Smart Cities: Opportunities, Challenges, and Security Threats

Ehab Khalifa
Future center for advanced research and studies

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 maximizing the use of the available resources, reducing energy consumption and waste, creating an environment that enhances creation and innovation, and improving the quality of life for people by reducing the cost of living and making life easier and safer.

Smart cities have become a priority in developments strategies of many countries all over the world. This is simply because they are among the main incentives to development, as they stimulate economic growth and accommodate population growth. It is estimated that in 2025 around 10 million people will be living in 34 smart cities all over the world (Smart Cities in USA",2018), and that almost 70% of the world population will be living in such cities in 2050(Building the Future's Smart Cities, 2016).

In spite of their various advantages smart cities have many national and cyber security concerns. 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. If these services are targeted by a successful cyber-attack, the consequences in that case would be unaffordable to national security and people lives.

So, this paper is seeking to discuss the impotence to have smart cities for development and its consequences to national security.

METHODOLOGY

This study is a desktop normative study, discuss the gains and threats of smart cities. First it will focus on the widespread adoption of smart cities between nations, and second discuss the reason that push countries to adopt this model of cities and the gain they are seeking to have through this model, third it will discuss various security threats that can arise from smart cities, and finally a conclusion with some recommendation for the mitigation of smart city threats.

GLOBAL TREND

There are many projects to adopt smart cities one of them is The European Smart Cities project which lunched in 2007, whose goal is to build 70 smart cities (Giffinger , Rudolf, 2007). The project is part of the Europe 2020 Project, which aims at improving services and increasing job opportunities.

On the other side, In July 2014 Narendra Modi, the Indian Prime Minister, declared that 100 smart cities, equipped with the latest technologies, were to be built around India, as part of the project of modernizing 4000 old Indian cities. 15 billion dollars were allocated for this project ("$15 Billion Investments in Smart Cities, 2017).

Also Singapore occupies an important position in the Annual Smart Cities rankings. For instance, it came first in Juniper Smart City Ranking in 2016("Singapore Named 'Global Smart City – 2016", 2017). Besides, it has a program for developing the whole country that aims at making Singapore the first smart country in the world. The program was announced in November 2014 by the Prime Minister, Lee Hsien Loong, as part of the Smart Nation Initiative (Transcript of Prime Minister Lee Hsien Loong's speech at Smart Nation launch on 24 November, 2014).

In the Gulf Region, the United Arab Emirates is building smart cities that are developing rapidly. It is noteworthy that Dubai is one of the fastest growing smart cities in the whole world. In October 2013 it launched the "Dubai is a Smart City" initiative- an initiative which encompasses 500 smart initiatives and services, including the Silicon Park Project. The park, which cost almost 300 million dollars, was built on 150,000 square meters. Emirates also began building the Abu Dhabi-based Masdar, meant to be a smart, environment-friendly city that would achieve sustainable development. This has to do with the rise in using IT devices and apparatuses in Emirates and with the fact that Emirates ranks first, in relation to the other countries of the Middle East, and 22nd, in relation to the countries of the world, on the digital development ranking, according to the World Economic Forum(Using IT devices in Emirates is above global rates, 2017).

North African countries have witnessed similar initiatives. For example, Morocco has announced intentions to change six main cities into smart cities by 2026. These are Casa Blanca, Rabat, Tangier, Fez, Ifrane and Marrakesh. It also announced that many sustainable smart cities, operating on sun and wind energy, will be built. Egypt announced that the fourth generation of Egyptian cities, based on the concept of smart cities, shall be the standard city type in the new administrative capital, East Port Said and New Alamein (Alzzahraa 2016).

Many information technology companies launched smart city initiatives, such as the Smart City Challenge Initiative, launched by IBM in 2010 at the cost of 66 million dollars. It involved sending 800 technology experts to more than 130 cities all over the world, with the aim of helping employees arrive at smart solutions that would guarantee a high degree of administrative efficiency (IBM, 2017).

ESSENTIAL FOR DEVELOPMENT

One of the main reasons why countries tend to adopt the smart city model is the huge and rapid population growth which leads to the overcrowdedness of traditional cities, resulting in complicating its traditional problems. These countries, consequently, try to make use of the gains of the fourth industrial revolution in overcoming these problems. They are also bent on increasing economic growth, improving the quality of life and facing security threats. Following is a more detailed discussion of the motives behind building smart cities around the world:

Overpopulation

One of the most important problems that governments worldwide have to face is the rapidly growing population of the big cities. Till the eighteenth century only 5% of the world's population lived in cities(Harrison, 2016). Most people lived in rural areas and on riversides so that they can easily satisfy their need for food. However, after the first industrial revolution, which took place in the eighteenth century and had steam and coal as its impetus, people began to move from rural to urban areas, seeking a

better life. The second industrial revolution broke out in the nineteenth century with the advent of electricity, the result being that more and more people were leaving their villages for the city. This tendency has even been reinforced by the third industrial revolution, which took place in the 1960s, as a result of the developments in the field of computer, which came to be known as "the digital revolution".

In the early 21st century city dwellers amounted to 50% of the world's population (3.3 billion people) in 2008 (Human Development Report, 2007/2008). This percentage is expected to rise to almost 70% by 2050 (i.e. more than 9 billion people) (The Smart City Project, 2016). In Europe, city dwellers represent 70% of the whole population, and the percentage is expected to rise to 80% in 2020 (Albino, Berardi, Dangelico, 2015). This is creating further challenges relating to the management and organization of cities around the world (The Millennium Development Goals Report, 2008).

This has led the governments to build big cities that can accommodate the ever-growing population, making use of the material and technical possibilities, created by the technological revolution, in managing these large numbers of people in a way that would result in sustainability and efficiency of organization. The smart city model is the most acceptable and adequate model as far as running big cities is concerned.

Attracting Innovative Minds

Nowadays, cities around the world are engaged in competitive relationships with one another, where competition is no longer political or military but mainly an economic competition created by the Global Supply Networks. Each city is trying to control as many global trade lines as possible (whether these are goods delivered by air or sea, or cash flows via banks, or strategic industries) with the aim of achieving economic progress. In order for this to happen these countries need to make use of human innovation. Therefore, they seek to attract creative people with exceptional skills, capable of coming up with new, nontraditional ideas that are important for fulfilling scientific and economic development (Harrison, Donnelly, 2018).

Many countries have adopt the smart city, projecting an image of themselves as countries that keep up with modernization and make use of the gains of the AI revolution, so that they can attract these innovative minds. This has particularly become a growing tendency following the 2008 global financial crisis. As a result, many skilled individuals have moved from such cities as Paris, New York and London to other cities that were able to attract them via their adoption of the new smart model(Harrison, Donnelly, 2018).

In other words, if a country wants to plan a new city, or if a city wants to build a new district or increase investment rates, it should provide the incentives that would motivate the targeted category of people. If these people are characterized by a high degree of creativity they are sure to be attracted by the smart city model, which would function as an open lab where they can experiment with original ideas.

Smart cities are centers where people can develop their skills; they attract people with all sorts of skills, be they natives of the country where the smart city is built or foreigners. The interaction between them makes it easier to share knowledge and experiences, and helps people discover their own potentials, provided that the principles of good governance are followed. This would eventually result in improving the educational process and developing individuals' skills so that they can become more intelligent and able to create and innovate.

Improving the Quality of Life for the Individuals

Adopting the smart city model can result in improving the quality of life for the individuals, through providing original solutions for traditional problems, such as the problems of pollution, traffic congestion and waste of energy. It is known that traditional cities consume 60% to 80% of the total energy available; they are also responsible, to a great extent, for the lead and carbon emissions harmful for humans and the environment (Albino, Berardi, Dangelico, 2015). However, good planning and incorporating smart technology in everyday life can help rationalize the use of resources, reduce harmful emissions and control traffic.

Smart initiatives enable people to have access to government and private services and to finish all transactions easily and efficiently. Adopting such initiatives also helps improve strategic services such as education, health care, and utilities.

Smart cities can help overcome the traditional problems of big cities, such as pollution, traffic congestion and administrative corruption. They also play a role in improving the quality of services, managing resources wisely, reducing operating costs, reducing energy waste, securing the highest safety levels and creating a suitable environment for innovation, all of which would eventually lead to achieving development.

In 2017, a report by Bank of America indicated that cities such as Singapore, London, New York, Paris and Tokyo can reduce crime rate and energy consumption by 30%, and waste of energy and traffic congestion by 20%, through increasing investment in smart city technology (McClay, 2017).

Following is an investigation of the gains and opportunities that can be created via building smart cities:

REDUCING POLLUTION

Smart cities can help reduce carbon emissions and pollution in general through adopting clean industries and environment-friendly buildings and depending on clean energy resources, such as electricity, solar energy, wind energy and water energy. Reducing pollution can also be achieved through adopting a smart transportation system, based on either self-driving cars or manual cars that use electricity and solar energy instead of fuel. Smart cities also have waste-to-energy systems and recycling systems that make environment-friendly products, as well as systems for treating sewage, rainwater and irrigation water. Smart systems reduce the waste of energy and rationalize the use of resources. An example is smart lighting systems, which work only when needed. Sensors and smart pollution monitors in the city would detect air and water pollution instantly; they would also measure the temperature, the atmospheric pressure and the level of chemical and carbon emissions, and their places, so that overcoming pollution and waste management can be facilitated (India Times, 2015).

OVERCOMING THE PROBLEM OF TRAFFIC CONGESTION

The smart city model provides a general framework for overcoming the problem of traffic congestion, through depending on smart technology and technological solutions that would provide accurate, instant information about the causes and points of traffic congestion. This is achieved via collecting big data from sensor systems installed on the streets as well as CCTV and smart traffic lights that work automatically according to traffic density, giving more time to more crowded streets (Khan, 2016).

Adopting smart traffic systems does not need huge investments. All it needs is installing cameras and sensory devices in roads and streets and building central control and management rooms. There is no need to restructure the city's infrastructure. Undoubtedly, this would be easier to do when planning for building a new city than it would be if the city is already there but needs to be changed from a traditional into a smart one. The accurate, instant information that these systems supply would facilitate operating self-driving cars in the city.

OVERCOMING ADMINISTRATIVE CORRUPTION

Smart cities basically depend on electronic systems; citizens have access to both government and private services via smart applications. The fact that no humans are involved limits the possibility of corruption. If anyone tried to tamper with the system, attempting any illegal activities, technical problems would arise, and then it would not be difficult to discover the doer (David, Justice, McNutt, 2015).

If need arises for the interference of humans, their responsibilities and authority would be strictly defined so that there can be no transgression on their part, or else the system would stop working, or at

least those in charge of the system would be able to know that certain uncompleted transactions have been attempted by a certain employee from the track records of the activities performed on the system. This would help detect attempts by corrupt employees to tamper with the system.

These smart systems save time and effort wasted in waiting for long hours, or even days or months for traditional transactions to be completed. A citizen can apply for whatever s/he needs to do via the internet or smart phone, upload the required documents to the system, and pay for the service online. Then the system would provide him/her with information concerning the status of his application, and the next steps that s/he must take so as to finish the transaction in the right way. In case there is delay, the citizen is informed about the cause, instead of having to deal with the unnecessary bureaucracy characteristic of traditional transactions. In fact, s/he never visits the government department responsible for the transaction in person unless there is an urgent need for it.

ACHIEVING SECURITY IN SMART CITIES

Surveillance systems and cameras are typically installed all over the smart city; they can be found everywhere (e.g. streets, stores, residential buildings, elevators, etc.) except for inside houses and offices. However, citizens may decide to install CCTVs and the like in their houses and offices too. This means that any attempt to threaten the security in the smart city would be discovered, and if a crime was committed it would be easy to know who the doer is. This also means that crime can be anticipated, and therefore prevented, through depending on OSINT (short for open source intelligence), which refers to the ability of obtaining intelligence information from the legal, open sources available on electronic systems and huge computers (Steele, 1997).

Open source intelligence is based on the idea that we live the age of big data that can be obtained from satellites, surveillance cameras, social media websites, the internet, applications that collect personal information, bank accounts, and sensors that collect information in streets and smart cars, let alone information available via newspapers, periodicals, TV channels, radio channels and books (InfoSec Resources, 2013).

Special software is used for analyzing these huge amounts of data and connecting them to government data bases and security systems instantaneously and simultaneously, so as to obtain indexes and analyses that would help to detect crises beforehand and construct scenarios for dealing with them. This would also help detect crime and keep decision makers and policy makers updated about public opinion trends, which, in turn, would facilitate the process of making political and security decisions.

ATTRACTING INVESTMENT AND ENCOURAGING INNOVATION

Smart cities have certain characteristics that make them attract foreign investment, such as their remarkable urban organization, their smart infrastructure, their well- informed citizens, their use of clean energy, as well as their cosmopolitan culture and their openness to the world. Not only do these characteristics attract investors but they also attract tourists who would like to see and try the modern technologies used in these cities.

Smart cities are also very fertile soil for innovation, because of the many open labs and idea incubators in them, which are necessary for innovators and entrepreneurs so that they can create in all fields (e.g. the scientific, technical, technological, etc.). This helps fulfill development, in its comprehensive sense, in the city (Gordon, 2016).

ENHANCING THE EFFICIENCY OF RESOURCES MANAGEMENT

Builders of smart cities are concerned with the wise management of the available resources, notably limited resources. These include land, energy, water and natural resources. For example, the optimal ways to make use of space are followed, through designing buildings and parking lots which can accommodate as many people and cars (respectively) as possible. They also give special attention to green areas and

areas separating buildings from one another, which would help overcome such problems as pollution and over-crowdedness.

In addition, comprehensive water management technology in smart cities helps control waste and pollution levels, and water quality. It also helps take precautions against floods and other water-related disasters, and deal with them as fast as possible in case they occur (The Union News Magazine. Issue: 2, 2016).

NATIONAL SECURITY THREATS

Threats to the national security of smart cities fall into two main categories: traditional threats and non-traditional threats. Following is an explanation of both:

Traditional Threats
Traditional threats include threats that target the infrastructure and government services in the smart city. They also include spying on people, institutions and organizations, waging cyber warfare, and competing to dominate cyberspace so as to use it in espionage and endangering E-commerce and vital economic sectors in the city. Following are more details:

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 (Lachow, 2009).

Targeting the GPS- upon which planes, self-drive 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 (Cerrudo, 2015).

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 SCADA (short for: Supervisory Control And Data Acquisition), systems, which are huge computer systems for controlling main power stations. If these systems were hacked the consequences would be catastrophic (CNN, September 27, 2007).

Besides, 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.

The Threat to Banking and Finance 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 doing 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-namely, 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 (Carnegie

Institution for Science, 2011). It is true that banks and financial institutions take whatever procedures needed to safeguard clients' accounts against hackers, but we must not forget that the client would always constitute a Trojan horse to system security. Many people can fall victims to scams, as hackers can send emails to them, asking them to update the information associated with their bank accounts, as a first step to stealing these accounts.

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, indispensible in smart cities. Despite their great importance, these devices constitute a threat to the smart city's security; they are billions and all over 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, so to speak, 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 dangerous, they can destroy the internet itself (Eastwood, 2017).

Targeting Artificial Intelligence Systems

Smart cities depend on AI technologies, such as Robotics systems, in factories, companies, stores, automated answering systems, self-drive cars, and drones. If these systems were hacked, self-drive cars, for example, could be re-programmed to run people over, and it would be extremely difficult to know who the doer is. 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 (Saptharishi, 2017).

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 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.

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- (Goodman, 2015). Besides, commercial drones can be equipped with weapons or bombs and programmed to attack people or civil aircraft, or-at least- to violate people's privacy by taking their photos (Goodman, 2015).

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. 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 (European Union Agency For Network And Information Security, December 2015).

Nontraditional Threats

A smart city can face nontraditional threats, the most important of which is that attempts to change the value system of a city so as to turn it into a cosmopolitan system can meet resistance on the citizens' part. This can result in division among the citizens, who would be afraid for their privacy and freedom. This can be detailed as follows:

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, is not likely to face such a problem.

Violating People's Privacy

The privacy of individuals is one of the most 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, 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? (Elmaghraby, 2014).

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 these data. This means that power and authority would be monopolized by those who have control over these 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 (Poole, 2014)

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.

CONCLUSION

Smart cities could help overcoming 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. They also play a role in improving the quality of services, managing resources wisely, reducing operating costs and energy waste, securing the highest safety levels and creating a suitable environment for innovation, but on the other hand, it raises a lot of security challenges and threats to national security.

Therefor a proactive measure should be taken to keep national security like employing large number of sensors and early warning systems could help discover cyber attack before it fulfills its goal, these sensors and systems could be used in critical infrastructure and government e-services, at the same time the state should work on developing tracing and offensive cyber capabilities to deter its enemies from hacking the smart city. International cooperation is also vital for national security through establishing

alliances, signing agreements, and sharing information with international community. Finally, social awareness is also important, 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.

REFERENCES

Albino, V., Berardi, U., Dangelico, R. M. (2015, April 11). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*. DOI: 10.1080/10630732.2014.942092, pp.1-17. Retrieved from https://goo.gl/fUbdKk

Azzahraa, F. (2016, December 13). *Machine sociology: Smart communities and changing citizens' values. Arab challenges*. Future Center for Advanced Research and Studies. Retrieved from https://futureuae.com/ar-AE/Mainpage/Item/2257/

Building the Future's Smart Cities (2016). *The Union News Magazine, 2*. The International Telecommunication Union. Retrieved from http://www.itu.int/en/itunews/Documents/2016-02/2016_ITUNews02-ar.pdf

Cerrudo, C. (2015). An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks, secure smart cities. *IOActive Labs*, p. 10. Retrieved from https://goo.gl/imXnwK

Critical Infrastructure: Threats and Terrorism (2006, August 10). US Army Training and Doctrine Command. FAS. Retrieved from https://fas.org/irp/threat/terrorism/sup2.pdf

Cyber Security For Smart Cities: An Architecture Model For Public Transport (2015, December). European Union Agency For Network And Information Security, pp. 27-29. Retrieved from https://goo.gl/iPhSRi

David, N., Justice, J., & McNutt, J. G. (2015). Smart Cities Are Transparent Cities: The Role of Fiscal Transparency in Smart City Governance, in, Manuel Pedro Rodríguez-Bolívar (ed.), *Transforming City Governments for Successful Smart Cities*, (New York: Springer, 2015), pp.69-86

Eastwood, G. (2017, October 11). *How smart cities can protect against IoT security threats*. Networkworld. Retrieved November 2, 2017, from https://goo.gl/HPKaHw

Elmaghraby, A. S., & Losavio, M. M. (2014, July). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491–497.

$15 Billion Investments in Smart Cities (2017, September 21). The Hindu Business Line, Retrieved October 20, 2017, from http://www.thehindubusinessline.com/economy/15b-investments-in-smart-cities/article9867761.ece

Fighting Climate Change: Human Solidarity in a Divided World (2007/2008). Human Development Report. UNDP. Retrieved from http://www.un.org/ar/esa/hdr/pdf/hdr0708/HDR_20072008_Complete.pdf

Giffinger, R. (2007, October). *Smart cities Ranking of European medium-sized cities*. Vienna University of Technology, Center of Regional Science. Retrieved from https://goo.gl/LcJyz

Gordon, J. (2016, June 23). *Smart City 2.0: Economic Development In A Digital Metropolis, Facility Executive*. Retrieved from https://facilityexecutive.com/2016/06/smart-city-2-0-economic-development-in-a-digital-metropolis/

Harrison, C., & Donnelly, I. A. (2016). *A Theory OF Smart Cities*. IBM Corporation. Retrieved December2, 2016, from http://www.interindustria.hu/ekonyvtar/en/Smart%20cities%20and%20communities/Publications/A%20theory%20of%20smart%20cities.pdf

IBM's Smarter Cities Challenge to Help Five Cities Improve Services to Their Residents (2017, July 20). IBM. Retrieved from http://www-03.ibm.com/press/us/en/pressrelease/52854.wss

Keeping the Nation's Industrial Base Safe From Cyber Threats (2011, September). Cyber Threats to National Security. Carnegie Institution for Science, Washington, D.C, p 11.

Khan, I. (2016, January 19). *Asia is Leading The 'Smart City' Charge, but we're not There Yet*. Retrieved from https://www.techinasia.com/asia-leading-smart-city-limitations

Lachow, I. (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, May 2009), pp. 437 – 464.

McClay, R. (2017, March 23). *Smart Cities: Companies Profiting from Urban Challenges*. Investopedia. Retrieved from http://www.investopedia.com/news/smart-cities-companies-profiting-urban-challenges

Mouse click could plunge city into darkness (2007, September 27). CNN. Retrieved November 8, 2017, from from https://goo.gl/y38AKL

OSINT (Open-Source Intelligence) (2013, September 11). InfoSec Resources. Retrieved from http://resources.infosecinstitute.com/osint-open-source-intelligence/

Poole, S. (2014, December 17). *The truth about smart cities: In the end, they will destroy democracy*. The Guardian. Retrieved from https://goo.gl/TPWSiY

Saptharishi, M. (2017). *The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology*. Wired. Retrieved January 23, 2017, from https://goo.gl/Xnqc92

Singapore Named 'Global Smart City – 2016. (2017, May 17). Juniper Market Research. Retrieved April 1, 2017, from https://www.juniperresearch.com/press/press-releases/singapore-named-global-smart-city-2016

Sing IT devices in Emirates is above global rates (2017). Emirati Gulf Newspaper. Retrieved August 3, 2017, from http://www.alkhaleej.ae/economics/page/f4a21f15-9c9e-4963-b042-adb2e468d2b4

Six ways how smart cities will benefit citizens (2015, September 1). India Times. Retrieved from https://economictimes.indiatimes.com/slideshows/infrastructure/six-ways-how-smart-cities-will-benefit-citizens/how-it-will-benefit-citizens/slideshow/48753936.cms

Smart Cities in USA (2018). Smart America. Retrieved May 20, 2018, from http://smartamerica.org/teams/smart-cities-usa/

Steele, R. D. (1997). Open Source Intelligence: What Is It? Why Is It Important to the Military? *Open Source Solutions Inc.,* 330-340. Retrieved from https://goo.gl/WtTvZC

The Millennium Development Goals Report (2008). The United Nations. Retrieved from http://www.un.org/millenniumgoals/pdf/MDG%20Gap%20Task%20Force%20Report%202008.pdf

The Smart City Project (2016). Retrieved December 26, 2016 http://smartcity-planning.co.jp/en/approach/index.html

Transcript of Prime Minister Lee Hsien Loong's speech at Smart Nation launch on 24 November. (2014, November 24). Prime Minister Office Singapore. Retrieved January 5, 2017 from http://www.pmo.gov.sg/newsroom/transcript-prime-minister-lee-hsien-loongs-speech-smart-nation-launch-24-november