Assessment of the Possibility of Cyber Space to Become a Political Field in the Industry 4.0 Era within OECD Countries

Aytaç Aydın
Kirikkale University

Abstract

With the globalization and trade wars of the 21st century, it has inevitably led to an increase in technological innovations and the emergence of the industrial 4.0 revolution. With Industry 4.0, socio-economy, culture, medicine, all areas of science, living spaces, and everyday activities are somehow linked to technology. The idea that the new popular movements, with the emergence of non-governmental organizations or trade unions by workers' actions, is undoubtedly far from the influence of the 1960-1980 period. Particularly in authoritarian regimes, the suppression of free thinking limits the scope of political activity. For individuals who cannot express their opinions freely or cannot declare their ideas under the roof of any non-governmental organization, the internet is undoubtedly one of the new fields of activity. Individuals can express their thoughts with virtual identities, especially through virtual environments where they can hide through vpn networks, organize and call for unification in areas where necessary. In addition, it is possible to carry out activities against the authority or companies by virtual activists who can use the internet at an advanced level. In this study, first of all, a historical explanation is given to the concept of industry 4.0 to point out the point of the virtual world, and then to draw attention to the effects of cyber-attacks within the OECD countries, it is emphasized that global cyber security index GCI and it is intended to draw attention that cyber area will turn into a new political war zone in the 4.0 years of the industry.

Keywords: Hack, Industry 4.0, Cyber Security

1. Introduction

The study began in 1969 and in 1995 all over the world can be used against our network boundaries with the Internet began to disappear as it unprecedented that day. The Internet has become the most important actor in transforming the world into a common market. This transformation led to the emergence of global trade wars and the virtual world as a new field of combat as the area of action of national and international security threats. This virtual space has created a process in which all countries of the world can intervene and play an active role for individuals in states and societies that can use information effectively. For this reason, cyber space is a highly effective area that states, firms and individuals cannot ignore. While the use of internet and cyber space, which began to become widespread in 1995, could not reach the popularity in terms of threat, nowadays, with the 4th industrial revolution, internet-based transactions begin to dominate in all areas of life. In this context, it is important to look at the 4th industrial revolution in order to reveal the fact that we will need cyber space security. The hactivist movements that have come up to this point are undoubtedly increasing their fields of activity.

1.1 Industrial Revolution In Historical Perspective

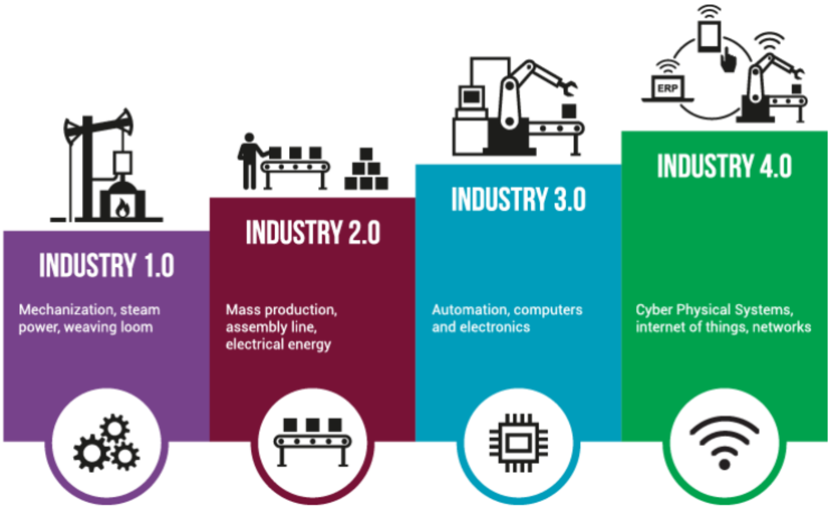
1.1.1 The First Industrial Revolution

For thousands of years, the production process was based on only two basics. The first was undoubtedly human labor and another production factor was the energy of domesticated animals. The world was first introduced to water mills and the first machine to produce energy sources. From the 15th century onwards, various small inventions followed by innovative inventions, machines using water as the main energy source, continued the developmental process. The development of steam machines, which began in 1784, was the next stage of production at the workshop level. In this period, which was seen as the childhood of capitalism, many small-scale guild masters, independent small craftsmen, provided their first capitalist accumulation through exploited wage laborers (Marx, 2009: 714). The first industrial revolution, which lasted until 1870, refers to the period in which weaving, shipping and rail networks became widespread in the textile industry.

1.1.2 The second industrial revolution

The second industrial revolution refers to the period of time between 1840-1870. This period is the period in which the assembly lines started to be used in the production with the use of electricity and new machines in which mass production depending on the division of labor takes place. The use of new machines is mainly to reduce production costs, to produce products at cheaper prices and to sell products at cheaper prices and to become more effective in competition. "The electric-powered production line began for the first time with the system installed in slaughterhouses in the US for slaughtering. But the actual implementation of the system was through mass production lines set up in Ford engine factories. This system used by Ford engine factories in automobile production has led to an increase in production scale and thus a reduction in costs and prices.” (Eğilmez, 2017). Unlike the first industrial revolution with the division of labor, it is the period in which production is based on the employment of women, children of all ages, workers who do not have any qualifications and in general terms cheap labor at all stages of production (Marx, 2009: 441).

Figure 1. Historical process of industrial revolution


INDUSTRY 1.0
Mechanization, steam power, weaving loom
INDUSTRY 2.0
Mass production, assembly line, electrical energy
INDUSTRY 3.0
Automation, computers and electronics
INDUSTRY 4.0
Cyber Physical Systems, internet of things, networks
ERP

Source:https://www.simio.com/applications/industry-40/index.php

1.1.3 The Third Industrial Revolution

The third industrial revolution came into our lives with the 1970s. 3. The industrial revolution is the period in which information and communication technologies have increasingly played an active role in the production processes, along with the concept of electronics, and the emergence of programmable machines. With the active use of the internet and computer, it indicates a fast-moving period (Bulut ve akçacı, 2017:52).

1.1.4 The Fourth Industrial Revolution

4th The industrial revolution, or the concept of industry 4.0, popularly called Marx, said about 150 years ago. "Every new invention that allows the production of something produced in two hours so far reduces the value of all similar products on the market. Competition forces the manufacturer to sell the product of two hours as cheap as the one. Competition activates the law of determining the relative value of a product by the labor-time necessary to produce it (Marx 1992:58). On the basis of these words, it has developed from the perspective of manufacturing faster and cheaper by withdrawing from human production processes for competitiveness and has taken its place in the literature with the Hannover 2011 industry fair held in Germany (https://www.endustri40.com/alamnyanin-endustri-4-0-vizyonu).

As the concept of virtual world becomes increasingly effective and the expansion of internet networks, the interaction of cyberspace with the physical world has accelerated the preparation of the fourth industrial revolution (Hirsch-Kreinsen,2014). The use of information and communication technologies from a new perspective has continued with the active use of cyber physical systems in the manufacturing industry (Prinz et al. 2016). With the 4th industrial revolution, digitalization and virtualization in production, taking steps towards the future in automation systems, working in harmony of multiple systems, emergence of communicating objects, working with people in harmony, effectiveness, efficiency running optimum processes on cost issues and have a self-functioning mechanism in all these processes stands out (Ittermann, Niehaus, Hirsch-Kreinsen, 2018). With the concept of industry 4.0, the increase in the development levels of the countries, the social development, and the effective position in the global markets allow all countries (underdeveloped or advanced) to realize the common benefit level without discrimination (Kagermann,2016). Industry 4.0 "is a collective term that includes many contemporary automation systems, data exchanges and manufacturing technologies. This revolution is a collection of values consisting of the internet of things, the services of the internet, and cyber-physical systems" (https:/www.endustri40.com/endüstri-tarihine-kisa-bir-yolculuk).

Looking at the Industry 4.0, component, cyber-physical systems, the internet of objects, Internet services, and smart factories emerges (Hermann, Pentek, Otto, 2015). Cyber-physical systems are systems in which calculation and physical processes are integrated with each other (Lee, 2007). It is based on three stages: storage and analytical center. Equipped with sensors and actuators. Data can be stored, analyzed and integrated with networks. Internet of Things; It is a network in which cyber-physical systems cooperate with each other with addressing schemes that differ from each other. Internet services; services are provided by service providers over the internet. The business model consists of infrastructure and all other services. smart factories; It is a set of systems that allows to make decentralized decisions by making copies of the physical world and communicating with people and objects through cyber space (Hermann, Pentek, Otto 2015).

The common feature of all components is that it allows remote control. These fields, which are accessible through cyber space, are very important in terms of allowing the production method information of the firms to be obtained through official and informal means, and to create all kinds of activities in the social / political field. Therefore, industry 4.0 continues to develop positively every day, leading to many cyber-attacks.

2. Cyber Space in the Fourth Industrial Revolution

Historically, when we look at the common characteristics of all industrial revolutions, every industrial revolution has resulted in the inevitable processes that affect all society and involve all states in some way. The 4th industrial revolution is undoubtedly expected to survive with the same effect as a historical result until a new industrial revolution. The fact that the 4th industrial revolution and the concept of internet has come up against companies, states and societies with a new perspective constitutes an area that should be prepared by all segments. These areas constitute a cyber space which is far more advanced than the effects of globalization on the elimination of borders. Cyber space is an important field of activity with many advantages and disadvantages. Cyber is used to describe concepts or entities involving computers and networks. The term cyber space is also used to describe the interrelated systems, software, hardware, and abstract or concrete context in which people communicate or interact (Aslay, 2017).

Cyber space creates an environment that allows many individual attacks to be carried out in an unorganized manner. Generally, it can be seen as a means of generating financial loss based on purely financial effects or generating income for the regulator of the attack. However, it is not enough to see this area as an area dominated by individual interests. The cyber space can often be transformed into a group of people with financial, social, political influences that can completely affect the social order, or a group of people who are acting independently of the same views.

Particularly with industry 4.0, in an environment where governments, firms and all individuals in the society are directly or indirectly involved in the Internet, the results have created an area that can be extremely effective and even destructive. The virtual environment is seen as an area where the activity does not reach a sufficient level because it often does not meet with the real environment and as a medium that cannot even be considered as a dissident in the society in general. In fact, it is thought that it cannot go beyond an area where instantaneous reactions and demands of the thoughts of non-social individuals, which have no influence by traditionalist people, have temporary and permanent effects are developed. However, this field creates an environment in which people of the same opinion are in constant dialogue with each other wherever they are in the world and that keeps their political perspectives open. As in the pre-1980 movements, the mass movements are far from the emergence of a physical encounter and a long-term political effort in the real environment. The new political activities create areas of activity where the masses can come together instantly and turn into instant mass movements. The most important point of this is that all the activities carried out in real areas, especially in authoritarian regimes, can be coded and possibly suppressed. In the virtual environment, individuals with developed political perspectives can hide themselves through vpn networks and can be physically present when they reach the highest stage of the political field in which they believe in the future of change.

2.1 Importance of Cyber Space

Cyber security has become an increasingly important part of our lives today. The degree to which networks can be interconnected in the cyber space means that all of our information, data, everything can be revealed and all stages from national critical infrastructure to basic human rights can be compromised (ITU,2017: 47). Therefore, it has taken its place among the extremely important basic points.

The cyber space is one of the areas where more and more attention needs to be given to, as companies and governments need to protect their data, play an active role in social events, and their effects are extremely severe and even destructive. In the 2018 global risk report, permanent inequality and injustice, domestic and international political tensions, environmental hazards and cyber deficits are identified as important risk areas among the four major concerns. Cyber attacks, which did not have the necessary importance until 2017, increased in importance as cyber risks increased after 2017 (ITU, 2018). In the 2019 global risk report, cyber risks are evaluated as very important due to the increasing efficiency of technology and the increasing use of artificial intelligence. In particular, concerns about data theft and cyber attacks are increasing. In 2019, it was pointed out that security measures should be taken against cyber attacks in the cross-border partnerships of the countries due to the necessity of cyber space where data privacy will be violated more for companies and governments (WEF,2019**).**

With Industry 4.0, arriving to and access to data has become easier. One of the main reasons for this is that objects can communicate with each other by grasping the Internet, and in case of a possible infiltration into this network, it provides access to many areas, especially in poorly structured networks, up to basic data.

With the access to the virtual network, operational processes can be affected in companies, data can be leaked through the basic software corrupt communication network, instant intervention can be provided by remote access, media and data flow can be monitored and displayed. In addition, physical damage may occur. It is possible to obtain confidential data of states through data networks (Lloyd's, 2018). Table 1 presents common cyber-event types, examples and potential outcomes. Table 1 sets out the width of the domain.

Table: 1 Common Types of Cyber Events

Extensive Cyber Case Types	Sample	Potential Results
Data Privacy Violation **(3rd party data)**	Unauthorized disclosure of personally identifable information of third parties.	Incident response costs, confidential infringement compensation, reputation damage, regulatory and legal defense costs, possible penalties and fines, responsibility of directors and civil servants.
Data Privacy Violation **(own data)**	Theft of trade secrets.	Intellectual property theft, responsibility of managers and civil servants.
Operational Technology Failure	Manipulation of control system.	Job interruption, penalties, physical property damage, bodily injury and death, responsibility of directors and civil servants.
Network Failure	An attack on server that causes a company website not be used.	Job interruption: loss of reputation, responsibility of directors and civil servants.
Disruption Of The 3rd Party System From The Sytem	Transmission of malware to a 3rd party system.	Responsibility for network security failure, regulatory and legal defense costs.
Disruption To External Server Provider	Corruption in the software application provided by the cloud service.	Contingent business interruptions.
Deletion or Corruption of Data	Malicious software that causes data to be deleted from networked computers.	Loss of data and software, regulatory and legal defense costs, product liability, responsibility of directors and officers.
Data Encryption	Prevents access to data or a network until a ransom is paid.	Cyber ransom and tribute.
Cyber Fraud Theft:	Illegitimate financial transfer, financial theft in the network or intrusion or social fraud, engineering-based data transfers.	Financial theft / fraud

Source: (OECD, 2017)

Cyber-domain activities or cyber-attacks are not just malicious software applications. Cyber-attacks can become a field of political activity, especially in authoritarian regimes. Those who operate in this field appear as hactivist identity.

2.2 Hacker and Hactivism

According to the definition of hacker, by Turkish language institution; He describes his knowledge of computer and communication technologies as someone who uses it to access confidential data and perform illegal, damaging work on networks (www.tdk.gov.tr access date: 10 May 2019). “The concept of hacker, except official definition; Rather than theorizing programming, they are passionate people who enjoy programs, find creative coding methods that will improve the capacity of a working system, and overcome the limitations and disruptions of the system” (Boschele and Öztürk 2017). The concept of hackers is often portrayed as a negative concept in international organization reports and the media. But the concept of hacking under such a restriction does not offer a correct perspective (Bülbül and Bingöl 2018). The first generation of hacker ethics activities emerged with demands that could lead to discussion. Today, changing and developing demands can be encountered. The first generation of hackers focused on the power to process information and to provide unlimited access to information. For many hackers, the attempt to make technology more democratic and accessible has been seen as an important field of activity. In 1971, the Youth international party was one of the first important activities of hackers that America did not want to support and be involved in the war against taxes on telephone bills for the Vietnam war financing and to protest against the Vietnam war with a social stance. Similarly, in 1981, the German chaos computer club demanded that all information be free of charge and advocated the development of an information society free of charge throughout the world as the necessity of human rights. The American programmer, hacker and open-access advocate, political activist Aaron Swartz, considered one of the greatest activists in the virtual world, is one of the most important characters in advocating free access to information. In 2011, Swartz allegedly downloaded thousands of academic articles from the JSTOR archive (Salvo, 2017). Today, there are many hackers who carry out many activities especially in terms of access to the right information source and transparency of information (Jordan and Taylor, 2004).

2.2.1 Hactivism

It is not correct to define the concept of hactivisim as a phenomenon that acts only from an ideological point of view. There are different perspectives within the concept of Hactivism.

Hactivism is seen as a new type of Internet threat in various sources. Hacking is perceived as an instrument used by independent people and increasingly used by individuals to promote their political ideology. It has been proposed that the objectives are to prevent communication using internet-supported networks and organizations (Hearn, Mahncke, Williams, 2009). Hactivism; Online activities of people who come together with various concerns make up the whole. Hactivists can be defined as societies with social and political concerns and can be defined as societies that exhibit cultural and political resistance that focus on many social concerns such as war, monopolization, globalization, neoliberal policies, telecommunications sector and media monopoly, education, health, local resistance. jobs, labor movements (Jordan and Taylor, 2004). Embody the concept of hactivism; Table 2 presents the spectrum of online and offline forms of activism.

Table 2: Spectrum of Online and Offline Forms of Activism

	Offline	Online
Conventional	**Activism:**	**Online Activism:**
	➢ Voting	➢ Online voting
	➢ Election prop	➢ Online campaign donations
	➢ Non-violent protests	➢ Online petition
	➢ Boycott	
Transgressive	**Civil Disobedience:**	**Hactivism:**
	➢ Sit-in	➢ Website disorders
	➢ Barricades	➢ Website redirects
	➢ Political graffiti	➢ Denial of service attacks
	➢ Wildcat strike	➢ Information theft
	➢ Underground press	➢ Site parody
	➢ Political theater	➢ Virtual sabotage
	➢ Sabotage	➢ Software development
Violent:	**Terrorism**	**Cyber Terrorism:**
	➢ Political bombing	➢ Hacking air traffic control
	➢ Political abduction	➢ Cutting the electricity grid
	➢ Tree Spiking	

Source: Xiang Li, Harvard Journal of Law & Technology Volume 27, Number 1 Fall 2013

In general, authoritarian regimes, supporters of globalization, neo-liberal politicians, the concept of hactivism, perceived as a threat among the supporters of globalization, are assumed by the opposing viewers to remove obstacles to access to information and to ensure a more democratic free and fair order. From a historical point of view, all industrial revolutions are seen as the confrontation areas of different views and opposing ideas. The refusal of the capitalist model of production in Russia in October 1917, the transition to the socialist model of production, and the subsequent cold war are examples of this. In this sense, 2014-2019 will be restricted and the Global Security Index (GCI) data will be applied in order to transform the cyber space into a political field of activity and measure its impact. The reason for selecting 2014 is that GCI was first published in 2014. The study is limited to the member countries of the Organization for Economic Development and Cooperation (OECD).

3. Global Cyber Security Index (GCI) in OECD Countries

The global cyber security index (GCI) was originally born in 2014 by ABI Research and the international telecommunications association (ITU). The first report is based on data from 105 countries. The report is still being prepared by ITU. The GCI provides information on the cyber security levels of nation-states. The basis of the index contents five main category; legal measures, technical measures, organizational measures, capacity building and international cooperation. (ITU, 2015). The sub-components that make up the index are shown in table 3.

Table: 3 Global Cyber Security Index (GCI), 5 Key Indicators and Components.

Legal	- Cybercrime Legislation - Cyber Security Regulation - Cyber Security Training
Technical	- National Computer Response Teams - Government Computer Intervention Teams - Sectoral Computer Incident Response Teams - Standard For Organizations - Standards And Certifications For Professionals - Child Protection
Organization	-Strategy -Responsible Institution -Cyber Security
Capacity Building	-Standardization Bodies -Good Practices - R&D Programmes -Public Awareness Raising -Vocational Training Courses -National Education Programs And Academic Curriculum -Incentive Mechanisms -Growing Cyber Security Industry At Home
Cooperation	-In-State Cooperation -Multilateral Agreements -Participation In International Forums -Public-Private Partnerships

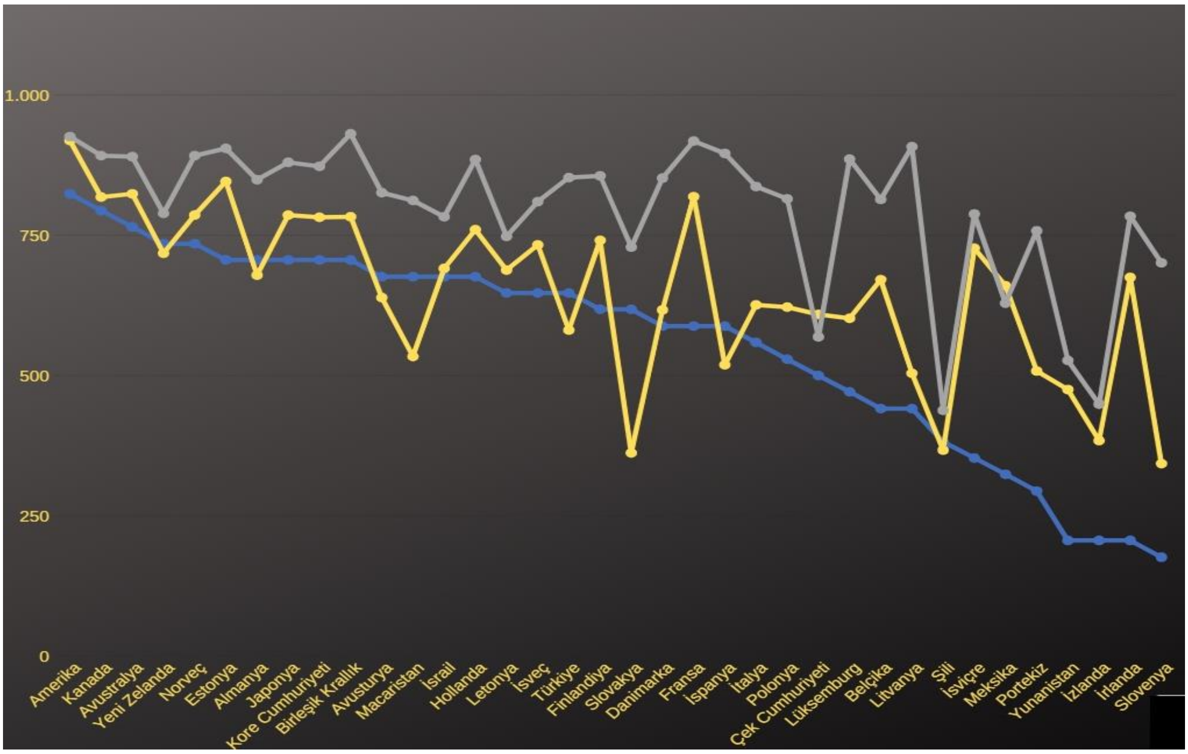
Source: Global Cybersecurity Index 2015

CI is a compound index in which five main categories are processed. The index is expressed in values from 0 to 1. 0 indicates the worst possible readiness and 1 indicates the best possible readiness (ITU, 2018). In order to measure the impact of cyber space, the GCI values that we refer to in our study will be examined by limiting the data of OECD member countries.

3.1. Global cyber security index (GCI) data in the OECD countries

Economic development and cooperation organization USA, Germany, Australia, Austria Belgium, Czech Republic, Denmark, Estonia, Finland, France, Netherlands, Ireland, Ireland, Spain, Israel, Sweden, Switzerland, Italy, Iceland, Japan, Canada, Korea, Latvia, Lithuania, Luxembourg, Hungary, Mexico, Norway, Poland, Portugal, Solva, Slovenia, Chile, Turkey, New Zealand, Greece consists of 36 member countries are located (http://www.mfa.gov.tr access date 20.05.2019). Graph 1 show the GCI values of OECD countries prepared from GCI reports published in 2015-2017-2018. the blue line represents the values in 2015 reports, the yellow line represents the year 2017, the gray line indicates the GCI values of 2018. According to the 2015 report, the best possible preparation belongs to America with 0.824 points. Canada is ranked 2nd with a value of 0.794. According to the values of 2017 report, America is at the top of the list with 0.919 values among OECD countries. Canada is ranked 4th with a value of 0.892. In the 2018 report, the UK ranks first with a value of 0.931. France, one of the most remarkable countries in the graph, increased its value from 0.588 in 2015 to 0.819 in 2017 and 0.918 in 2018. When Turkey’s value is 0.647 in 2015, it increased the value to 0.853 in 2018. When the graph values are taken into consideration, it is seen that all OECD countries have increased the measures in cyber field since 2015 and they have taken more and more measures.

Chart 1: GCI values for the years 2015-2017-2018



Source: Global Cybersecurity Index 2015, Global Cybersecurity Index 2017, Global Cybersecurity Index 2018

3.2 Samples of Cyber Attacks

Cyber space is becoming more and more effective every year. The economic impact of cyber-attacks has increased fivefold from 2013 to 2017. Ransom software programs increased by 300%. 87% of Europeans see cybercrime as a matter of internal security (EU, 2017). The Wannacry and notepad attacks in 2017 affected an estimated 300,000 victims worldwide. Wannacry attacks alone cost the world economy $ 4 billion. Several industries have been affected within the EU, including health care, telecommunications, transport and manufacturing (Europol, 2018). It is predicted that between 2015-2022, 9 trillion and 21 trillion dollars of economic risk will arise (OECD, 2017).

When the financial effects of cyber-attacks and the regions under attack are taken into consideration, it shows that no matter how high the GCI value is, all countries will be affected by cyber-attacks. In spite of all the measures taken, cyber-attacks have become periodically unavoidable and their consequences can affect all segments of society.

Conclusion

The most important feature that distinguishes the cyber field of activity from all other political spheres is its universality and not know any limit. Another area of this borderlessness with globalization is the commercial area, which is monopolized by developed countries.

The main concern of the developed countries is to increase their competitiveness in this commercial field. The concept of industry 4.0, which emerged with this reason, obliges every sphere of life to a digital transformation. This digital transformation has brought many cyber security vulnerabilities. In recent years, especially in OECD and EU reports, cyber security costs are frequently emphasized. Although the majority of these attacks were not carried out by a political cyber activist group, the economic dimensions of these attacks force all countries to take the necessary measures. As a matter of fact, a potential vulnerability has the potential to turn into a force that would disrupt the functioning of the whole system. For this reason, cyber space has started to become a new field of activity on a global scale especially in political demands. This stands as a field of political activity in front of anti -democratic structures as well as the demands of the received democratic rights. For this reason, it is important that the cyber field is given to every member of the society from an early age for the safety of individuals living in the society and the operation of a process in which more viable free thinking is dominant. Despite the continuous improvement in GCI values in the 2015-2018 period, the fact that cyber-attacks are still effective in economic terms reveals the size of cyber space. Particularly, cyber activity areas are expanding and the spreading of social demands through virtual networks will lead to the emergence of the virtual activist with the increasing effect day by day. This shows that a group of virtual activists can cause profound economic damages, and influence the social and political spheres. Therefore, structural reforms and the development of an equal and fair understanding of society are very important for countries.

References

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi, International Journal of Multidisciplinary Studies and Innovative Technologies, 1(1): 24 – 28.

Boschele,F,A., Öztürk, Ç, Ö.(2017). Dijital İletişim Teknolojileri ve Toplumsal Hareketler Bağlamında Hacktivizm, Üsküdar Üniversitesi Sosyal Bilimler Dergisi, sayı: 5, 429-452

Bulut, E., Akçacı, T.(2017). Endüstri 4.0 ve İnovasyon Göstergeleri Kapsamında Türkiye Analizi, ASSAM Uluslararası Hakemli Dergi (ASSAM - UHAD), 7, 50-72.

Bülbül, İ, Bingöl, E.P.(2018). Etik Hackerlığa Giriş Ofansif Siber Güvenliğin ABC'si!, 4. Baskı, İstanbul: Hayygrup Yayıncılık

Eğilmez, M. (2017). Endüstri 4.0 http://www.mahfiegilmez.com/2017/05/endustri-40.html, Erişim Tarihi: 10.01.2019.

Europol,(2018). Internet Organised Crime Threat Assessment (IOCTA) 2018 Erişim Adresi: www.europol.europa.eu Erişim Tarihi: 25.05.2019

EU, (2017). European Commission Cybersecurity 2017, Erişim Adresi:https://ec.europa.eu/, Erişim Tarihi: 28.05.2019

Hearn, K. Mahncke, J. R., Williams A.P.(2009). Culture Jamming: From Activism to Hactivism, Australian Information Warfare and Security Conference, Erişim Adresi: https://ro.ecu.edu.au/isw/3/ Erişim Tarihi: 18.05.2019

Hermann M, Pentek T,Otto B. (2015). Design Principles for Industrie 4.0 Scenarios:A Literature Review, Working Paper, 01, 1-15.

Hirsch-Kreinsen, Hartmut (2014). Wandel von Produktionsarbeit –"Industrie 4.0", wsi mitteilungen, 6, 421-429.

ITU,(2015). Global Cybersecurity Index 2015, Erişim Adresi:www.itu.int, Erişim Tarihi 10.05.2019

ITU,(2017). Global Cybersecurity Index 2017, Erişim Adresi:www.itu.int, Erişim Tarihi 10.05.2019

ITU,(2018). Global Cybersecurity Index 2018, Erişim Adresi:www.itu.int, Erişim Tarihi 12.05.2019

Ittermann P., Niehaus J., Hirsch-Kreinsen H. (2018). In Der Industrie 4.0 Trendbestimmungen und arbeitspolitische Handlungsfelder, 308, 1-71.

Jordan, T, Taylor, P., (2004), HACTIVISM AND CYBERWARS Rebels with A Cause, Published by Routledge, London.

Kagermann, H., Anderl, R., Gausemeier, J., Schuh, G., Wahlster, W., (Eds.), (2016). Industrie 4.0 in a Global Context: Strategies for Cooperating with International Partners(acatech STUDY), Munich: Herbert Utz Verlag.

Lee A, Edward (2007). Computing Foundations and Practice for CyberPhysical Systems: A Preliminary Report, https://www2.eecs.berkeley.edu/Pubs/TechRpts/2007/EECS-2007-72.pdf, (Erişim Tarihi: Aralık, 2018).

Li, Xiang.(2013). Hactivism and the First Amendment: Drawing the Line Between Cyber Protests and Crime, Harvard Journal of Law & Technology Volume 27, Number 1

Lloyd's, (2018). Networked World Risks and opportunities in the Internet of Things, Erişim Adresi:https://www.lloyds.com Erişim Tarihi 15.05.2019

Marx,K.(2009).Kapital, Alaattin Bilgi (çev). Ankara: Sol Yayınları

Marx,K.(1992).Felsefenin Sefaleti, Ahmet Kardam (çev). Ankara:Sol Yayınları

MFA, İktisadi İşbirliği ve Gelişme Teşkilatı (OECD), Erişim Adresi: http://www.mfa.gov.tr/iktisadi-isbirligi_ve-gelisme-teskilati-_oecd_.tr.mfa Erişim Tarihi: 20.05.2019

OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264282148-en

Prinz C., Morlock F., Freith S ., Kreggenfeld N., Kreimeier D., Kuhlenkötter B.(2016). Learning Factory modules for smart factories in Industrie 4.0. Procedia CIRP, 54, 113 – 118.

Salvo,D.P.,(2017). “Coder,” “Activist,” “Hacker”: Aaron Swartz in the Italian, UK, U.S., and Technology Press, International Journal of Communication 11.

Türk Dil Kurumu güncel Türkçe sözlük içinde, Erişim Adresi: www.tdk.gov.tr.,Erişim tarihi: 10 Mayıs 2009)

WEF,(2019). The Global Risks Report 2019 14th Edition, Erişim Adresi: http://wef.ch/risks2019, Erişim Tarihi 15.05.2019

https://www.endustri40.com/endustri-tarihine-kisa-bir-yolculuk, (Erişim Tarihi: 12.04.2019).

https://www.endustri40.com/almanyanin-endustri-4-0-vizyonu, (Erişim Tarihi: 01.04.2019).

https://www.simio.com/applications/industry-40/index.php, (Erişim Tarihi: 08.04.2019).