trade secret is of interest to cyber espionage. Especially with the attack type defined as "Advanced Persistent Threat" (APT) in the literature, unauthorized person / group can access the network, stay unnoticed for a long time and get all the information about production (Wangen, 2015). Cyber espionage is also a threat to factories' research and development (R & D) activities and databases.

Industry 4.0 is, in general, more vulnerable to cyber espionage than conventional manufacturing, because the high number of intelligent and connected business processes increases cyber threats. For Industry 4.0-based manufacturing companies, it is very likely that specific information about the production infrastructure such as product information and technical specifications will be stolen through cyber espionage methods (Taute, 2017). In this context, the Industry 4.0-based production approach creates cost and efficiency while creating a highly open environment for cyber espionage. In the near future, factories are expected to increase their security measures against cyber-espionage activities because it seems unlikely that security forces will take preventive measures in individual and subjective dimensions within the scope of cyber defence.

2.3. Digital Forensics - Crime Scene Investigation

In the classical investigation methods, it is the duty of the security forces to determine the identity of the perpetrators and to lead them to stand before the judicial authorities after the crime has been committed. In this context, the investigation and detection of attacked computer networks and data storage environments require technical knowledge (Thames and Schaefer, 2017). The need for technical information brings along the need for regular training of security forces and the need for personnel to specialize in Industry 4.0-related digital crimes.

Specialized personnel in the current IT field have been trained in order to carry out minor forensic investigations. With Industry 4.0, performing a major forensic examination is essential, given the size of the data. In addition, the ability to perform the related major examination allows security forces to see and inspect all the data of smart factories. At this point, it is necessary to provide a sterilized environment in which security forces will not be attacked by cyber-attacks for the investigation to be conducted in a healthy manner.

In minor forensic investigations, the image of the study data is taken and work is done on the image, which secures the master data. But at a major level, it is now quite difficult and costly to physically take the image of large data, often based on cloud technology. Analyzing data without taking an image involves different risk factors.

2.4. Cyber Terrorism

Cyber terrorism is the attack on computers, networks and information stored therein which include the social and political goals of a government or a people (Al Mazari, Anjariny, Habib and Nyakwende, 2018). It is in the nature of cyber terrorism that the attack creates an impact on society and intimidates people and involves violence. For this reason, critical production facilities are within the target area of cyber terrorism (Gordon and Ford, 2002; Gordon, 2004).

Cyber terrorism is a type of attack in which cybercriminals turn into digital terrorists with political considerations. Since the Industry 4.0 system is built on efficiency, the system is vulnerable to attacks by cyber terrorists because of the low level of network security and the possibility of propaganda in society following the attack. When the targets of cyber terrorism are considered, it can infiltrate critical production facilities for different purposes, foremost being for the purpose of propaganda and destroy the technical structure of information and production or render the information invaluable by sharing this confidential information with others. It is known that existing terrorist groups are actively working on cyber terrorism techniques. There are threat analyses and many academic studies on how the cybersecurity information accessed by ISIS, which has grown in recent years, can create a disaster on critical infrastructures (Hilse, 2014).

2.5. Supply Chain Security

Together with the technology of the Internet of things and the digitalization of the supply chain with the help of sensors (Tjahjono, Esplugues, Ares and Pelaez, 2017);

- Work accidents have been reduced with automatic material circulation,

- With unmanned warehouses operating 24/7 and fast vehicle loading and unloading systems, optimization of warehouse areas and stock management has been ensured,

- And there has been an increase in the profit and productivity ratios of the factories.

With smart factories taking a series of security measures in their own right, many of the biggest security breaches started with a supplier, and mass data were often revealed with information being stolen (Pereira, Barreto and Amaral, 2017). That the criminals enter the supply chain within the scope of industry 4.0 and access the smart factory through rational actors provide more opportunities for cyber-criminals. These attacks usually occur in the form of interfering with the system and destroying data or intentionally modifying it in order to destroy the system.

Attacks by cybercriminals on smart factories can be prevented by using modern cybersecurity measures such as adaptive authentication and behaviour analysis. Furthermore, it is considered that the security system including the simultaneous recording system used in blockchain technology will become ineffective with the development of quantum computers in the near future (Aggarwal, Brennen, Lee, Santha and Tomamichel, 2017).

2.6. Internet of Things (IoT)

The concept of "Internet of Things" refers to the network connection between objects. It is an indispensable part of new business processes that emerged with Industry 4.0. It is a fact that especially the efficiency of production and the quality of people's life will increase together with the distribution of network data in the Internet of Things technology (Hozdić, 2015). However, this system contains a great number of entry points that are potentially exploitable (Vasilomanolakis et al., 2015). Especially IoT devices are known to have security vulnerabilities due to non-cryptographic sending, unsafe web interfaces, low-security software protections, and inadequate authorizations (Lee and Lee, 2015). Devices in IoT generally do not use strong data encryption techniques. Although the security structures used in the devices in the Internet of Things are stronger than conventional wireless network connections, they are not sufficient. Some IoT applications support sensitive infrastructure and strategic services such as smart grids and facility protection (Lee and Lee, 2015). In addition, devices with Internet of Things technology store all kinds of data they receive through their sensors, which will be more valuable than other physical traces in forensic examinations. For example, it will be easier to reach a lot of information such as when and from which source a product offered on the market was taken and which processes it was subjected to.

In our daily life, the problem of privacy will increase with the technology of the Internet of Things, which is becoming widespread in various devices from smartwatches to mobile phones. Although there is a partial resistance to accepting IoT by companies and individuals, especially due to its weaknesses in terms of security and confidentiality, it is still preferred because of its high gains as well as risks. However, it is difficult to say that critical facilities in industrial production are fully protected from cyberattacks before the security problem of IoT is solved. For this reason, it is necessary to take active firewall protections in every object where IoT is active. It is possible to overcome the security problems created by the Internet of Things technology with security measures that generate strong cryptography. The high safety measures cause the centre of gravity to deviate from the efficiency area. Therefore, in the near future, devices with Internet of Things technology are expected to have powerful cryptosystems that can revise themselves continuously.

2.7. Legal Order

The profitable earnings structure revealed by the concept of Industry 4.0 will motivate criminals and bring along new types of crime. In this context, it is necessary to revise the laws in order to fight against new types of crime because one of the most important steps of the fight is the deterrent force of the laws. It is important that laws are revised periodically, just like the type and methods of crime, and that criminal behaviour is defined in the law. With the changes to be made in the law, security forces are required to intervene in a reactive manner and to proactively prevent possible crimes.

The greatest uncertainty in the near future is that there is no universal agreement as to which legislation will be applied if the data within the cloud storage companies operating in different countries are subjected to judicial review. The data on the cloud storage system can be collected on a single server; besides, as opposed to the current order, firms can compartmentalize data and store them on multiple servers as a tactic of defence against cyberattacks (Lillis, Becker, O'Sullivan and Scanlon, 2016). The dispersion of cloud services may require a structure that can involve more than one legal judicial system, as it may sometimes concern more than one state. In this environment, it is still partially uncertain according to which state's laws and regulations the digital traces related to the evidences will be collected and how the coordination will be carried out. In order to combat crime effectively, it is necessary to collectively work on universal laws with international organizations, academic structures and commercial organizations.

RESULT

Before Industry 4.0, cyber-attacks were among the important problems for technology-based organizations and institutions. However, with Industry 4.0, these security issues have become more specific problems and the concept of automation has added new paradigms to security issues. As a result, the victimization of cyber threats has increased in general. In this context, together with the changes expected to occur on the basis of Industry 4.0, the followings can be put forward;

– Thanks to the Internet of Things, each object's being open to the network connection will provide production maximization, but may also cause security flaws,
– With the concept of big data, the demand status in the presence of smart factories, the importance of the analysis of the data regarding production and marketing will increase,
– Storing big data collected over the Internet of Things in cloud systems in physical or virtual environments may cause security flaws,
– The importance of cryptology will increase with the measures taken for increasing data security,
– The data analyses performed by the security teams at a minor level will reach a major level with the concept of big data and security teams are currently not sufficient to work in this field (receiving image on big data will be very difficult and costly, since performing analysis on the data without receiving image has different risk elements, the topic remains uncertain.),
– The items, which have the Internet of things technology, have more potential than the physical traces in terms of forensics for the solution of the crime,
– New cyber risks that enable destruction by remotely commanding for production lines and digital supply networks connected to automation system can emerge,
– With the gradual removal of the boundaries between the real and virtual world, the areas known as cyber-physical production systems (CPS) will become more blurred,
– A security flaw that can occur in production plants will provide some terrorist organizations, which have the concern of finding a place for themselves in the society, with the opportunity to take cyber terrorism actions,
– In case that the cloud storing services are given to the companies operating in different countries, a structure that can include more than one nation-state judicial system will be required since the forensic analysis to be performed on the cloud storing data will be a concern to more than one state,
– In parallel with the constant change of the technology, the technical information need of the security teams will increase day by day, cybercrimes will become more complicated and the solution will become more difficult.

In the analysis performed, it is clear that Industry 4.0, which aims at production maximization, will cause security problems with its current situation. Currently, our industry is between Industry 2.0 and Industry 3.0. Within this scope, it is essential to enhance the technical background of the security teams in order to prevent the crimes that may occur in the future. It is expected that the most appropriate action type of security teams is the security-focused defence understanding. Within the framework of this understanding, a proactive attitude should be exhibited and approaches similar to the ones used by cybercriminals should be adopted. In today's world where the technology changes rapidly, it should be considered that a statical defence understanding cannot be accepted and security teams should adopt a dynamic cybercrime intervention policy in order to fight against new threats.

REFERENCES

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. Ledger, 3(3), 1-21.

Al Mazari, A., Anjariny, A. H., Habib, S. A., & Nyakwende, E. (2018). Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 608-621). IGI Global.

Aljawarneh, S. A., Alawneh, A., & Jaradat, R. (2017). Cloud security engineering: Early stages of SDLC. *Future Generation Computer Systems*, *74*, 385-392.

Assunção, M. D., Calheiros, R. N., Bianchi, S., Netto, M. A., & Buyya, R. (2015). Big Data computing and clouds: Trends and future directions. *Journal of Parallel and Distributed Computing*, *79*, 3-15.

Bendel, O. (2015). *Chancen und risiken 4.0*. Unternehmerzeitung, 2(21), 35.

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, *56*, 684-700.

Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M., & Yin, B. (2017). Smart factory of industry 4.0: Key technologies, application case, and challenges. *IEEE Access*, *6*, 6505-6519.

Chen, H. (2017). Applications of cyber-physical system: a literature review. *Journal of Industrial Integration and Management*, *2*(03), 1750012.

Chiu, Y. C., Cheng, F. T., & Huang, H. C. (2017). Developing a factory-wide intelligent predictive maintenance system based on Industry 4.0. *Journal of the Chinese Institute of Engineers*, *40*(7), 562-571.

Gordon, S. (2004). Privacy: A study of attitudes and behaviors in US, UK and EU ınformation security professionals. Symantec White Paper.

Gordon, S., & Ford, R. (2002). Cyberterrorism?. *Computers & Security*, 21(7), 636-647.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

Harley, C. K. (2018). Reassessing the industrial revolution: a macro view. In *The British Industrial Revolution* (pp. 160-205). Routledge.

Hilse, L. G. (2014). Risks of ISIS-Cyber-Terrorism. *Larshilse*, 72, 16.

Hozdić, E. (2015). Smart factory for industry 4.0: A review. *International Journal of Modern Manufacturing Technologies*, *7*(1), 28-35.

Jin, X., Wah, B. W., Cheng, X., & Wang, Y. (2015). Significance and challenges of big data research. *Big Data Research*, *2*(2), 59-64.

Klingenberg, C., & Do Vale Antunes Jr, J. A. (2017). Industry 4.0: What Makes it Revolution. In *Predavanje na konferenci 24th International EurOMA conference Edinburgh: Inspiring Operations Management, Edinburgh* (Vol. 1, No. 5).

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440.

Lee, J., Ardakani, H. D., Yang, S., & Bagheri, B. (2015). Industrial big data analytics and cyber-physical systems for future maintenance & service innovation. *Procedia Cirp*, *38*, 3-7

Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, *3*, 18-23.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. arXiv preprint arXiv:1604.03850.

Liu, Y., Peng, Y., Wang, B., Yao, S., & Liu, Z. (2017). Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*, *4*(1), 27-40.

Mayer-Schönberger, V., Cukier, K. (2013). Big data. [electronic resource] : a revolution that will transform how we live, work, and think. Res. Manag.

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., & Ueda, K. (2016). Cyber-physical systems in manufacturing. *Cirp Annals*, *65*(2), 621-641.

Morrar, R., Arman, H., & Mousa, S. (2017). The fourth industrial revolution (Industry 4.0): A social innovation perspective. *Technology Innovation Management Review*, *7*(11), 12-20.

Nguyen, H., Tran, K., Zeng, X., Koehl, L., Castagliola, P., & Bruniaux, P. (2019, July). Industrial Internet of Things, Big Data, and Artificial Intelligence in the Smart Factory: a survey and perspective.

Paelke, V. (2014, September). Augmented reality in the smart factory: Supporting workers in an industry 4.0 environment. In Proceedings of the 2014 IEEE emerging technology and factory automation (ETFA) (pp.1-4). IEEE.

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, *13*, 1253-1260.

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston Consulting Group*, *9*(1), 54-89.

Schluse, M., Priggemeyer, M., Atorf, L., & Rossmann, J. (2018). Experimentable digital twins—Streamlining simulation-based systems engineering for industry 4.0. *IEEE Transactions on Industrial Informatics*, *14*(4), 1722-1731.

Stearns, P. N. (2018). *The industrial revolution in world history*. Routledge.

Taute, B. (2017). Improving cybersecurity for industry. *CSIR Science Scope*, *12*(3), 52-55.

Thames, L., & Schaefer, D. (2017). *Cybersecurity for industry 4.0*. New York: Springer.

Tjahjono, B., Esplugues, C., Ares, E., & Pelaez, G. (2017). What does industry 4.0 mean to supply chain?. *Procedia Manufacturing*, *13*, 1175-1182.

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0-A Glimpse. *Procedia Manufacturing*, 20, 233-238.

Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015, September). On the security and privacy of internet of things architectures and systems. In *2015 International Workshop on Secure Internet of Things (SIoT)* (pp. 49-57). IEEE.

Vogel-Heuser, B., & Hess, D. (2016). Guest editorial Industry 4.0–prerequisites and visions. *IEEE Transactions on Automation Science and Engineering*, *13*(2), 411-413.

Wan, K., Hughes, D., Man, K. L., Krilavicius, T. & Zou, S. (2011). Investigation of Composition Mechanisms for Cyber Physical Systems. *International Journal of Design, Analysis and Tools for Circuits and Systems*, *2*(1), 30-40.

Wang, S., Wan, J., Li, D., & Zhang, C. (2016). Implementing smart factory of industrie 4.0: an outlook. *International Journal of Distributed Sensor Networks*, *12*(1), 3159805.

Wangen, G. (2015). The role of malware in reported cyber espionage: A review of the impact and mechanism. *Information*, *6*(2), 183-211.

Wübbeke, J., & Conrad, B. (2015). 'Industrie 4.0': Will German Technology Help China Catch Up with the West?. *China Monitor*, *23*, 1-10.

Yin, S., & Kaynak, O. (2015). Big data for modern industry: challenges and trends [point of view]. *Proceedings of the IEEE*, *103*(2), 143-146.

Zhou, K., Liu, T., & Zhou, L. (2015, August). Industry 4.0: Towards future industrial opportunities and challenges. In *2015 12th International conference on fuzzy systems and knowledge discovery (FSKD)* (pp. 2147-2152). IEEE.