Uluslararası Yönetim Akademisi Dergisi
Yıl: 2019, Cilt: 2, Sayı: 1, ss.51-63

https://doi.org/10.33712/mana.548909

Cyber Security of Critical Infrastructures in Smart Cities

Akıllı Şehirlerdeki Kritik Altyapıların Siber Güvenliği

Volkan GÖÇOĞLU
Dr., Afyon Kocatepe Üniversitesi,
Dinar UBYO, volkangocoglu@gmail.com,
https://orcid.org/0000-0002-7036-2416

Makale Başvuru Tarihi / Received: 03.04.2019
Makale Kabul Tarihi / Accepted: 23.04.2019
Makale Türü / Article Type: Araştırma Makalesi

ÖZET

Anahtar Kelimeler:

Akıllı Şehir,

Siber Güvenlik,

Kritik Altyapılar,

Akıllı şehir birçok farklı alandan araştırmacıların ilgisini çeken popüler bir konudur. Kamu yönetimi alanında bir çalışma alanı olmasına rağmen, mühendislik bilimlerindeki araştırmacılar tarafından odaklanılan teknik boyutlara da sahiptir. Öte yandan, çok disiplinli katkıları içeren bir sınırı olan akıllı şehirlerin bir de güvenlik boyutu vardır. Şehirlerin güvenliği, çağlar boyunca önemli bir mesele olmuştur, ancak akıllı şehirlerin ortaya çıkması, internet ve iletişim teknolojilerinin gelişimi ve akıllı şehirlerdeki kritik alt yapıların sanal ağlarla birbirlerine bağlanması sonucunda, güvenliğin yeni bir boyutu güvenlik çalışmalarının ana başlığı haline gelmiştir. Bu başlık siber güvenliktir. Bu çalışma, akıllı şehirlerde özellikle kritik altyapılara odaklanan siber güvenlik meselelerini sorgulamayı amaçlamakta ve akıllı şehirlerdeki kritik altyapıların siber güvenliğini sağlamak için öneri niteliğinde bir model ortaya koymaktadır.

ABSTRACT

Keywords:

Smart City,

Cyber Security,

Critical Infrastructures,

Smart city is a trending topic that many researchers from different disciplines are interested in. Even though it is supposed to be a study field of public administration, it has also technical dimensions which are focused on by researchers from engineering sciences. On the other hand, there is a security dimension of smart cities which has a boundary that includes multidisciplinary contributions. The security of cities has been an essential issue throughout the ages, but with the emergence of smart cities, the development of internet and communication technologies, and as a consequence of interconnection of critical infra structures in the smart cities, a new dimension of security has been emerged as the headline of security studies. This headline is cyber security. This study aims to investigate cyber security issues in smart cities particularly focusing on critical infrastructures and presents a recommendatory model for providing cyber security of critical infrastructures in smart cities.

1. INTRODUCTION

Since the end of Second World War and beginning of Cold War, a big competition on space researches was started between capitalist and socialist systems. It was claimed that hard effort on research and development in this field had lunched the new space age. After decades witnessed the space researches made by United States of America and Socialist Soviet Russia, in the 20th century, the researches on computer and communication systems were concentrated and in the 21st century the researches on these technologies hit the top. The development of the computer and communication systems has changed the ways of reaching information for people in daily life. New communication tools such as e-mail, social media, instant messaging, live streams and video calling have emerged. Internet has become a larger network day by day and it has returned a portal that is used for entertaining, communicating, shopping, voting and even governing. In this societal change shaped by the development of computer and communication systems (Celik, 1998:54), people's perception of information was also changed beside the production, distribution and usage of knowledge. This age is called as "information age" and the society of this age called as "information society" (Webster, 2014:19). Cyber security has emerged as a reflection and necessity regarding to these changes and developments.

Smart city can be assumed as another reflection of information age and society. Smart cities are covered by advanced equipment and software of latest technology such as industrial control systems, internet of things, Supervisory Control and Data Acquisition and Distributed Control Systems (PWC, 2018) and critical infrastructures interconnected with these components. Depending on this cyber network between things, structures and software, beyond being a physical structure, critical infrastructures have become cyber-physical structures in smart cities. Thus, the cyber security of these critical infrastructures in smart cities has been a vital issue for regional and national security. The researchers from various disciplines have focused on this issue and aimed to investigate problems and solutions in order to provide cyber security of smart cities.

Cyber security of smart cities is an issue that is getting more vital day by day. The report of Center for Strategic and International Studies (CSIS, 2019) and article of Forbes (2019) underline the cyber-attacks on cities. According to reports, in March 2018, online services Atlanta city municipality had been the target of cyber-attacks and were disrupted after a ransomware attack struck the city's networks, demanding $55,000 worth of bitcoin in payment. Recovery of the system vulnerabilities cost 2.6 million dollars for the government. Similarly, cyber-attack to Sacramento Regional Transit systems in November 2017, cyber-attack to Sweden Transport Administration systems in October 2017 and cyber-attack to San Francisco Municipal Railway are some examples showing the importance of cyber-security of smart cities. These examples reflecting the situation may be enhanced and the cyber-attacks on cities are increasing while more cities are becoming smarter.

Critical infrastructures of smart cities are the vital facilities in delivering public services by central and local governments. In the context of the research question determined as "What are the actions for providing the cyber security of critical infrastructures in smart cities?", this study aims to investigate cyber security issues in smart cities particularly focusing on the critical infrastructures and presents an original framework and a recommendatory model for providing cyber security of critical infrastructures in smart cities. In the first part of the study, keywords and key elements of cyber security are investigated. In the second part of the study, smart city has been tried to conceptualized and the content of smart city concept is examined. Finally, in the last part of the study, cyber security of critical infrastructures in smart cities is examined and a model created by the researcher is presented.

2. KEYWORDS FOR CYBER SECURITY

In the information society, cyber security has recently become an important concept in human's life, depending on the development of information and telecommunication (I.T.) technologies. The origin of the word "cyber" comes from the origin of "cybernetic" which is a featured concept in defining the control and communication of animal and machine systems (Wiener, 1948). "Cyber Space" is another concept that has the same origin and draws the boundaries of cyber security's conceptual definition. On the other hand, cyber space is an intangible concept the same as with cyber security and it includes software, data, networks and field although it is sheltered in physical hardware of technology (Clark et al, 2014). Finally, cyber security is defined by The National Initiative for Cybersecurity Education (NICE), as a process or activity that consists of the protection of I.T. systems and the information in these systems towards potential cyber-attacks and threats. To expand the conceptual framework of the definition, the elements such as operations and security in cyberspace policy, strategy, standards with all kinds of threats, vulnerabilities, deterrence, international integration, preparedness, resistance, rescue policies, security of global information and communication infrastructure related to military, diplomacy and intelligence can be added to definition. International Telecommunications Union (ITU) defines the cyber security as the total of the equipment, policies, security concepts, actions, courses, best practices and technologies to protects the cyber space, people, institutions and even countries. (Korff, n.d.). According to this definition, cyber security has dimensions in personal, institutional and national levels. In this study, national dimension of cyber security is examined particularly on the scope of smart cities.

There are six key concepts for better understanding of cyber security's scope. As Graham et al. (2010:2-6) states, three of these concepts known as the Central Intelligence Agency (CIA) triad are confidentiality, integrity, and availability. These concepts must be well understood by anyone who aims to protect a system. The other three of the concepts: authentication, authorization, and nonrepudiation are for the security professionals. To sum up shortly, *confidentiality* guarantees that the related information is not presentable for the individuals, processes, or devices who are not authorized. *Integrity* points out that the data in the system is integrated and there is no inaccurate data and unauthorized modifications in the system. *Availability* provides users a good access to information system. *Authentication* is to verify the source of message or entries which is entered in the system. *Authorization* enables the pioneer security of the system and determines the permissions of users in accessing, changing and making modifications on information in the system. Lastly, *nonrepudiation* is to detect that the source of data is confirmed with proof of delivery and the receiver of data is confirmed with proof of the sender's identity.

Beyond the concepts described above, cyber security has also other common used concepts. These concepts are used by not only cyber security professionals but the society. One of these concepts is "cyber-attack". Cyber-attack is a concept that is a sensitive issue in the world of internet. The concept defined by Farhat et al. (2016) as "an attack initiated from a computer against a website, computer system, or individual computer (collectively, a computer) that compromises the confidentiality, integrity, or availability of the computer or information stored on it". There are also different sorts of cyber-attack modelling techniques. Al-Mohannadi et al. (2016:70-71) examine three of cyber-attack modelling techniques in their study. The first technique they stated is diamond model. The model associates with some meta-features such as timestamp, phases, result, directions, methodology and resources and it bases on evaluation of the capability of targeted victim and attacker who are using the network. One of other technique is named as Kill Chain. This is a well-structured technique that contains of a chain of steps. The attacker gathers information about victim, he/she chooses weapons to attack and delivers them to the target. In following process, exploitation starts. The victim installs the malware to computer, unconsciously. Finally, the attacker takes the control of the system and reaches the data he targeted. The third technique is Attack Graph. This is a defense based modelling. Attacks graphs are conceptual diagrams to determine the vulnerability of the system, the quantity of potential attacks and set of actions to prevent system from these attacks.

Although cyber-attack issue concentrated on individual dimension focusing on the "bad guys" (unauthorized individuals with maliciousintent) (Denning and Denning, 2010:29), it has also national dimension. Cyber-attacks that are aiming various political and military targets, may cause serious national security ramifications (Geers, 2010:298). Stuxnet attack can be an instance to show the danger of cyber-attacks on national dimension. This case which U.S.A and Israel attacked to Iran's nuclear facilities by cyber tools, noted in literature as one of bigger cyber-attacks targeted a national security (Mueller and Yadegari, 2012; Bronk and Tikk-Ringas, 2013; Collins and McCombie, 2012; Baylon, 2017). With the explosion of nuclear reactors in the Iran's nuclear facilities, the case of Stuxnet show the world that cyber-attacks may cause not only cyber but also physical damages for countries (Gocoglu, 2018:281).

Another concept that commonly used in cyber security literature is "cyber-exploitation. This can be defined as a process comes along after successful cyber-attacks. Cyber-exploitation emerges from vulnerabilities in the cyber systems. It describes the using, changing or getting benefited from information in systems by unauthorized users. As Snyder et al. (2015:3) states, attacker can use this information for various intents such as leaking out the technology, assessing targeted system capabilities, improving some countermeasures to framework of the system, and providing intelligence for a massive attack against the system. Consequently, against to cyber-exploitations, cyber programs should be applied for regular and routine assessment and testing of national cybersecurity capacity to investigate exploitable weaknesses and bugs in the systems (Tohme et al, 2015). As an example for fighting with cyber-exploitation, U.S.A underlined in the national cyber strategy (NCS, 2018:9) that, most cybersecurity risks to critical infrastructure stem from the exploitation of known vulnerabilities.

Risk, threat, and vulnerability concepts are also included in cyber security literature as they included in national security literature. These three concepts are related each other. A weakness on system causes vulnerability and a vulnerability in the system causes risk and threat on the system. According to this, it has become an important issue for the governments to make public policies to avoid threats on cyber systems and critical infrastructures. As it is stated in Italian National Strategic Framework for Cyberspace Security published by Presidency of the Council of Ministers (PCM, 2013:18), in order to avoid the vulnerabilities from being exploited, mitigation, risk assessment and management plan including physical, logic and procedural cybersecurity measures should be arranged. On the other hand, for governments, critical infrastructures are main elements to be secured from cyber-attacks. These structures will be examined in depth on the context of smart cities, in the third part of the study.

3. EXTRACTING THE COMPONENTS OF SMART CITY

In a big part of 20th century, the idea that a city could be smart was not to be more of than an imagination which was appeared in popular media. With the sudden development of computable devices across many scales and with limited intelligence being embedded into such devices, the prospect that a city might become smart and sentient even, has become a new reality (Batty et al, 2012:482). Recently, sustainable urban growth has ermerged as a significant issue for the local and central governments. An addition to urban growth, migration is also a process that should be managed well in order to keep infrastructures of cities resistant to this burden of governance. Increasing demand of supply for water, energy, transportation, healthcare, education, and safety, governments seek solutions from advanced information-communications technology (ICT) and new working practices to reduce costs, improve efficiency, and deliver the quality of life citizens expect, while balancing budgets (Naphade et al, 2011: 32). As a reflection of this seeking, the concept of the smart city has been quite fashionable in public policy agenda as a strategy to mitigate unprecedented challenges of urban growth, increasing population intensity and to provide citizens a better life quality (Osman, 2018:620; Woodhead, 2018:1510).

Internet of things (IoT) is a concept that raised nearly at the same period with smart cities. Even though the two concepts have consolidated roots, they have raised from different origins. Smart city has existed, thanks to need of greater cities which is governed more effectively by using the technology while IoT has existed as a reflection of advanced technology (Gul, 2018:11) and allowed people and things to be connected anytime, anywhere and anyway (Perera et al, 2014:81). The function of IoT in smart cities is to provide data collection as well as big data and help the analysis and to use this data for the services and needs (Ming Wu et al, 2018:1). As Batty et al.' (2012:482) state, smart cities are often described as organisms of instruments across many scales that are connected each other through multiple networks that provide continuous data regarding the movements of people and materials in terms of the flow of decisions about the physical and social form of the city. In a wider view, based on Roch et al.' (2012:216) definition formed from a comprehensive literature review, smart cities have many dimensions such as education of population, human and social capital, sharing of knowledge in public, public dialogue and participation beside use of internet and communication technologies. Similarly, several researches have emphasized the role of human capital and education, social and relational capital, and environmental issues as important drivers of urban growth (Osman, 2018:620; Caragliu et al, 2011:66; Ramos et al, 2018).

Although different dimensions of smart cities are referenced in the studies from different aspects (Hollands, 2008:306), the main issues on smart cities are generally concentrates on the role of ICT infrastructures such as smart buildings, smart farms, smart hospitals, smart transportation, and other smart labeled domains.

For providing a smart city that is functionalized in a smart and sustainable form to ensure sustainability and efficiency, integrated infrastructures (Musa, 2016:1; Sahin, 2018:10) and services into cohesive units which can be monitored and controlled by smart devices, should be presented (Alavi et al, 2018:590). These electronically integrated infrastructures enable citizens to use resources in cities in more efficient way, to make public transport more attractive, and to provide planners and decision-makers big data to allocate resources more accurately (Townsend, 2013; Yigitcanar et al, 2019; Neirotti et al, 2014:26; Allwinkle and Cruickshank, 2011:2). Big data connects the data flow between citizens, public agencies, non-governmental organizations and private sector as it connects the infrastructures such as transport infrastructures, electricity infrastructures, energy distribution networks, communication infrastructures and natural resources (Dwevedi et al, 2018:2; Neirotti et al, 2014:26). As Lim et al. (2018:86) point out, the use of big data in governing, contributes to the creation of useful content for various actors of public policy, including citizens, visitors, local governments, and private sector companies. For an instance that handle in their article, Seoul government collects data from related institutions about public health, transportation, and residence, then generates them as a dataset to be useful for scientists. According to all these explanations, for a clear answer to the question "which components are supposed to be smart for being a smart city?" the Table 1 below can present a well-structured view:

Table 1. Components of Smart Cities

Components of a Smart City	Related Aspect of Urban Life
Smart Economy	Industry
Smart People	Education
Smart Governance	E-Democracy
Smart Mobility	Logistics & Infrastructures
Smart Environment	Efficiency & Sustainability
Smart Living	Security & Quality

Source: Albine et al. (2015: 11), adapted from Lombardi et al. (2012).

As it is underlined before, the most highlighted dimension of smart cities in related literature is the use of internet and communication technologies in city and local government affairs. On the other hand, there are various different dimensions of smart cities although they are emphasized rarely and these dimensions are important to make a full conceptualization of smart cities. These mostly neglected dimensions are put forward in some researches depending on the researcher's study field and experimental background (Gil-Garcia et al, 2015:64-65). The dimensions of smart cities are presented in these studies from the perspective of citizens, governments, economy and environment (Degbelo et al, 2016:2). The domains of smart cities are covered in a holistic view by a wider definition called as "smart society. This concept includes smart Non-Governmental Organizations (NGOs), private sector companies and also public agencies (Mecek and Kocakula, 2019:203). Nevertheless, for a well-structured description, Yin et al. (2015), have presented the dimensions of smart cities in a holistic view. Table 2 below, reflects the summary of their analysis on the domains of smart cities from different perspectives.

Table 2. Classification of Smart City Application Domains

Domain	Sub-Domain
Government (more efficient)	E-government, Transparent government, Public service, Public safety, City monitoring, Emergency response
Citizen (happier)	Public transport, Smart traffic, Tourism, Entertainment, Healthcare, Education, Consumption, Social cohesion
Business (more prosperous)	Enterprise management, Logistics, Supply chain, Transaction, Advertisement, Innovation, Entrepreneurship, Agriculture
Environment (more sustainable)	Smart grid, Renewable energy, Water management, Waste management, Pollution control, Building, Housing, Community, Public space

Source: Yin et al. (2015).

It is seen in the Table 2 that there are various topics in smart city issue to focus on academically. The Table 2 also shows us some similar components that are underlined in Table 1 (Albine et al, 2015:11), which are musts for being a smart city. In Table 2, government is to improve the internal and external efficiency. On the other hand, government enables citizens and other relevant organizations to access the public and official briefs, ensures and improves the capability of public services; monitors the security in the city; and take actions quickly and effectively in emergency. Citizens are able to access to needed information from public agencies and institutes, get advanced public services such as health care, education, environmental services, transportation which are developed by advanced technology and smart systems. In business, management systems are tending to be more effective and efficient. Smart systems are used in logistics and supply chain platforms and methods. The way of smart advertising provides more widely and accurately advertising. In the sectors of business such as production, agriculture, finance, consulting; fostering innovation andcommerce, smart systems will support the expanding of producers, partners and customers. Environment applications get more sustainable thanks to smart systems. For example, need of water and energy supply may be determined in the count results of citizen's behavior and demand, by advanced smart systems. Waste management benefits the advantages of smart systems such as sensor monitoring and real time control systems (Yine et al, 2015). On the other hand, government, citizens, business, environment and the sub-domains of these components are also supposed to be smart to become a smart city (Sadioglu and Erdincler, 2018:87). Rusen Keles' (2019) statement in a review of a daily news website[1] support this idea. He emphasizes that "The ones supposed to be smart are not cities but the governors". As this study focuses on the integrated critical infrastructures of a smart city, in the next part of the study critical infrastructures and the cyber security of these will be examined in depth.

4. CYBER SECURING OF CRITICAL INFRASTRUCTURES IN SMART CITIES

Critical infrastructures which can be described as the set of physical cyber and organizational subsystems (Prochazkova and Prochazka, 2018) are vital systems for people to maintain their casual and social routines, security, health care services, economic and societal welfares. Beyond, these systems have also vital significance for public safety, national security and the economic welfare of countries. According to this key role on regional and national security, infrastructures are on the focus of countries' security strategy. European Union (EU), released a directive (Network Information Security) to collect attention on the importance of critical infrastructure security of countries and necessitated member countries to raise the basement of their security capabilities of critical infrastructure frameworks (Marsh and McLennan, 2017).

Even though the number and categorization of critical infrastructure systems are not stable in the world, a general classification can be presented by compiling from various country. For instance, Czech Republic determines their critical infrastructures as communication and information systems, water supply systems, energy supply systems, transportation systems, finance systems, sewer systems emergency services and lastly, basic services (Prochazkova and Prochazka, 2018). USA aligns some additional systems as critical infrastructures such as postage and shipping systems, nuclear reactors, substances and wastes, governmental facilities, critical production facilities, defense industry, national monuments and icons, dams, chemistry (ITCI, 2010:5).

In recent years, by development of ICS and smart cities, critical infrastructures have become initial components of regional and national security issues as they have been interconnected each other by internet and corporate networks (Karabacak et al, 2016:47). Most of command and control systems in critical infrastructures including nuclear weapon and reactor systems have been embedded with computer chips, GPS devices, sensors, other tracking devices and cameras (Andress and Winterfeld, 2011:5; Prochazkova and Prochazkova, 2018; ISF, 2015). Thus, critical infrastructures considered as physical systems, have now turned to cyber-physical systems (Boyes et al, 2016). This hardware today, poses new challenges particularly in smart cities, for cyber security providers and computer engineers (Ficco et al, 2017:179) as they are targets of cyber-attacks threating national security of countries.

Command and control systems are varied upon a number of frameworks such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). They are usually called as Industrial Control Systems (ICS) for an umbrella term. ICS have a vital role in delivering services to critical infrastructures such as energy, communication and manufacturing among others (Maglaras et al, 2018:42). They also monitor and supervise the critical infrastructures. In smart cities, critical infrastructures and ICS are strongly engaged each other. ICS are used in these cities to monitor and control generation and distribution plants, oil refineries, nuclear plants, public transportation system, health care systems, airway systems and etc. (Tesfahun and Bhaskari, 2016:54; Simon, 2017:2). Additionally, they engaged with robust communication network that allows citizens to reach central or local government services (Prochazkova and Prochazka, 2018).

[1] To reach the related interview, please visit, https://www.politikyol.com/politikyol-dosya-rusen-keles-akilli-kent-olmaz-kenti-yonetenler-akilli-olur/

Smart cities have interconnected networks which are providing smarter transportation and traffic management, reducing energy and power waste. U.S Department of Homeland Security released a report about the future of smart cities and analyzed critical infrastructures focusing on transportation, electricity and water infrastructures (DOHS, 2015). Table 3 below shows us the key smart technologies, their technologic developments, and their use in smart cities.

Table 3. Key Smart Technologies in Smart Cities

Sector	Cyber-Physical Technologies Examined
Transportation Systems Sector	Autonomous Vehicles Positive Train Sector Intelligent Transportation Systems Vehicle-to-Vehicle and Vehicle-to-Infrastructure
Electricity Subsector	Smart Power-Generation Plants Smart Distribution and Transmission Advanced Metering Infrastructures
Water and Wastewater Systems Sector	Smart Water Treatment Smart Water Distribution Smart Water Storage

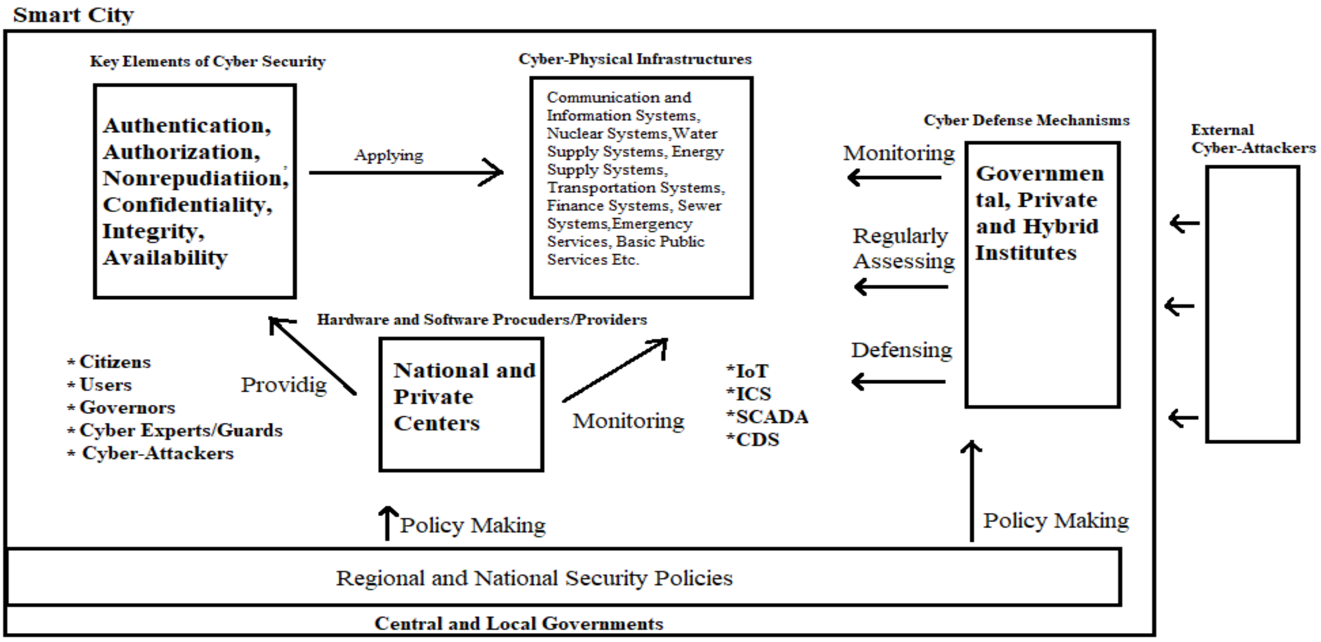
Source: DOHS, 2015:3

The Table 3 above, presents smart infrastructures that interconnected with smart devices. The use of these technologies depends on resource availability, accessibility of infrastructures and user preferences. The authorization to connection of these systems are changeable as it is vital for providing cyber security. For example, residents are allowed to connect to public transportation agenda systems to get information about number of trips, in contrary, they are not allowed to connect to the signaling infrastructure surface. Therefore, it is essential to determine different security levels and accessibility selections for different functions of these smart systems. Security preventions must provide perfect algorithms for authorization, authentication and nonrepudiation mechanisms.

IoT increases vulnerability risk in smart cities by providing data collection and allowing to be connected to critical infrastructures anytime and anywhere (Buschsieweke and Gunes, 2017). As Barnes et al. underline, vulnerabilities of ICS are increased where connectivity of cyber systems is greatest and access control of these systems is the weakest. They also emphasized that there are four domains of cyber vulnerabilities have a great risk for being a target of cyber-attacks (Limba et al, 2017). These domains are internet technologies domain (IT), ICS domain, communications domain and physical domain as the cyber security of this domains is vital for smart cities. On the other hand, Morag (2014:7) highlights six types of risk on these computer systems: 1) risk due to IT such as hardware and software, process and individuals, 2) risk due to integrated network including outside partners such as banks, financial agencies and etc., 3) risk due to third party-suppliers such as cloud providers, 4) risk due to corruption in IT equipment, 5) corruptive new, emerging technologies and 6) threats to supplier infrastructures. It is important here to underline that; domestic production of the hardware, software, cyber and physical infrastructures robust the security by preventing the insider cyber-attacks that may originated from the producers.

The types of risk are to be increased day by day and even second by second regarding to increasing interconnectivity between critical infrastructures and other cyber systems in smart cities caused by emerging IoT (PWC, 2018). As a consequence of the risks, cyber security in smart cities has begun to be a trending topic in academic researches. In order to provide the continuity of public and critical services such as governance, health care services, energy distribution, and financial services, both cyber and physical infrastructures must be protected well (Ijaz, 2016:613). Considering all the issues handled in key assets of cyber security and critical infrastructures in smart cities, a main security framework can be created as it is presented below in Figure 1.

Figure 1. Main Framework for Cyber Security of Smart Cities


Smart City
Key Elements of Cyber Security
Authentication, Authorization, Nonrepudiatiion, Confidentiality, Integrity, Availability
Applying
Cyber-Physical Infrastructures
Communication and Information Systems, Nuclear Systems,Water Supply Systems, Energy Supply Systems, Transportation Systems, Finance Systems, Sewer Systems,Emergency Services, Basic Public Services Etc.
Cyber Defense Mechanisms
Monitoring
Regularly Assessing
Defensing
Governmental, Private and Hybrid Institutes
External Cyber-Attackers
Hardware and Software Procuders/Providers
* Citizens
* Users
* Governors
* Cyber Experts/Guards
* Cyber-Attackers
Providig
National and Private Centers
Monitoring
*IoT
*ICS
*SCADA
*CDS
Policy Making
Policy Making
Regional and National Security Policies
Central and Local Governments

Opening up the framework, components in the figure can be described with their functions in the system. Key elements of cyber security are front protection keys for all the operations made by user and also administrators. These keys represent the fundamental principles of the control system. Functions of these principles are to provide good and secure access to the system. The availability of data usage, detection of the source that data received, authentication and authorization of users and administrators.

Critical infrastructures integrated with cyber networks, hardware and software, are main components of smart cities. In recent years, depending on advanced technology, cities tend to get smarter by revising their infrastructures. These revised and digitalized infrastructures constitute a big portion of cyber security of smart cities as they are main facilities for delivering public services. Therefore, they are generally first targets of cyber-attacks to collapse the smart city systems. The cyber security of these critical infrastructures become primary focus of the protection model.

National (public) and private centers are responsible for the production of hardware and software systems used in the smart cities and critical infrastructures. Additionally, they are also responsible for co-monitoring of the hardware and software they provided to system. This responsibility brings out a two-tier system of security check. The other check mechanism is carried out by cyber defense mechanisms that consist of governmental, private and hybrid institutes. The coordination between these institutes and public-private centers is the most important issue in providing cyber security in the smart cities. The institutes have operational defensing function beside monitoring and assessing. Consequently, operational strategies, systems, frameworks and standards are determined by these institutes in accordance with central and local governments' policies as well as national and international legislative regulations.

Central and local government have regulatory role in the system. With the help of the departments which are established for expertise of cyber security in central and local governments, standards of cyber security and international frameworks for smart city protection are up-to-date followed. Strategic issues such as making public policies on cyber security and design an emergency action plan are arranged in governments. In the scope of these regulations, operational actions by police and military forces against to cyber-attacks are determined. Although it isn't shown in the Figure 1, legislative body of the state is included in this component to enact needed laws to determine the details of operational and also political framework for the cyber security of smart cities.

To make the model more tangible, a scenario can be created. In the scenario, a smart city with a great cyber security is fictionalized. There are three main components in running systems of the smart city: cyber-physical infrastructures consist of integrated cyber networks, hardware and software producers/providers (HSP), defense mechanisms and awareness of key elements for cyber security. Citizens, users, governors, cyber experts/guards, local government, central government and domestic/external cyber-attackers are the actors take part in the smart city which has critical infrastructures interconnected by IoT, ICS, SCADA and CDS. According to cyber security policies made by central and local governments, defense mechanisms and hardware/software producers work collectively to prevent the cyber-attacks to the cyber-physical infrastructures. These policies are significant for determination of the main actions to provide the cyber security in the smart cities. For example, as a macro cyber security policy, central government may support the nationalization of cyber-physical infrastructures (Gocoglu, 2018), hardware and software and even ICS, SCADA and CDS. In harmony, local government may countenance national companies and use national products (if there are) in the design of smart systems in public services. Going back to the scenario, citizens, governors, and other users use smart systems to receive or deliver services. There are also domestic and external cyber-attackers who want to exploit the system. For a potential cyber security risk on the critical infrastructures, cyber defense mechanisms that consist of governmental, private and hybrid institutes are always ready as they monitor systems instantly and practice regularly to assess the defense strategies determined in accordance with regional/national cyber security policies. The sensors technology (Lucas et al, 2018; Huo et al, 2019) that allows controllers to realize degradations on systems instantly, is used all over the smart systems and critical infrastructures. Key elements of cyber security; authentication, authorization, nonrepudiation, confidentiality, integrity and availability are assimilated by these institutes in ensuring the smart systems. All smart systems are also being monitored by hardware/software producers/providers which are collectively working with defense mechanisms to establish a double-check security tracking. Most of the users in the city have capability to benefit from the advantages of smart systems and also have minimally required education of cyber- security to be aware of cyber risks concerning them. They have also opportunities to provide feedback to governors about attacks and cyber risks. In such a case, feedbacks are immediately transmitted to HSP and defense mechanisms. HSP and defense mechanisms are quite sensitive for this feedbacks beside routine cyber security controls.

The scenario presented above generate a cyber security framework for the critical infrastructures that are interconnected by IoT, ICS, SCADA and CDS in smart cities. The implementation of model requires innovator public policies made by local and central governments. On the other hand, some regulatory laws may be also required for the authorization of the institutes that will provide cyber security and take actions against the cyber-attacks. These policies and regulatory laws which can be the focus of future researches and technical details of the connection with components can be designed by the researchers from different disciplines such as computer engineering, electronic engineering and etc.

CONCLUSION

In this study, a model including main framework for providing cyber security of critical infrastructures in smart cities is presented. This framework can be modified by other researchers due to increasing cyber security needs of developing smart cities and emerging technology. As a study made by a social scientist studying in public administration discipline, technical dimension of cyber security is neglected in the model. On the other hand, the policies and regulatory laws that will provide an official basement for the model are required. For further studies, similar but comprehensive models including various dimensions of cyber security and critical infrastructures may be presented by corporate works of researchers from different disciplines. Additionally, further studies on legal and political basement of the model are needed.

The model presented in the study provides a main framework for cyber security of critical infrastructures in smart cities where IoT, ICS, SCADA and CDS are interconnected and commonly used in receiving and delivering of public services. It presents some components which are tough to be appropriate to set up cyber security systems for critical infrastructures in smart cities. The fiction visualized in Figure 1 and stimulated in the scenario, are just recommendatory and are also open for revisions in different cities depending on their capacity of technological development, the potential of cyber security risks and vulnerabilities. In a consideration that countries and cities have different technological levels of smart cities, the model may be overcapacity or insufficient for different countries. On this scope, revised models that meet the needs of specific cities may be created to provide the cyber security of critical infrastructures in smart cities.

REFERENCES

AL-MOHANNADI, Hamad, MIRZA, Qublai, NAMANYA, Anitta, AWAN, Irfan, CULLEN, Andrea and DISSO, Jules (2016), *"Cyber-Attack Modeling Analysis Techniques: An Overview",* **4th International Conference on Future Internet of Things and Cloud Workshops**. ss.69-76.

ALAVI, Amir H., JIAO, Pengcheng, BUTTLAR, William G. and LAJNEF, Nizar (2018), *"Internet of Things-enabled smart cities: State-of-the-art and future trends",* **Measurement,** S.129, ss.589-606.

ALBINO, Vito, BERARDI, Umberto and DANGELICO, Rosa Maria (2015), *"Smart Cities: Definitions, Dimensions, Performance, and Initiatives",* **Journal of Urban Technology,** S.22(1), ss.3-21.

ALLWINKLE, Sam and CRUICKSHANK, Peter (2011), *"Creating Smart-er Cities: An Overview",* **Journal of Urban Technology**, S.18(2), ss.1-16.

ANDRESS, Jason and WINTERFELD, Steve (2011), **Cyber Warfare - Techniques, Tactics and Tools for Security Practitioners.** USA: Elsevier.

BARNES, Ken and JOHNSON, Brian (2004), **Introduction to SCADA protection and vulnerabilities.** Idaho: Idaho National Engineering and Environmental Laboratory.

BATTY, Michael, AXHAUSEN, Kay W., GIANNOTTI, Fosca, POZDNOUKHOV, Bir, BAZZANI, Armando, WACHOWICZ, Monika, OUZOUNIS, Georgios, PORTUGALI, Youval (2012), "*Smart Cities of The Future*", **The European Physical Journal Special Topics**, S.214, ss.481-518.

BOYES, Hugh, ISBELL, Roy and WATSON, Tim (2016), *"Critical Infrastructure in the Future City Developing Secure and Resilient Cyber–Physical Systems*", **Critical Information Infrastructures Security 9th International Conference**, Limassol Cyprus. Springer.

BRONK, Christopher and TIKK-RINGAS, Eneken (2013), *"The Cyber Attack on Saudi Aramco, Survival",* **Global Politics and Strategy,** S.5(2), ss.81-96.

BUSCHSIEWEKE, Marian and GÜNEŞ, Mesut (2017), "*Securing Critical Infrastructure in Smart Cities: Providing Scalable Access Control for Constrained Devices*", **28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications.**

CARAGLIU, Andrea, BO, Chiara Del and NIJKAMP, Peter (2011), "*Smart Cities in Europe",* **Journal of Urban Technology**, S.18(2), ss.65-82.

CLARK, David, BERSON, Thomas and LIN, Herbert S. (2014), **At the Nexus of Cybersecurity and Public Policy. Computer Science and Telecommunications Board.** National Research Council, Washington DC: The National Academies Press.

CSIS (2019). **Significant Cyber Incidents Since 2006.** Center for Strategic and International Studies.

ÇELİK, Ahmet (1998), *"Some Notes On the Information Society",* **Hacettepe University Journal of Faculty of Letters,** S.(15)1, ss.53-59.

DEGBELO, Auriol, GRANELL, Carlos, TRILLES, Sergio, BHATTACHARYA, Devanjan, CASTELEYN, Sven and KRAY, Christian (2016), *"Opening up Smart Cities: Citizen-Centric Challenges and Opportunities from GIScience",* **International Journal of Geo-Information,** S.5(16), ss.1-25.

DENNING, Peter J. and DENNING, Dorothy E. (2010), "*The Profession of IT: Discussing Cyber Attack*", **Communications of the ACM**, S.53(9), ss.29-31.

DOHS (2015), **The Future of Smart Cities: Cyber-Physical Infrastructure Risk**. U.S: Department of Home Land Security.

DWEVEDI, Rajneesh, KRISHNA, Vinoy and KUMAR, Aniket (2018), "*Environment and Big Data: Role in Smart Cities of India*", **Resources**, S.7(64), ss.1-10.

FARHAT, Vince, RAYSMAN, Richard and CANALE, John (2016), **Cyber Attacks: Prevention and Proactive Responses. Practical Law**. Thomson Reuters.

FICCO, Massimo, CHORAS, Michal and KOZIK, Rafal (2017*), "Simulation platform for cyber-security and vulnerability analysis of critical infrastructures"*, **Journal of Computational Science**, S.22, ss.179-186.

FORBES (2019), **Cities Are Facing A Deluge Of Cyberattacks, And The Worst Is Yet To Come**, Cesar Cerrudo Forbes Councils Forbes Technology Council.

GEERS, Kenneth (2010), "*The challenge of cyber attack deterrence*", **Computer Law & Security Review**, S.26, ss.298-303.

GIL-GARCIA, J. Ramon, PARDO, Therasa A. and NAM, Taewoo (2015), "*What makes a city smart? Identifying core components and proposing an integrative and comprehensive conceptualization*", **Information Polity**, S.20, ss.61-87.

GOCOGLU, Volkan (2018), "*The Assessment of Turkey's Cyber Security Policies in the Context of Public Policy Analysis"*, **Unpublished Doctoral Thesis**. Hacettepe University Institue of Socail Sciences, Ankara.

GUL, Huseyin (2018). *"Impact of Digitization on Public Administration, Public Policy and Research in These Fields"*, **Yasama Dergisi**, S.36, ss.5-26.

GRAHAM, James, HOWARD, Rick and OLSON, Ryan (2011), **Cyber Security Essentials**. U.S. Taylor and Francis Group.

HOLLANDS, Robert G. (2008), "*Will the real smart city please stand up?*", **City**, S.12(3), ss.303-320.

HUO, Da et al. (2019), "*Chance-Constrained Optimization for Multienergy Hub Systems in a Smart City*", **Transactions on Industrial Electronics**, S.66(2), ss.1402-1412.

IJAZ, Sidra, SHAH, Munam Ali, KHAN, Abid and AHMED, Mansoor (2016), "*Smart Cities: A Survey on Security Concerns*", **International Journal of Advanced Computer Science and Applications**, S.7(2), ss.612-625.

ISF (2015), "*Smart City Security: Building for the future",* **Information Security Forum**.

ITCI (2010), **The Protection of Critical Infrastructures**, Information Technology and Communication Institution, Ankara.

KARABACAK, Bilge, YILDIRIM, Sevgi Ozkan and BAYKAL, Nazife (2016), "*A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness*", **International Journal of Critical Infrastructure Protection**, S.15, ss.47-59.

KARABACAK, Bilge, YILDIRIM, Sevgi Ozkan and BAYKAL, Nazife (2016), "*Regulatory approaches for cyber security of critical infrastructures: The case of Turkey*", **Computer Law & Security Review**, S.32, ss.526-539.

KORFF, Douwe (t.y.), **Cyber Security Definitions**, Associate of the Oxford Martin School of the University of Oxford's Global Cybersecurity Capacity Centre, UK.

LIM, Chiehyeon, KIM, Kwang-Jae and MAGLIO, Paul P. (2018), "*Smart cities with big data: Reference models, challenges, and considerations*", **Cities,** S.82, ss.86-99.

LIMBA, Tadas, PLETA, Tomas, AGAFONOV, Konstantin and DAMKUS, Martynes (2017), "*Cyber Security Management Model for Critical Infrastructure",* **The International Journal Entrepreneurship and Sustainability Issues**, S.4(4), ss.559-573.

LUCAS, Clemencio Morales, LOPEZ, Luis Fernando Mingo and BLAS, Nuria Gomez (2018), "*Natural Computing Applied to the Underground System: A Synergistic Approach for Smart Cities*", **Sensors**, S.18, ss.1-20.

MAGLARAS, Leandros A., KIM, Ki-Hyung, JANICKE, Helge, FERRAG, Mohamed Amine, RALLIS, Stylianos, FRAGKOU, Pavlina, MAGLARAS, Athanasios and CRUZ, Tiago J. (2018), "*Cyber security of critical infrastructures*", **ICT Express**, S.4, ss.42-45.

MARSH and MCLENNAN (2017), **Cyber Threats: A Perfect Storm About to Hit Europe?**, FireEye.

MECEK, Mehmet and KOCAKULA, Özge (2019). *"E-Devlet ve E-Yönetişimde İdari, Siyasi ve Etik Sorunlar"*, **E-Yönetişim** (Ed. Bekir PARLAK and Kadir Caner DOĞAN), Beta Yayınları, İstanbul.

MORAG, Nadav (2014), **Cybercrime, Cyberespionage, and Cybersabotage: Understanding Emerging Threats**, Colorado Technical University, USA.

MUSA, Sam (2016), *"Smart Cities - A Roadmap for Development"*, **Journal of Telecommunications System & Management**, S.5(3), ss.1-3.

NAPHADE, Milind, BANAVAR, Guruduth, HARRISON, Colin, PARASZCZAK, Jurij and MORRIS, Robert (2011), *"Smarter Cities and Their Innovation Challenges"*, **Computer**, ss.32-39.

NCS (2018), "*National Cyber Strategy*", **Washington: The White House**, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Erişim tarihi: 31.01.2019).

NEIROTTI, Paolo, MARCO, Alberto, CAGLIANO, Anna Corinna, MANGANO, Giulio and SCORRANO, Francesco (2014), "*Current trends in Smart City initiatives: Some stylised facts"*, **Cities,** S.38, ss.25-36.

OSMAN, Ahmed M. Shatat (2019), *"A novel big data analytics framework for smart cities"*, **Future Generation Computer Systems**, S.91, ss.620-633.

PCM (2013), **National Strategic Framework for Cyberspace Security**, Presidency of the Council of Ministers, Italy.

PERERA, Charith, ZASLAVSKY, Arkady, CHRISTEN, Peter and GEORGAKOPOULOS, Dimitrios (2014), *"Sensing as a service model for smart cities supported by Internet of Things"*, **Transactions on Emerging Telecommunications Technologies**, S.25, ss.81-93.

PROCHAZKOYA, Dana and PROCHAZKA, Jan (2018), **Smart Cities and Critical Infrastructure**, Smart Cities Symposium Prague, ss.1-6.

PWC (2018), **Creating Cyber Secure Smart Cities**, PWC, ss.1-32.

RAMOS, Francisco, TRILLES, Sergio, TORRES-SOSPEDRA, Joaquin and PERALES, Francisco J. (2018), *"New Trends in Using Augmented Reality Apps for Smart City Contexts"*, **International Journal of Geo-Information**, S.478, ss.1-23.

ROCHE, Stephane, NABIAN, Nashid, KLOECKL, Kristian and RATTI, Carlo (2012), *"Are 'Smart Cities' Smart Enough?"*, **Spatially Enabling Government, Industry and Citizens**, ss.215-235.

SADIOGLU, Ugur and ERDINCLER, R. Erkut (2018), *"Akilli Kentler ve Turk Kentleri Için Politika Onerileri"*, **Küreselleşme Sürecinde Yerel Hizmet Yerel Siyaset** (Ed. Ayşegul MENGI and Deniz ISCIOGLU), Ankara University Press, Ankara.

SAHIN, Savas Zafer (2018). *"Evolution of the Relationship between Urban Planning and Urban Infrastructure"*, **Planlama**, S.28, ss.6-11.

SIMON, Tobby (2017), "*Critical Infrastructure and the Internet of Things"*, **CIGI: Global Commission on Internet Governance**, S.46, ss.1-11.

SNYDER, Don, POWERS, James D., BODINE-BARON, Elizabeth, FOX, Bernard, KENDRICK, Lauren and POWELL, Michael H. (2015), **Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles**. RAND, CA.

TESFAHUN, Abebe and BHASKARI, D. Lalitha (2015), *"A SCADA Testbed for Investigating Cyber Security Vulnerabilities in Critical Infrastructures"*, **Automatic Control and Computer Sciences**, S.50(1), ss.54-62.

TOHME, Walid, LINDEYER, Jeremy, HARB, Imad and PAPAZIAN, Sevag (2015), "*Cyber security in the Middle East A strategic approach to protecting national digital assets and infrastructure*", **E-Report**, https://www.strategyand.pwc.com/media/file/Cyber-security-in-the-Middle-East.pdf (Erişim tarihi: 20.01.2019).

TOWNSEND, Anthony M. (2013), **Smart cities: Big data, civic hackers, and the quest for a new utopia**, WW Norton & Company, New York.

WEBSTER, Frank (2014), **Theories of the Information Society**. Routledge.

WIENER, Norbert (1948), **Cybernetics, or Control and Communication in the Animal and the Machine**, MIT Press, Cambridge (UK).

WOODHEAD, Roy (2018), "*Building a Smarter City*", **International Journal of Technology**, S.7, ss.1509-1517.

WU, Shiann Ming, GUO, Dongqiang, WU, Yenchun Jim and WU, Yung Chang (2018), *"Future Development of Taiwan's Smart Cities from an Information Security Perspective"*, **Sustainability,** S.10, ss.1-18.

YIGITCANLAR, Tan, KAMRUZZAMAN, Md., FOTH, Marcus, SABATINI-MARQUES, Jamile, DA COSTA, Eduardo and LOPPOLO, Giuseppe (2019), *"Can cities become smart without being sustainable? A systematic review of the literature"*, **Sustainable Cities and Society**, S.45, ss.348-365.

YIN, Chuantao, XIONG, Zhang, CHEN, Hui, WANG, Jingyuan, COOPER, Daven and DAVID, Bertrand (2015), *"A literature survey on smart cities"*, **Science China Information Sciences**, S.58, ss.1-18.