The Impact of Smart City Model on National Security

Ehab Khalifa

Smart cities could help overcome traditional problems of big cities, such as pollution, traffic congestion and administrative corruption. They can stimulate economic productivity, accommodate population growth, and make lives more convenient, but at the same time, they raise many security threats to national security.

Daily life needs in smart cities are based on information and communication technologies. Houses, infrastructure, transportation, communication, government services, as well as commercial and industrial services, etc. are controlled by smart systems dependent upon artificial intelligence and the Internet of things[1]. If these services are targeted by a successful cyber-attack, the consequences in that case would be unaffordable to national security and to people's lives.

This article seeks to analyse the impact of smart cities on national security, and it comes in three main sections. The first one defines smart cities and its different models, the second one analyses the impact of adopting the smart city model on national security, and the conclusion tries to provide some recommendations of how to decrease national security risks in the smart city.

Keywords: smart cities, national security, cyber security.

Introduction

Many countries around the world have adopted smart city models which depend on cloud storage platforms, Internet of things and artificial intelligence systems, with the aim of improving the quality of live

Ehab Khalifa. The Impact of Smart City Model on National Security. *Central European Journal of International and Security Studies* 14, no. 1: 52–73.

for its citizens, opening new opportunities for economic development, and making the best use of available resources.

In smart cities, infrastructure such as communication systems, transportation systems, power stations and all government services are dependent on information communication technology. However, this gives rise to particular fears and threats. For instance, cyberattacks on the city's infrastructure can mean ending the lives of large numbers of people in a matter of no time, in the event the cyberattacks target airlines, railways, self-driving cars, hospitals, automated bascule bridges or traffic lights. This is an immediate threat to the country's national security.

Apart from this, smart cities can be targeted by different kinds of cybercrime, such as cyber scams, piracy, blackmail and online sexual harassment. Credit cards, bank accounts, and the financial sector, not only of the smart city but also of the entire country, can be threatened by cyber-attacks. The situation becomes all the more dangerous during conflict or war, if the state has been targeted by its enemies or rival regional or international powers, as cyberattacks in this case would be a lethal weapon targeting smart cities and highly affect national security.

Consequently, many countries are changing their national security strategies so that they should encompass such concepts as cyber power, cyber deterrence and cyber conflict[2], to protect all the potential targets in the event of cyber warfare.

The 'smart cities' concept is relatively new, associated with the emergence of smart growth in the 1990s, and it was first used by academics primarily concerned with urban planning, with the aim of describing the rejuvenation of urban infrastructures through incorporating communication and information technologies into them[3]. Technical dimensions took precedence as the prime concern was finding the optimal way to incorporate information and communication technologies in urban planning.

Despite the widespread popularity of the concept, there is no clear-cut definition of what a smart city is[4]. This lack of agreement on what a smart city is has much to do with the existence of many terms likely to be mistaken for synonyms of the term 'smart cities' (e.g. intelligent cities, digital cities, virtual cities, etc.). In fact, the term 'smart' is opted for simply because it covers technical, social, architectural and economic dimensions.

Smartness is mainly based on the integration between technical dimensions (i.e. devices, systems, sensors and artificial intelligence), social dimensions (i.e. interpersonal relationships) and physical planning (as related to the technological constituent). Intelligence, by contrast, exclusively has to do with the technical aspects pertaining to developing systems and applying machine learning, so that machines can make autonomous decisions, hence the term 'artificial intelligence'. As for the term 'digital city', it refers to the broadband communication services incorporated in the infrastructure so as to facilitate communication between citizens, government and businesses. Therefore, all intelligent systems are digital by default. Finally, the term 'virtual city' refers to the physical/virtual dichotomy, regarding the city as composed of a physical component, which, in turn, consists of systems, devices and infrastructures, and a virtual component, namely, the virtual space which acts as a medium joining all the different elements together. It is noteworthy that the term 'smart city' covers all the concepts and elements (i.e. systems, infrastructures, and Internet) in addition to the individuals, the essence of the smart city. The term also covers the social and urban dimensions[5].

The smart city is not characterized by technology and information knowledge only, it also characterized by certain unique social features, one of which is its social infrastructure, which consists of intellectual capital and social capital. Another is its environment, which encourages innovation through enhancing education, learning, acculturation, knowledge, human relationships, policies and laws, and supports human intelligence and urban development processes in general.

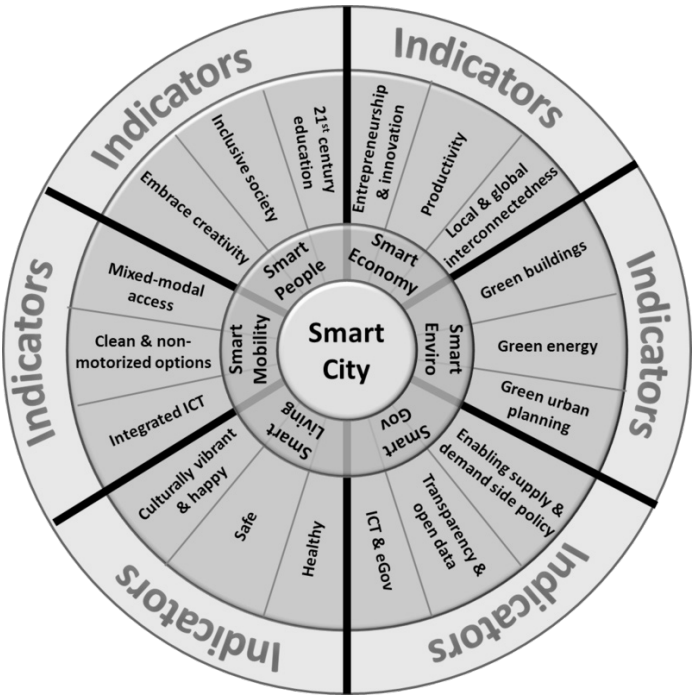
The following are the main criteria and dimensions of smart cities:

- A smart city depends on high technology, which helps connect individuals, information and city components efficiently, hence the city's sustainability, the innovativeness and competitiveness characterising trade in it, and the high quality of life in it[6].
- A city becomes smart when all the available resources and technologies are systematically used to develop the urban centers so that they should become integrated, habitable and sustainable[7].
- A smart city is typically equipped with information and communication technologies, which provide citizens with services in digital and electronic forms[8].
- The underlying concept of smart cities is that of multi-dimensional development. Information and communication technolo-

gies are simply mechanisms or tools for facilitating the development process in the state[9].

- A smart city is not all about modern technology; it must provide its inhabitants with the highest quality of life, and create opportunities to make life patterns more harmonious so as to achieve development for those who live in it[10].
- A city is smart when investment in human and social capitals and in the structure of the traditional means of communication (i.e. transportation) and modern means of communication (i.e. information and communication technologies) contributes to enhancing sustainable economic development and achieving a high quality of life. This is achieved through effective management of natural resources, which, in turn, is brought about by teamwork, commitment and cooperative, participation-based management[11].
- A smart city functions in an ambitious, creative way. This applies to its economy, population, governance, mobility, environment and lifestyle, and depends on the positive participation of able, enlightened, independent citizens in the decision making process[12].

Fig 1. Cohen Smart City Wheel



Study framework and methodology:

This section presents a Smart City model that the article builds upon. It is a framework developed by Boyd Cohen called the 'Boyd Cohen Wheel'[13], the model encompassing the various elements of smart cities, indicated in chart No (1), which has gained wide acceptance in academic circles as a model for studying smart cities. It was translated into many languages, such as French, Swedish, Dutch and Spanish. According to Cohen, the elements of a smart city are the following[14]:

1. **Smart Economy:** The smart economy is characterized by a high degree of creativity, manifest in employing advanced technologies in industrial production, modernizing services and accelerating production and industrialization processes through depending on machinery. It also depends upon incorporating the national economy into the global economy and revitalizing the smart city's economy so that it can live up to competition. The main requirements for creating a smart economy are entrepreneurship, innovation, productivity, and local and international solidarity and cooperation.
2. **Smart Transportation:** This means improving the quality of transportation services inside the city, as well as enhancing the traffic sector and related surveillance processes. This can be achieved through utilizing modern technologies, such as using surveillance cameras and electronic monitoring techniques. Applications which analyze information immediately should also be used, so that the right decision can be arrived at in the right time. In addition, different means of transportation should be available inside the city, including public transportation, private sector transportation, environment-friendly cars, autonomous cars, as well as bicycles.
3. **Smart Environment:** The first step to creating a smart environment is the clean urban planning of the city. This depends upon utilizing information and communication technologies and monitoring techniques in distributing public areas and green areas around the city. It also has to do with choosing styles of building that would achieve the utmost degree of efficiency, effective management of natural resources, reducing gas emission, and cleaning water canals and activating them so as to achieve sustainability. The indices of a smart environ-

ment are: green buildings, clean energy, and balanced urban planning.

4. **Smart People**: The citizen is an important element of the process of development in the smart city. In fact, the ultimate goal of making cities smart is improving the quality of life for the citizen. The citizens of a smart city are typically well-educated and open-minded towards the Other. They also accept difference and enjoy a high degree of personal flexibility. They should be encouraged to take part in the decision-making processes in the society of the smart city, using social platforms and their different channels. The indices of a smart citizen are innovation-based education, a culture of acceptance and openness, and giving priority to creativity and uniqueness.
5. **Smart Life:** This means improving the environment and the quality of life for the citizens, and can be achieved through encouraging the citizens to connect with one another efficiently and enhance the way they manage their surroundings (e.g. their houses, personal belongings, companies, businesses, etc.) through depending on the Internet of things and Internet-based social platforms. This would create a lively, healthy and happy lifestyle.
6. **Smart Government:** Technology in the smart city enhances connections inside the government itself, as well as between the different government organs, the government and the citizens and the government and the different state sectors (commercial, social, etc.). The government services and any information citizens need can be accessed through the Internet. This enhances government accountability and transparency and facilitates data availability. It also makes it easier for the government to respond quickly to the society's needs.

It is worth noting that Cohen model has one strong weakness, which is that it does not include Smart Energy (Smart Grids) as an element, while the Smart Energy and Smart Grids are critical to National Security.

Also, there are several paradigms and approaches that tried to analyze and understand smart cities before Cohen. One of them was introduced by The Center of Regional Science in Vienna University, which focused on six different elements for a city to be smart[15]:

- **Smart Economy,** fully digitalized systems characterized by Innovative spirit,

- **Smart People,** have a certain Level of qualification and are interested in learning,
- **Smart Governance**, that depends on digital democracy,
- **Smart Mobility,** that depends upon transport infrastructure and logistic services,
- **Smart Environment,** based on effective management of resources and achieving sustainability,
- **Smart Living** depending on achieving security and a high quality of life.

Another paradigm provided by Professor Nicos Komninos depends on the following four components[16]:

- infrastructure including electricity and internet networks necessary for founding a city which is based upon knowledge and information,
- using the internet and digital technology in changing the style of living and working in the city.
- incorporating communication and information technologies into the infrastructure of the city.
- making information and communication technologies available for the citizens so as to enhance creativity, education and learning.

However, as mentioned before, this study adopts the Cohen Wheel model, which seems more recent and comprehensive regardless of its limitations.

The relationship between the smart city model and national security

Smart cities are classified into different models in the light of four criteria - each model has a direct impact on national security. The first of these is the kind of technology used in the smart city, which can be either closed source technology that can only be developed by the company that created it, or an open source technology that any developer or programmer can work on. The second criterion is the agent(s) contributing to the process of building the city whether it is the government or the private sector alone or the private sector in collaboration with civil society, working in accordance with a government strategy. The third is the nature of the sector that the city in question serves. This can be a specialized sector, such as the energy sector, or general sectors of the city, targeting the population

as a whole. The fourth, and last, criterion is the "construction type"; while some smart cities are built from scratch, others are simply old, "classical" cities that have been turned into smart ones**.** They are indicated in chart No (3).

1. Technology used in the smart city:
Two kinds of cities can be identified in this respect. These are:

A. Closed source smart cities:
Cities that are built and developed by only one company, such as IBM or Cisco, so that no other company can further work on these cities, unless it cooperates with the company that "originated" them. The originating company does not make the information it receives from the sensors in the city available to the programmers and developers, and so they are not allowed to develop new technologies or contribute to innovations of any kind to the city. The company also does not allow the platforms used in running the city to share data with the platforms of other companies. In other words, the system that the company uses to operate the city it creates is also its own creation, and is typically a completely homogenous, closed system that never accepts any technologies from outside the protocol designed by the company[17]. A case in point is Songdo, a smart city built by Cisco in South Korea, specialized in serving the trade and business sector[18].

B. Open source smart cities:
Open source technology is that which can be developed and updated by more than one company, or individual. New technologies can be accepted by the system. A case in point is the FIREWARE initiative, a non-profit European initiative funded by governments, international organization, and top communication companies in Europe. The aim of the initiative is to develop sensor devices and systems and introduce them on a wide scale into the countries of the EU. The systems herein mentioned are open source systems; the information collected in the city is made available to the developers via public API interfaces, which helps them develop smart technologies and solutions for the city. Different sectors of the society would take part in the process of planning, founding and developing[19]. Among the cities that adopted this technology are New York and Barcelona[20], the latter of which placed second in the rankings of smart cities in 2016[21].

It is noteworthy that open source cities cost less, compared to closed source ones, as far as systems and technologies are concerned. The reason is that maintenance and development are not the responsibility of one company, but instead everyone's. This makes it possible for more than one company to take part in developing the city, and the cost is paid by the sector that needs maintenance or developing.

Instead of having to continue dealing with one company regardless of cost, the government can choose from different offers. Individuals can take part in building the city, through buying the systems most affordable to them (and compatible with the standard specifications of the city), installing and using them wherever they like[22], without having to ask for the help of one company that monopolizes the processes of installing and operating systems.

This model is supported by some international non-profit laboratories and organizations, such as the Public Lab (short for the Public Laboratory for Open Technology and Science), an international community of researchers and programmers engaged in developing open source applications and tools with the aim of making them available to all researchers all over the world so that they can also take part in developing, testing and experimenting with them. Fab Lab Barcelona goes so far as to making it possible for the citizens to take part in the processes of developing and testing, with a view to enhancing citizen participation and developing the concept of the smart citizen. This is achieved through the use of DIY techniques (where DIY is short for Do It Yourself)[23].

The smart city model according to technology used has a direct effect on national security. Closed source smart city models raise questions regarding security and privacy, from one side the city developer in this model is one company who owns the operation systems, and so has access to all of the information of the cities, knows where is the weaknesses and from where the danger can come. From another side it could also leave a backdoor to have illegal access to information when needed.

Another concern arises if the developing company is not from the same country (which usually happens). In that case, the relationship could subject to the influence of other international actors. This doesn't mean that open source smart city model is better - although it is characterized by more transparency as it involves making designs and codes available for everyone, the availability of designs, codes, and

Fig 2. Smart city models

information could make it very difficult to prevent hacking and digital piracy (see Fig 2).

2. Agents participating in building the city:
According this criterion, smart cities can be classified into three stakeholders:

A. Government:
Smart city development often requires involvement of a government body to make deliberate choices and engage in city challenges in the most effective way[24]. It has the legal authority, financial resources, and the strategic vision needed in the development process. It also encourages the private sector and civil society to fulfill the construction of the smart city.

A. Private sector construction:
Where the private sector primarily means the top technology companies in the world, which are capable of building the city and providing all its technological requirements, such as real-time traffic control systems, crime detection and prevention systems, security cameras, networks, communication lines and environmental information systems[25].

B. Civil society participation:
Citizens, civil society and academic society cooperate with the private sector in building, developing and managing smart cities. This is achieved through enabling programmers, pirates and developers to innovate and experiment in the city, and present solutions and suggestions. Thus, managing the smart city becomes some sort of collaborative work, where everyone has his/her fair share of responsibility[26].

This type of smart city makes it possible for small companies, civil society organizations, universities, and government institutions to launch initiatives that can accelerate the process of changing the city in question into a smart city. For example, the efforts of university teachers and students can be directed towards developing technologies, software and devices in university laboratories that can be useful to the change process.

But this model also brings national security concerns - the agents participating in development process will have to deal with massive quantities of sensitive data collected from both individuals and sensors, which can be misused by them or by third parties and affect national security directly.

3. Purpose of building a smart city:
A smart city can be a millennial city that serves all the individuals in the society, or specialized/sectorial city, which serves specific sectors in the country such as the energy sector:

A. Millennial cities:
These are either cities originally built to be millennial cities, or cities turned into millennial cities. They provide the daily needs of all those who permanently reside in them. Examples of these are Singapore and New York. It is noticeable that we are talking here about real cities inhabited by citizens involved in natural human activities.

B. Sector cities:
These are cities built with the aim of serving a certain sector (industrial, commercial, etc.). People, therefore, do not permanently live in them. Such cities cannot accommodate a large population in the first place; they are built with a view to provide a suitable environment where a certain sector can exercise innovation and creativity. A case in point is PLanIT Valley, a Portuguese smart city specialized in IT technology and the Internet of things[27].

This type of smart city lacks the 'human feel' of traditional cities. This is, in fact, one of the main criticisms of it; human beings are the essence of the city, and their welfare should be the ultimate goal, or else the city would lose its raison d'être[28].

A cyber-attack on the millennial city could affect large number of people. Also adopting sectorial smart city model that is the focus of specific sectors like energy or communication could be a real threat because the whole sector could be affected, resulting in huge damage.

4. Construction type of smart city:
Some cities are originally built as smart cities; others are traditional cities that are turned into smart ones:
A. New cities:
These are cities built from scratch, on a vacant, uninhabited plot of land. It is built either by the private sector or by both the private sector and the civil society. It originates as a smart city, capable of fulfilling certain purposes. An example is Masdar, an Abu Dhabi-based smart city.

B. Legacy cities:
Some legacy cities are turned into smart cities. A case in point is Manchester in the UK, and Monterrey in Mexico[29]. In such cases the existing lifestyle, as well as the existing infrastructure (e.g. buildings, roads, services, etc.) should be taken into consideration, so that the technol-

ogy used should be suitable for the city's status quo. In that case some variabilities and gaps could be left unintentionally, resulting in a national security risk.

Applying the "Cohen" model to national security risks and threats:

When applying the "Cohen" model for smart cities to national security, several risks arise:

1. Smart Economy Risk The dilemma that different needs of everyday life in

- Direct Economic risk through hacking banking and financial systems:

Depending on smart technologies is a double-edged weapon as far as banking and finance systems are concerned. On the one hand, these systems facilitate financial transactions and transfers between accounts. This has a positive impact on investment and development. On the other hand, hacking these systems is a blatant threat to the stability of the financial transactions, which detracts from the city's ability to achieve one of its most important goals, contributing to improving the economic situation in the country and achieving development.

As smart cities are primarily economic and financial centers, pirates' success in hacking their banking and financial systems would result in transferring billions of dollars from various clients' accounts in a matter of seconds. Apart from the economic loss, the transferred money may be used in financing illegal activities or terrorism, which means that another national security threat can be added to the list[30].

- Indirect Economic risk resulting from losing confidence in the economic and financial sector:

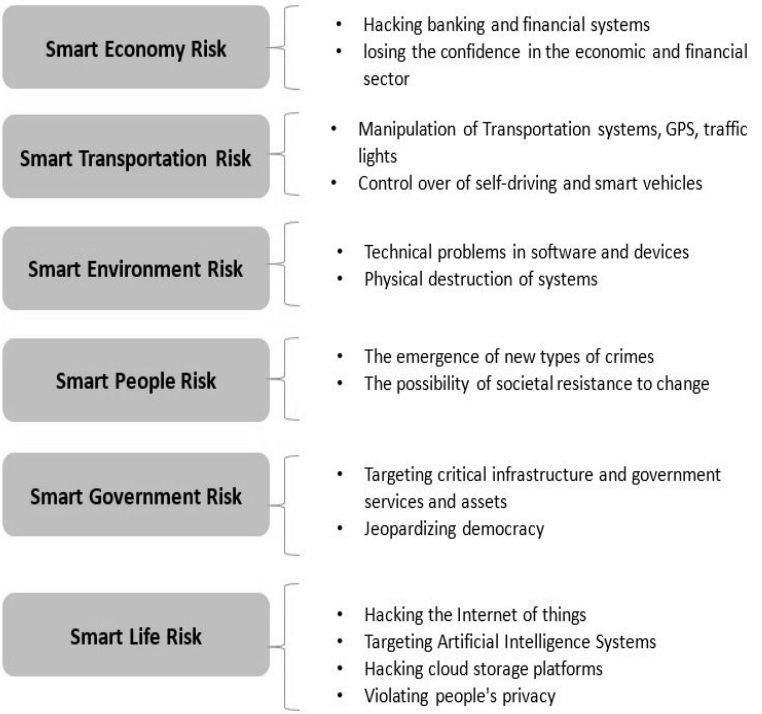
Hacking anything has economic consequences. A study by Oliver Wyman has found that cybercrime will cost $1 trillion annually by 2022[31]. *Harvard Business Review* expects that the next economic crisis will not come from financial shock, but from a cyber-attack that causes disruptions to financial services capabilities, especially payments systems, resulting in a loss of confidence in the global financial services system[32].

2. Smart Transportation Risk

- Manipulating traffic and transportation systems:

Transportation systems have become more digitalized, with a wide range of data flowing across systems, tracking and monitoring both

Fig. 3. Applying "Cohen" model for smart cities on national security



digital and physical networks. As more devices, control systems, and transportation means are connected online, more disruption to physical assets is possible because of a cyber-attack[33].

• Smart and self-driving vehicles control over:

Targeting the GPS- upon which planes, self-driving cars and different vehicles greatly depend- or hacking the traffic system and manipulating traffic lights, for instance, can result in serious consequences; in addition to human casualties, the movement of traffic in the city can be paralyzed, let alone the economic losses that can result. Losses would be even heavier if the targets were power and gas stations, as life in the city mainly depends on energy[34].

3. Smart Environment Risk

• Technical problems in software and devices:

A smart city is primarily a technology-based city. Essential to its existence are software, cables and devices, all of which, unfortunately, are liable to damage, defects and jamming.

• Physical destruction of systems:
The reasons could be technical, but they can also be environmental. Damage can be caused, for instance, by temperature change, natural disasters or intentional intervention with the aim of destroying the city's smart system. Another reason is defects in the city's software or in the communication networks, the wireless Internet or the GPS. This would of course paralyze life in the city[35].

4. Smart People Risk
A smart city can face nontraditional threats, like the attempts to change the value system of a city so as to turn it into a cosmopolitan system meeting resistance on the citizens' part. This can result in division among the citizens, who would be afraid for their privacy and freedom

• The emergence of new types of crimes:
Technology is always a two-edged weapon. It is true that it can be in humanity's service but it is also true that it can be threatening and destructive. Total dependence on technology in smart cities can lead to a rise in the numbers of certain crime types, such as online harassment and blackmail. It may also result in the emergence of crimes not known before. For instance, 3D printers can be used, either by ordinary people or by terrorists, in making weapons. They can also be used in forging products (and therefore infringing intellectual rights or counterfeiting antiques[36]. Additionally, commercial drones can be equipped with weapons or bombs and programmed to attack people or civil aircraft, or to violate people's privacy by taking their photos[37].

• The possibility of societal resistance to change:
Smart cities attract the best minds in all fields, either from the country where the smart city is built or from other countries. In fact, attracting them is the real goal behind building the smart city. However, the citizens of a traditional, relatively homogeneous, city may not at first accept the idea that their city, in the process of changing into a smart city, would be home for people from different cultural backgrounds. These changes are likely to meet resistance, notably in societies where the nationalist spirit is strong. Foreigners taking the important posts in the city can provoke nationalist feelings and lead the citizens to reject the new cultures. However, it is noteworthy that such a threat is more likely to occur in traditional cities that are changed into smart cities, whereas smart cities which are built from scratch (where they

are no natives who would adopt xenophobic attitudes to foreign cultures) would not likely face such a problem.

5. Smart Life Risk

• Hacking the Internet of things:

Internet of things devices are typically popular in smart cities, being used in institutions, sensors, companies, houses, restaurants, cafes and even streets. They are, in short, indispensable in smart cities. Despite their great importance, these devices constitute a threat to the smart city's security; they are present throughout the city; they are all connected to the Internet, but they are not particularly very well secured. Therefore, if they were hacked through viruses, worms and Trojans, they would immediately turn into a 'smart' army that can destroy the critical infrastructure, including banks, power stations, dams, hospitals and communication systems. They can also paralyze financial and banking services, and all government services. Even more dangerously, they can destroy the Internet itself[38].

• Targeting Artificial Intelligence Systems:

Smart cities depend on AI technologies, such as robotics systems, in factories, companies, stores, automated answering systems, self-driving cars, and drones. If these systems were hacked, self-driving cars, for example, could be re-programmed to run people over, and it would be extremely difficult to know who the perpetrator was. Similarly, drones and robots can be re-programmed, at least in theory, to kill and destroy. It is not difficult to see why hacking these systems can be one of the most serious dangers which humans can face[39].

• Hacking cloud storage platforms:

Cloud storage platforms are among the centers used for managing smart cities; they are where all the information coming from the sensors all over the smart city, and from the many government institutions, are stored. Different pieces of information are linked so as to enhance the decision-making processes and reduce the technical support cost. Despite its many advantages, these storage clouds raise many questions that have to do with security. Were they hacked, much sensitive information concerning the country and its citizens would be disclosed, with dangerous consequences.

• Violating people's privacy:

The privacy of individuals is one of the controversial issues concerning smart cities. The citizens' data, digitized and stored on smart phones,

clouds, etc., are always in danger of violation from inside the city or from outside it, either by organized crime groups or by other countries. Credit card information, GPS information, biometric data, medical data, etc. are always available for the companies that operate the smart city. Besides this, people may feel uncomfortable because of the security cameras that would meet them wherever they go, hence the classical question: must we jeopardize people's security to protect their freedom or must we restrict their freedom to ensure their safety?[40]

6. Smart Government Risk

• Targeting critical infrastructure and government assets:

A smart city's infrastructure depends on smart technologies that require uninterrupted Internet connections. These technologies are used in power stations, petroleum refineries, nuclear reactors, chemicals factories, hospital systems, finance and banking services, communication and transportation systems, traffic, radio and TV broadcasting services, navigation, air navigation and satellites. Targeting these systems only takes minutes but can cause heavy casualties[41].

The US Department of Homeland Security broadcasted a video of a staged cyberattack on a power grid in which a computer virus was used. The virus was able to tamper with the power frequency. As a result, the power grid eventually exploded. Most critical energy sectors, such as electricity, petroleum, dams and nuclear power stations use Supervisory Control and Data Acquisition (SCADA) systems, which are huge computer systems for controlling main power stations. If these systems were hacked the consequences would be catastrophic[42].

All government services in the smart city are potential targets for such threats, as they are based on the smart government model, where citizens can use all services and do all transactions via smart phones and the Internet. Targeting these services means paralyzing government services and institutions, which would be catastrophic to millions of citizens[43].

• Jeopardizing democracy:

The fact that all data would be in the hands of the smart city's managers can constitute a serious threat to democracy. The local, or the central, government, enjoying full access to citizens' data, would be able to have full knowledge of their interests, attitudes, preferences and priorities through analyzing data. This means that power and authority would be monopolized by those who have control over this data. This

is likely to endanger democracy as this information can be used in manipulating elections in favor a certain candidate, which is a dire threat to the integrity of the electoral system[44].

In addition, governments of other countries may begin online propaganda campaigns to influence the citizens. Russia, for instance, was accused of helping Trump to win the American presidential elections against the Democratic candidate Hilary Clinton by funding a publicity campaign with the aim of making people vote for the Republican candidate.

In the end, smart cities would be more appealing to cyber criminals and cyber terrorism to conduct their operations, the harm that can be expected as a result from a cyber-attack on a smart city conducted by state or non-state actors can affect directly the state national security. The confidentiality, integrity and availability of all governmental and private services can be threatened. In addition, privacy and individual personal freedom could be affected. The quality of life that the smart city aims to achieve would be at risk, and new national security strategies that can deal with this kind of new threats are needed.

Conclusion

Smart cities represent a lifestyle totally based on making use of such unprecedented technological developments as artificial Intelligence systems, the Internet of things and big data, with the aim of having high quality of life for people. However, they create several threats to national security, which make the smart city model questionable from security perspective. At the same time, governments could reduce the security risk to smart cities through adopting some measures, and then making the best use of the smart city mode. These measures can be achieved through three different levels which work together:

A. The technical level:

This is most complicated, costly, and dangerous level, and includes plans, systems, and resources that cooperate to achieve state resilience and flexibility in cyberspace. It involves the following:

- Developing tracing and offensive capabilities:

The first element in deterring an adversary in cyberspace from threating a smart city making the adversary realize that you are able to find him, follow him, and strike back more fiercely, regardless of the type of

adversary (state, terrorist group, criminal organization, or individual). This could be achieved by developing tracing and offensive capabilities which simultaneously allow you to find and punish your enemy.

• Broad scope of early warning systems:

Employing large number of sensors and early warning systems could help discover an attack before it fulfills its goal. These sensors and systems could be used in critical infrastructure and government e-services because they form the most important targets for attacks within a state. The cost of such an initiative would be expensive, but is nothing compared to the damage that could be levied by a sophisticated cyber-attack.

• Spare traditional networks and backup data resources:

Critical infrastructure should function properly at all times, even when targeted by cyberattacks. To achieve this, another conventional and manual network could be established as a backup network so that if the state fails to contain the attack, it can move to the spare network. Diversifying backup data resources is also essential; in the event of data damage, the state would still be in possession of the source. But we should realize that having several backup data resources could form a point of weakness unless we also increase data security by implementing different layers of security and data encryption.

• Transforming from "network security" to "environment security":

It is not sufficient to simply secure the network to protect critical institutions and infrastructure from penetration; the entire environment must be secured which includes everything surrounding the network such as buildings, minds, behaviors, and procedures.

B. The political level:

States can protect their interests in cyberspace by establishing alliances, signing agreements, and sharing information. Smaller or less secure states could join in alliance with highly-secured states and big security companies, to form an alliance that would defend their cyberspace interests. Additionally, regional and international military alliances and organizations can develop their own goals and strategies to also operate in cyberspace. Agreements on information-sharing between security and intelligence agencies within and among nations is also important to increase tracing and attribution capacities within cyberspace.

C. The societal level:
Every member of society is responsible for helping secure that society. Everyone should be aware of the threats stemming from cyberspace as well as how to address them and reduce the amount of damage associated with cybercrimes and cyberwarfare. This could be achieved through education and social awareness. It is increasingly important to provide cyber education at schools and create a talented generation capable of dealing with cyber threats. Tech companies should also fulfill their social responsibility to teach individuals how to make the best use of their technology and avoid any negative aspects. Mass media should also focus on cyber security topics in order to warn people of cyber threats not only from an operational standpoint, but also from a technical one.

Ehab Khalifa can be reached at the e-mail address *ehabakhalifa@gmail.com*.

Endnotes

1 "Powering smart cities with AI and IoT" (2018), *Microsoft*, , on <https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-Infographic-PoweringSmartCitieswithAIandIOT.pdf> (accessed Jan8, 2019)
2 Darko Galinec, Darko Možnik & Boris Guberina(2018), "Cybersecurity and cyber defence: national level strategic approach", *Journal for Control, Measurement, Electronics, Computing and Communications,* available at https://www.tandfonline.com/doi/full/10.1080/00051144.2017.1407022
3 Papa, Rocco & Gargiulo, Carmela & Galderisi, Adriana (2013), "Towards an Urban Planners' Perspective on Smart City", *Tema Journal of Land Use, Mobility and Environment***.** Vol. 6. 5-17.
4 "Smart Cities The importance of a smart ICT infrastructure for smart cities" (2017), *Deloitte*, p 6 on <https://www.stokab.se/Documents/Nyheter%20bilagor/SmartCityInfraEn.pdf> (accessed March 2, 2017)
5 Vito Albino, Umberto Berardi, Rosa Maria Dangelico (2015), "Smart Cities: Definitions, Dimensions, Performance, and Initiatives", *Journal of Urban Technology,* 11 April 2015, DOI: 10.1080/10630732.2014.942092, pp.1-17 accessible at: <https://goo.gl/fUbdKk> (accessed March 6, 2017)
6 Almirall E. Bakıcı, J. Wareham (2012), "A Smart City Initiative: The Case of Barcelona", *Journal of the Knowledge Economy*, Vol. 2, No.1, pp. 1–14.
7 J.M. Barrionuevo, P. Berrone, J.E. Ricart (2012), "Smart Cities, Sustainable Progress", *IESE Insight*, Vo.14 , , pp. 50–57
8 Taewoo Nam, Theresa A. Pardo (2018),, "Smart City as Urban Innovation:

Focusing on Management, Policy, and Context", *State University of* New York: *Center for Technology in Government University* at Albany, p.168, accessible at: https://goo.gl/TpZcME

9 Ibid., p.168

10 Taewoo Nam, Theresa A. Pardo (2018), "Smart City as Urban Innovation: Focusing on Management, Policy, and Context", *State University of New York: Center for Technology in Government University at Albany*, p.168, accessible at: < https://goo.gl/TpZcME> (accessed April 09, 2018)

11 Maritsa Fargas (2018), "Smart Cities: The Dream and the Reality, *Environment Center for Arab Citie"s,* Accessible at <https://goo.gl/zbFQSj> (Accessed April, 9, 2018)

12 **"**UN. Smart Cities: A Provincial Perspective" (2015**),** *The Government Summit Research Series*, p. 14. Accessible at <https://goo.gl/8NrV9M> (accessed May 13, 2017)

13 Boyd Cohen (2014), **"**The Smartest Cities In The World 2015: Methodology", *Fast Company*, November 20, accessible at: <https://goo.gl/Ty8a6s> (accessed jan15, 2017)

14 Ibid.

15 Rudolf Giffinger (2007), "Smart cities Ranking of European medium-sized cities"**,** *Vienna University of Technology*, Center of Regional Science, accessible at: <https://goo.gl/LcJyz > (accessed Jan 9, 2017)

16 Nicos Komninos (2002), "Intelligent Cities: Innovation", *Knowledge Systems and Digital Spaces*,London: Spon Press,.

17 "IEEE member warns against closed approach to smart cities" (2017), *Technative*, accessible at: <https://goo.gl/zTbMXM> (accessed: November 5, 2017)

18 Saskia Sasse (2011), "The Future of Smart Cities", *Open Transcripts,* accessible at: <http://opentranscripts.org/transcript/future-of-smart-cities/> (accessed: November 6, 2017)

19 "Smart Cities" (2017), *Fiware*, accessible at: <https://www.fiware.org/smart-cities > (accessed November 7,)

20 "How APIs are powering smart cities" (2017), *BBVA*, accessible at: <https://goo.gl/meXUYY> (accessed: October 12, 2017,)

21 "The World's 5 Smartest Cities" (2016), *Internet of things institute*, accessible at: <http://www.ioti.com/smart-cities/world-s-5-smartest-cities> (accessed: October 20, 2017)

22 Vasilis Niaros (2016), "Introducing a Taxonomy of the "Smart City": Towards a Commons-Oriented Approach?", *Journal for a Global Sustainable Information Society*, Vol. 14, no. 1, pp. 51 – 61.

23 DIY techniques, *Public Lab*, accessible at: <https://publiclab.org/> (accessed: October 25, 2017)

24 Gabe Batstone (June 2018), "The role of government in innovation and smart city planning"*, smart cities world*, Accessed April 12, 2019, available on https://www.smartcitiesworld.net/opinions/opinions/the-role-of-government-in-innovation-and-smart-city-planning

25 Vasilis Niaros, op.cit., pp. 51 – 61.

26 Ibid.

27 Ibid.

28 Adam Greengfield (2013)**,** **"**This is Part I of The city is here for you to use: 'Against the smart city"**,** *New York: Do projects*, pp. 10 – 50.

29 Christopher Mines (2011), "3 Kinds of Smart Cities Shaped by IT", *Greenbiz*, accessible at: <https://goo.gl/zD5nCq> (accessed Oct 27, 2017)

30 "Keeping the Nation's Industrial Base Safe From Cyber Threats, Cyber Threats to National Security" (2011), *Carnegie Institution for Science*, Washington, D.C, p 11
31 DeBrusk, Chris, Mee, Paul (2018), "Cyber Risks That Hide In Plain Sight", *oliver wyman*, accessed April 13, 2019,available on https://www.oliverwyman.com/our-expertise/insights/2018/jun/cyber-risks-that-hide-in-plain-sight.html
32 Mee, Paul, Schuermann, Til (September 2018), "How a Cyber Attack Could Cause the Next Financial Crisis", *Harvard business review*, Last accessed April 13, 2019,available on https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis
33 "Cyber Risk in the Transportation Industry" (2015), *MARSH*, accessed April 15, 2019, available on https://www.marsh.com/uk/insights/research/cyber-risk-in-the-transportation-industry.html
34 Cesar Cerrudo (2015), "An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks, secure smart cities", *IOActive Labs*, p. 10, accessible at: <https://goo.gl/imXnwK> (accessed Nov, 2, 2018)
35 "Cyber Security For Smart Cities: An Architecture Model For Public Transport" (2015), *European Union Agency For Network And Information Security,* pp. 27 – 29, accessible at: <https://goo.gl/iPhSRi> (accessed Jan 9, 2018)
36 Marc Goodman (2015), "Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It", *US: Penguin Random House,* February, pp. 1 – 5.
37 Ibid.
38 Gary Eastwood (2017), "How smart cities can protect against IoT security threats", *Networkworld*, accessible at: <https://goo.gl/HPKaHw> (accessed: November 2, 2017)
39 Dr. Mahesh Saptharishi (2017), "The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology", *Wired*, accessible at: <https://goo.gl/Xnqc92> (accessed: January 23,)
40 Adel S. Elmaghraby, Michael M. Losavio (July 2014), "Cyber security challenges in Smart Cities: Safety, security and privacy", *Journal of Advanced Research*, Volume 5, Issue 4, Pages 491–497
41 Irving Lachow (2009), "Cyber Terrorism: Menace or Myth?", in: D. Kramer, Stuart H. Starr, Larry Wentz (eds.), Cyber power and National Security, *Washington D.C: National defense University*, pp. 437 – 464.
42 "Mouse click could plunge city into darkness" (2007), *CNN*, accessible at: <https://goo.gl/y38AKL > (accessed: November 8, 2017)
43 "Critical Infrastructure: Threats and Terrorism, US Army Training and Doctrine Command" (2006), *FAS*, (pp. 1 – 5), accessible at: <https://fas.org/irp/threat/terrorism/sup2.pdf>
44 Steven Poole (2014), "The truth about smart cities: In the end, they will destroy democracy", *The Guardian*, December 17, accessible at: <https://goo.gl/TPWSiY > (accessed 10 Oct, 2017)