EUROPEAN CYBER SECURITY ORGANISATION

SMART CITIES AND SMART BUILDINGS SECTOR REPORT

Cyber security for the smart cities sector

WG3 I Sectoral Demand

MARCH 2018

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg3_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

This document will be continuously updated based on developments within the sector and ECSO members' input.

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION

Smart cities is a complex “task”. Many things have to be taken into account, including IT security. No matter what stage you are at, be it preliminary planning or final implementation, it is never too late to think of cyber security and make sure that everything is safe.[1]

For the activities of this working group, we start from the definition given by the Urban Tide and Scottish Government[2] where we might add “the” critical factor which are the people: “*The Smart City can be defined the integration of data and digital technologies by the human being into a strategic approach to economic, environment, social, technological sustainability for citizen well-being*”.

The nature of system development and deployment is in the early stages of a significant, fundamental evolution in scale, complexity, interconnectedness, and interactivity.

We need to take into account the complexity of the smart city challenge, the concept of Internet of Things (IoT) and cyber-physical systems (CPS), and the current state of smart cities[3].

Several barriers currently exist to effective and powerful smart city solutions[4]:

- First, many current smart city ICT deployments are based on custom systems that are not interoperable, portable across cities, extensible, or cost-effective.
- Second, a number of architectural design efforts are currently underway (e.g. ISO/IEC JTC1, IEC, IEEE, ITU and consortia) but have not yet converged, creating uncertainty among stakeholders.
- Third, secure by design means that the applications and the devices have been designed from the ground up to be secure.

To design, build, and operate interconnected systems of people, software, machines, and data so complex that they are, “...likely to have billions of lines of code....”, we have to note that:

- Current engineering methods, tools, and best practices are insufficient for designing and constructing ultra-large-scale systems;
- New methods and tools of design, analysis, and operation are required.

Rather, those large-scale systems must be *cultivated* into functional existence by continuous integration and optimisation of its component systems of systems. Systems of this level of complexity,

[1] https://securingsmartcities.org/?page_id=2

[2] “The Smart City can be defined as the integration of data and digital technologies into a strategic approach to sustainability, citizen well-being and economic development”, UrbanTide and Scottish Government, 2014

[3] Pollak, B (Ed.), Feiler, P., Gabriel, R., Goodenough, J., Linger, R., Longstaff, T., Kazman, R., Northrop, L., Schmidt, D., Sullivan, K., Wallnau, K. (2006). Ultra-Large-Scale Systems: The Software Challenge of the Future. Software Engineering Institute. Retrieved from: http://resources.sei.cmu.edu/asset_files/Book/2006_014_001_30542.pdf

[4] https://pages.nist.gov/smartcitiesarchitecture/

especially the components of such emerging systems of systems project types, have been studied additionally as:

- Cyber-physical systems,
- Socio-technical systems,
- Complex, large-scale, integrated, open systems
- Multi-scale systems.

The purpose of this document is to provide a general overview about cyber security in the smart city and all that this entails, with its complex nature and breadth of stakeholders, along with recommendations to face the current and future challenges.

2 Landscape

Smart citizens in the smart city

The aspects surrounding the smart city are closely related to cyber security. Nevertheless, Smart Cities starts with smart citizens! As more people move to urban areas, cities face ever more economic and environmental challenges, including resource constraints, economic re-structuring, ageing populations, and pressures on public finances.

In their efforts to accommodate growing urban populations and the accompanying challenges, governments can use modern information and communication technologies to create "Smart Cities" and smart buildings that improve the quality and interactivity of urban services while reducing costs and ensuring sustainability.

For the last few decades, visionary city administrations have started looking closely at ways to enhance quality of life for city dwellers. However, with today's constrained resources, they face new and wide-ranging pressures:

- Population growth places increasing demands on new and existing services, sometimes to the detriment of quality.
- The prolonged economic crisis has progressively eroded investments in services for citizens.
- Central government has to comply with international carbon emission targets and cities play a major role in emission production.
- As energy requirements grow, pollution increases, supply needs to be managed efficiently and critical infrastructure needs to be protected.
- Ageing urban infrastructure can be a ticking time bomb, especially in recessive economies.
- Public safety and security is becoming increasingly challenging.
- Citizens are becoming more demanding, particularly the younger population of the so-called 'digital natives'.
- People are increasingly using unsecured Wi-Fi hotspots to access personal information (email, social network, Internet banking) and exposing themselves to various types of attacks.
- City governments are expected to address all of these challenges, on top of existing issues. This drives the need to create an ecosystem of ICT vendors, energy suppliers, building companies, health providers and education bodies; all engaged in providing state-of-the-art solutions in every field.

In addition to saving energy, smart buildings improve the indoor experience for occupants: on a sunny day, windows automatically darken themselves and when sensors detect an empty room, the heat automatically turns off. Buildings that employ these types of energy-saving technology improve occupants' quality of life, workers' productivity, and students' chances for academic success.

The smart city experience involves systems and objects interconnected through various technologies, like local, wide and wireless networks. The amount of data generated by these systems can reach a considerable size. Big Data will need to be appropriately and centrally stored, managed, analysed, and protected.

"Someone" in the city must supervise the interaction between systems and will have to ensure continuity, integrity and resilience. With time, the interconnected and interdependent services of smart cities will evolve under a centralised governance dashboard of specialised stakeholders, responsible for setting policies and processes, managing ICT assets, services and protocols, and ultimately administering the services for constituents. ICT control and management capabilities will be crucial, to guarantee an efficient, secure and resilient governance and delivery.

A smart city is an urbanised area where multiple sectors cooperate to achieve sustainable outcomes through analysis of contextual real-time information shared among sector-specific information and operational technology systems:

- Smart grids and energy efficiency. It is estimated that cities are responsible for between 60% and 80% of the world's energy use. Optimising delivery and consumption is vital.
- Buildings, both residential and commercial, provide an important opportunity to optimise energy consumption and enhance the wellbeing of residents and workers. Intelligent buildings, particularly office environments, can leverage smart grid technologies to influence energy supply and consumption by controlling lighting, climate control and IT.
- Intelligent transportation. Keeping the city moving is critical. Transportation strategies have an impact on public safety, the environment, energy, rapid response services, the ability to do business, and critical deliveries.
- Connected healthcare. Healthcare delivery can benefit from a connected approach, with Electronic Patient Records available to all medical services. This will enable public health professionals and clinicians to collaboratively access information in a secure way, at any time, from anywhere and from any device. In many cases, telemedicine solutions, connected through broadband, wireless or satellite, can prove vital in situations where the infrastructure or specific contingencies do not allow for the physical presence of a specialist.
- Public safety and security. Above all, cities need to be safe. Public safety and security has become paramount for city administrations, whether protecting against crime, natural disasters, accidents or terrorism.
- Wireless communications and hotspots. Both large and small municipalities offer free wireless hotspots in addition to those provided by airports, hotels, and shops. As this trend is set to continue, given the popularity of the service, more and more citizens will be exposed to potential vulnerabilities.

Smart city and cyber security

According to a recent paper published by Forbes, 6 Ways To Make Smart Cities Future-Proof Cybersecurity Cities[5], smart cities must adjust and adapt to the requirements of the new cyber security landscape, characterised by:

- ***The expansion of the attack surface*** with the introduction of new points of potential vulnerability such as connected and self-driving cars, and the Internet of Things (71%

[5]https://www.forbes.com/sites/gilpress/2018/02/14/6-ways-to-make-smart-cities-future-proof-cybersecurity-cities/3/

of local governments say IoT saves them money but 86% say they have already experienced an IoT-related security breach);

- ***A wider range of attacker motivations***, including ransomware (it was the motivation behind 50% of attacks in the US in 2017, with ransom payments totaling more than $1 billion) and hactivism (drawing attention to a specific cause, adding cultural and political dimensions to cyberattacks);
- ***Increased consumer concern*** about personal data privacy and loss (30% of customers will take action following a data breach—demand compensation, sue or quit their relationship with the vendor);
- ***Not enough people*** with the right expertise and experience (the much talked-about cyber security skill shortage is exacerbated in municipalities which find it hard to compete for scarce talent with organisations with much deeper pockets; this challenge becomes even more severe with the introduction of new approaches to cyber security involving new tools based on machine learning and artificial intelligence);
- ***Insisting on fast time-to-everything*** (*Agile* is not agile enough) results in reduced quality of cyber security applications.

What must be done to meet these challenges? Here's a shortlist of priorities for leaders of smart cities worldwide:

- ***Prepare*** for the worst—develop a protection strategy and emergency plans, and get outside experts to help;
- ***Practice***—training and testing and more training and testing and simulations;
- ***Automate***—implement a continuous adaptive protection, automate the process of detection and response, apply algorithms liberally, including AI and machine learning--based solutions;
- ***Upgrade***—keep up with attackers' new methods and tools, improve the state of hardware and software including leveraging the cloud and big data analytics and invest in elevating the skill level of the people responsible for cyber security defense;
- ***Share***—raise public awareness, disclose your experiences, and exchange information with other local governments;
- ***Separate and disinfect***—insert a virtual layer between the internal network and the internet, allowing only for sending commands and showing display windows, and make downloadable files harmless by deleting areas where programs may exist or transform them into safe data, regardless if they are malicious or not.

Life in the cyber security trenches, for local governments and all other organisations, will continue to get very interesting.

3 User Engagement

This section proposes recommendations to enhance the level of cyber security within smart cities. They are directed towards different groups of stakeholders:[6]

- Municipalities should support the development of a harmonised cyber security framework which allows smart city operators to implement common guidelines.
- Operators should develop a clear definition of their security requirements
- Manufacturers and solution vendors should integrate security in their products
- The European Commission and Member States should clarify the responsibilities of every actor
- Cyber security has a cost that integrates technical and non-technical solutions.
- Users of city services, Users are the citizens but could also be assets in a city (thinking of citizen2machine, machine2machine, etc.), if we think that enabling a dialogue should be the final goal (“cities are where dialogues take place” cit. I. Calvino).
- City providers, public and private.

[6] https://www.enisa.europa.eu

4 Sector Specificities

The role of data in safe cities

Fundamental to the creation of smart cities is the generation, analysis and sharing of large quantities of data. Indeed, the main aim of smart cities technologies is to make cities data-driven; allowing city systems and services to be responsive and act upon data in real-time:

- Intelligence: the first and most important stage of security is surveillance and intelligence gathering. This calls for equipment such as CCTVs and biometrics hardware and software to collect the essentials in its raw, unprocessed form. A secured network for transmission of data is important to ensure non- tempering of data.
- Analysing Data collected: Analytics help digest, decode and make sense of the terabytes of information and data collected, by providing secured storage, analysis and forensic tools. Change from byte-sized to bite-sized for effective prevention against threats or reaction to a calamity and provide situational awareness.
- Mobilising the Resources: There is human intervention in any security installation with physical security apparatus from perimeter protection to communication devices for personnel on the move. The effective mobilisation of people and equipment is crucial to the entire infrastructure of a steadfast and secured location.

The interconnectivity of people, devices and organisations in today's digital world opens up new vulnerabilities — access points where the cyber criminals can get in. The multiplying effect of today's cyber security challenges presents an opaque universe of threats that often come from unexpected or unforeseen domains which have an escalating effect.

Securing smart cities aims to solve the existing and future cyber security problems of smart cities through collaboration between companies, governments, media outlets, other not-for-profit initiatives and individuals across the world. As they invest in smart technologies to improve services and save money, cities also need to step up security against cyber threats. Cities are incorporating new technologies at an increasingly rapid pace, becoming ever smarter. Newer technologies — along with faster and easier connectivity — allow cities to optimise resources, save money and provide better services to their citizens.

Starting from the three previous topics, the city must highlight the following:

- Insecure Products & Insufficient Testing: one of the biggest concerns about smart buildings and smart cities is that the sensors in the equipment can be hacked and fed fake data, which could be used for all manners of mischief, like causing signal failures that shut down subways or allowing contaminants into the water supply.
- Huge, Complex Attack: the trouble is, the notion of "internal network" doesn't really translate to smart cities. The trend is, the smarter the city, the more computer systems, the more integration between the systems, and the more open the access to the data collected by all those systems.
- Lack of Oversight and Organisation: "Who's responsible when a smart city crashes?". Some experts agree that in many cities there is still no clear cyber security leadership, and that cities need to establish city-specific security operations centres, not just for information

sharing, but also for cross-function vulnerability assessment and incident response planning.

It's important to remember that cyber security is a city-wide issue and not just a technology risk. Since many opportunities for IoT will arise through technological integration and collaboration, which will continue to increase in complexity — this complexity breeds risk.

To effectively manage the risks in a smart city, it is important to clearly define the limits of that ecosystem:

- Data Privacy and protection concerns: Privacy is considered as a basic human right and is protected by national laws in different ways. Privacy concerns include the acceptable practices with regards to accessing and disclosing personal and sensitive information about a person. Smart city technologies capture data relating to all forms of privacy and drastically expand the volume, range and granularity of the data being generated about people and places. Privacy can be threatened and breached by a number of practices which are normally treated as unacceptable, however are part of operations in a smart city eco system.
- Surveillance: Watching, tracking, listening to or recording a person's activities
- Aggregation: Combination of various aspects of data about a person to identify a trend or pattern of activities.
- Data leakage: Lack of data protection policies can lead to leakage or improper access of sensitive information.
- Extended usage: Use of data collected for period longer than stated or for purposes other than the stated purpose without the subject's consent.
- Insecure Hardware: One of the major concerns about smart cities' sensors in the equipment, buildings etc. is that they are insecure and not tested thoroughly.
- Larger Attack surface: Smart city operations utilise a complex, networked assembly of ICT infrastructure to manage various services. Any device that is connected to the network is vulnerable to being hacked; the number of potential entry points is multiplied in Smart Cities.
- Bandwidth consumption: Thousands of sensors, or actuators, trying to communicate to a single server will create a flood of data traffic which can bring down the server. Additionally, most of the sensors use an unencrypted link to communicate, and hence, there are possibilities of security lapses.
- Application risk: Apps have accelerated the integration of mobile devices in our daily lives. From mapping apps, to social networking, to productivity tools, to games, apps have largely driven the smartphone revolution and have made it as significant and as far-reaching as it is today.

Beyond the potential for human or computer error, smart cities will provide cyber threat actors with a large attack surface to target and potentially exploit and incorporate into broader campaigns:

- Cybercriminals - As we have described above, smart cities will be composed of thousands – if not millions – of interconnected devices. Such a structure is a boon to criminal actors able to create or purchase and subsequently deploy self-propagating malware, variants of which have been known to proliferate across multiple connected networks.

- Cyber activists - As cyber activist groups grow increasingly capable and, in some cases, more radical, smart cities will provide them with an attack surface enabling a broad range of attacks from those akin to nuisances such as defacements of a city's billboards, to the more extreme targeting of a smart city's energy grid with the aim of physical destruction.

The potential destructiveness of a cyber-attack on smart cities is such that even the threat of compromise of the city's system is likely to be treated by governments and businesses as an existential one.

As the underlying network of smart cities will encompass most aspects of life within the city, if that network were to be compromised by an attacker, it would grant them unfettered access to a target individual or organisation. For instance, state-owned competitors could compromise a smart city's infrastructure to gather intelligence on a large number of rival private sector firms. This information could include movements of their executives within the city, private and commercial communications grabbed from the ubiquitous presence of 'free Wi-Fi hotspots' managed by the city, and many more. Moreover, organisations operating within the city are likely to have their networks overlap to some extent with the city's own network, or at the very least, have frequent data transfers from their networks to that of the city. This would enable highly advanced threat actors such as nation states to exploit weaknesses within a city's infrastructure to reach a target organisation and compromise the confidentiality of its network.

Open issues to consider in this context are:

- Data & Privacy: the way we manage data in a secure way to reduce cyber security issues in the city.
- Interoperability: you must go through very vast grounds for interoperability. This point is different from the other verticals. There is a broad need for interoperability specific to the e-services cluster and smart cities.
- We are dependent on results from other domains to enable the process for new services.
- We could state the problems and the needs.
- Looking at cross-correlations between other verticals when they are acting in one single landscape (that is the city).

Key people in safe cities

There are plenty of smart city careers to consider in the next coming years. Within smart city technology the advances in IoT sensors and analytics platforms will result in the creation of thousands of new hybrid positions that utilise a range of skills. Cities are becoming "smarter" and this will spur the creation of thousands of traditional technical jobs. At the same time, new positions will arise that are more of a hybrid of two or more job categories, as Cisco Services has defined in its strategy[7], and cyber security is in the centre of this new "movement with exciting opportunities":

- Machine learning scientist: As cities increasingly leverage IoT deployments and are able to collect more data about weather, traffic, etc. from their assets in the field and mine it with

[7] https://www.techrepublic.com/article/15-hot-tech-jobs-for-smart-cities-in-2018-and-beyond/

third-party applications, data scientists are needed to analyse and create more value from that data and bridge data silos.

- Data scientist: often described as a unicorn because of their rare ability to transform human expertise and judgments into artificially intelligent models that can 'reason' about complex problems.
- Developer: a new increasing demand for more developers, including software developers, platform developers, and database developers.
- Cyber security analyst: everything that we do as part of smart cities will need to be safe and secure.
- Cloud architect: cities are full of solution providers with new smart city applications to enable better management of their assets (parking, lighting, sensor monitoring, water management, etc.).
- Industrial network engineer: new technologies for collecting data from a city's assets that are becoming more and more connected (cellular LPWA, LPWA, private network, Wi-Fi, etc.).
- Alliance/partnership manager: is needed to select the best IoT technology to bring value to the city, based on that city's specific needs.
- Virtual reality specialist/evangelist: will have multiple applications in smart cities (helping operators, technicians, public safety for medical/emergency response, etc.).
- Chief city experience officer: there are CIOs and CTOs in cities but there is also a need for someone thinking about the blending of physical and digital infrastructure, and what experiences need to be created for citizens and businesses in a city.
- Autonomous driving scientist and data specialist: these scientists and specialists will be responsible for enhancing automobile safety—creating a car that won't crash.
- Geospatial and mapping scientist: will use GIS and other software to produce, display, and analyse geographic information to propose R&D software solutions that follow emerging trends in mapping and geospatial systems.
- Energy efficiency engineer: managing energy consumption is increasingly crucial if smart cities are to be sustainable—whether in battery-operated phones and laptops or in huge data centres that collectively use billions of kilowatts of electricity each year.
- Network reliability engineer: cyber-attacks and disruptions are major threats to crucial infrastructure; ensuring secure, reliable communications has become vital.
- Urban informatics analyst: data collection is ubiquitous in smart cities. Making connections between data and human behaviour will enable problem-solving that results in more liveable cities.
- Integration engineer: will work with multiple systems, sharing data and using information from one system to drive another.

5 Market Study

The global smart city technology market is growing. According to market research and consultancy firm Navigant Research, the sector's revenues will reach $36.8bn (£28.35bn) in 2016. Despite the sector's growing profitability, many cyber security experts are concerned that smart city technologies are being adopted faster than the technology needed to protect them.

The potential market for smart cities could be more than $1 trillion by 2020, with technology helping to improve everything from traffic control and lighting to energy and water management.

Frost & Sullivan in their report "Strategic Opportunity Analysis of the Global Smart City Market", predict that Smart cities are anticipated to create huge business opportunities with a market value of $1.565 trillion by 2020.

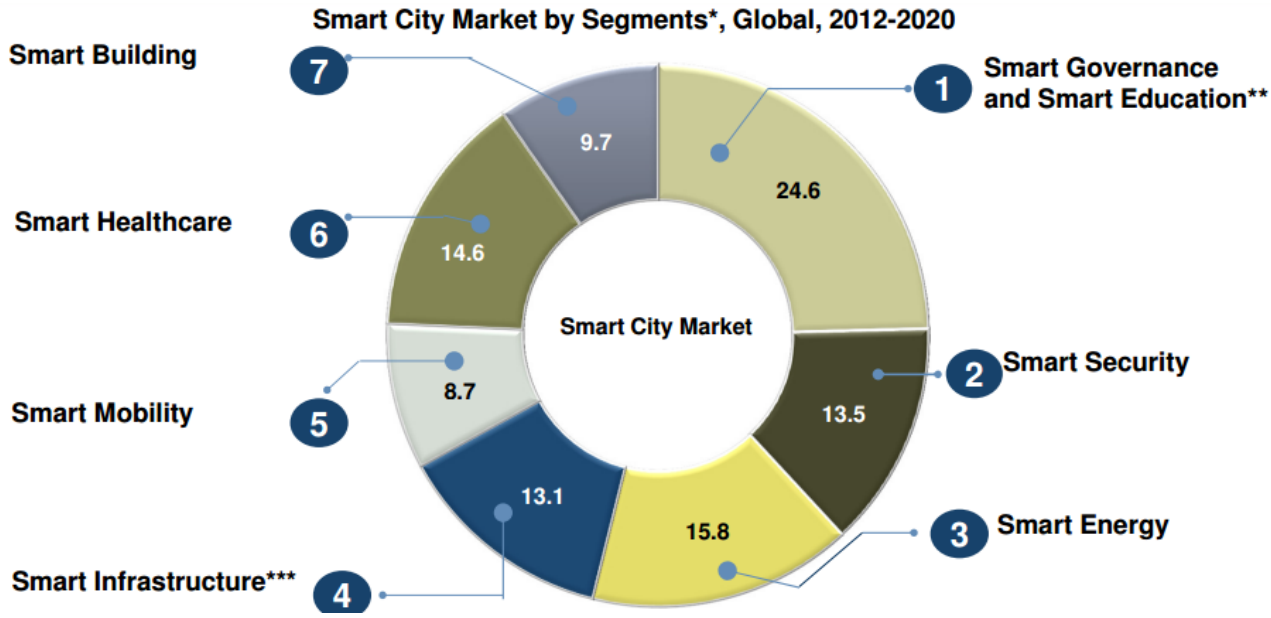

Figure 1 - Smart City by Segments

The Technavio market research company expects the global smart city market to expand by **16.6%** per year between 2014 and 2019. Another important market segment is the Internet of Everything (IoE) market. In the 21st century, IoE technology is making life easier for people. In the Research and Markets report "Global Internet of Everything (IoE) Market, By Technologies, Services, Applications, Devices, Verticals, & Regions - Trends & Forecast, 2015-2020" is estimated that by 2020, more than 50 billion of devices will connect to the internet and the IoE market is expected grow $23.97 trillion.

Competition

According to Frost & Sullivan, the main competitors in the smart city market segment are: IBM, Microsoft, Google, Hp, Oracle, SAP, ST Elettronics, Cisco, Alcatel, Ericsson, O2, Tyco, Serco, General Electric, ABB, Siemens, Senergy, and other shown in Figure below.

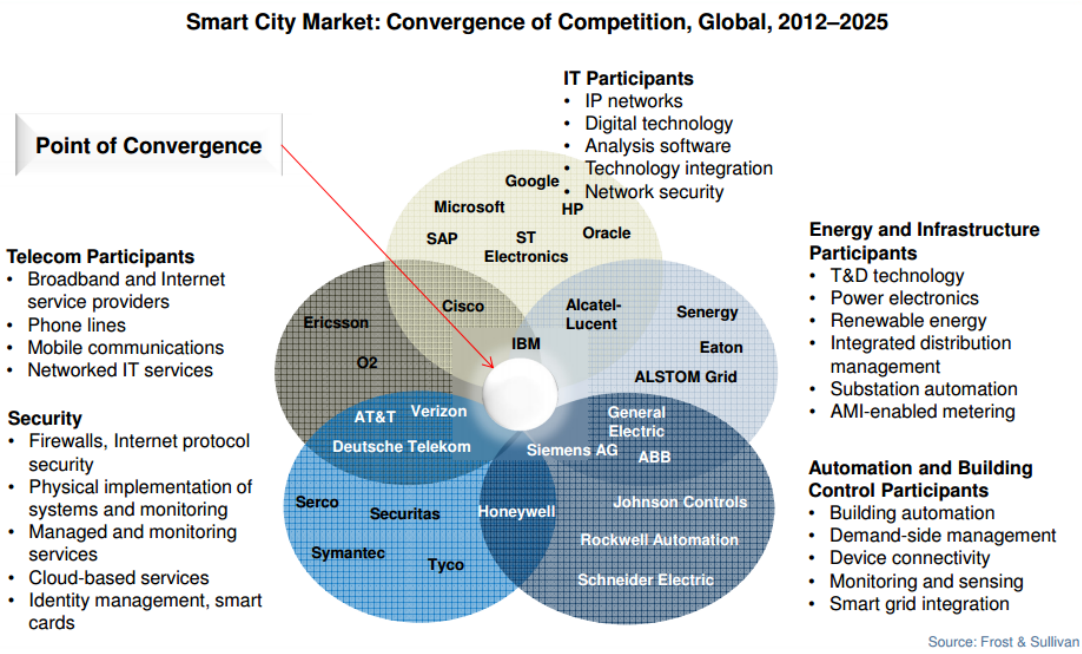

Figure 2 - Smart City Market

According to Research and Markets report, the large enterprises consider the IoE as the objective and strategy. Also, they would look to go for strategic acquisitions to remain competitive in the market. Major players such as Cisco, PTC Inc., QUALCOMM, Apple and Google are planning to create innovative products/services to support IoE market growth. The main competitors in the IoE market are: Cisco Systems, PTC, Qualcomm Technologies, Amazon.com, SAP SE. Samsung Electronics Co. Ltd., General Electric Company, Ericsson, Schneider Electric SE, Accenture PLC, Hewlett-Packard Development Company, L.P, Oracle Corporation, Freescale Semiconductor, Atmel Corporation, Continental AG.

Cities around the world — whether considered smart or not — face significant cyber security threats. These problems could have a direct impact on government, residents and the companies and organisations doing business there. Cyber security in cities is extremely important, but we have yet to fully realise the risk.

The global smart city market is expected to reach US$1.565 trillion in 2020, with one-half of smart cities from North America and Europe[8]. E-Services to citizens, such as e-Payments, e-Exchange, e-Sharing, etc., will empower citizens with real-time access to personal data and related services.

[8] Source: Frost and Sullivan

Although the exact form that smart cities will eventually take remains uncertain, organisations and city planners can take many precautions to ensure a smoother implementation process and, ultimately, more secure infrastructure[9]:

- Prioritise the security of critical assets: Contemporary networks are already impossible to protect in their entirety, a problem which will apply equally to smart cities. Some components of the system will have to be made more secure than others. Public and private city providers will need to work together to identify the city's critical assets and oversee the institution of appropriate security measures.
- Behaviour based security: Auditing millions of separate devices for signs of malware is simply not feasible. A more workable approach would be to evaluate the behaviour of smart city components and systems against an established baseline of normal functionality or network behaviour.
- Rapid component replacement: Given the potential for component failure or attacks compromising these components, an automated replacement system will enhance the security of the whole system.
- Segment critical assets of private organisations from the city's network: Paramount to the security of organisations in the smart city environment is the segmentation of their critical assets from the city's network.
- Connectivity and digital networking followed by cyber/network security and a clear vision and objective for the future. Additional components identified as crucial by the respondents are resilience and vision of a city as a system of systems.
- Reference architecture for data exchange in Smart Cities: Exchange is happening mainly among transport operators and/or transport-related operators as well as between transport operators and citizens. This integration leads to interdependencies that may bring cascading effects in case of an incident.
- Understanding and use of cyber security policy and critical assets are poor: Most respondents do not have a cyber security policy in place and do not use institutionalised and codified definitions for critical assets, either in business or societal critical terms. However, more mature organisations tend to have a more formalised approach towards critical assets.
- Lack of transversal information sharing on threats and incidents: Threats appear to be multi-faceted and directed against IT systems, data, infrastructure but also organisational structure (i.e., mismanagement) and the entire IPT infrastructures.
- Knowledge of cyber security: Overall, organisations in the city are not so willing to exchange information about cyber security, probably because of the reputational costs and other indirect losses related to cybercrime.
- Adoption of cyber security measures has been slow: Several cyber security measures and responses appear to be implemented by transport and SC operators following their level of maturity with some of the measures not fully deployed yet, which indicates that cyber security responses are rather new and in the making. The current lack of guidelines and good practices regarding cyber security limits the dissemination and acquisition of knowledge.

[9]http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf

Imagine what could happen if one or more technology-reliant services stopped working. What would commuting look like with no working traffic control systems, street lights or public transportation? How would citizens respond to an inadequate supply of electricity or water, dark streets and no cameras? What if waste collection was interrupted during the summer?

Cities are currently wide open to cyber-attacks which presents a real and immediate danger. The more technology a city uses, the more vulnerable to cyber-attacks it is, so the smartest cities face the highest risks. It's only a matter of time.

For cities, being prepared is key to preventing bigger problems and chaos. That means:

- Ensuring that the infrastructure is secure;
- Conducting a security audit of technologies before they are implemented; and
- Preparing an action plan in the case of a cyber-attack.

When we combine the fact that the technology used by smart cities can be easily hacked with the knowledge that there are cyber security problems everywhere, smart cities risk becoming dumb cities.

Cities are incorporating new technologies at an increasingly rapid pace, becoming ever smarter. Newer technologies — along with faster and easier connectivity — allow cities to optimise resources, save money and provide better services to their citizens.

We see two types of attitudes in market:

- Those who care about safety & security
- Those who care more about functionalities

The General Data Protection Regulation (GDPR) is forcing companies to explicitly state what the breaches are within their infrastructure.

If one specificity is interoperability, we can identify market opportunities looking at solutions for increasing (or enabling) interoperability between cyber security systems proposed by the different verticals.

References

ENISA, https://www.enisa.europa.eu

EY (2016). “Cyber Security A necessary pillar of Smart Cities”, http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf

Forbes, https://www.forbes.com/sites/gilpress/2018/02/14/6-ways-to-make-smart-cities-future-proof-cybersecurity-cities/3/

Frost and Sullivan (2013). “Strategic Opportunity Analysis of the Global Smart City Market”

NIST, International Technical Working Group on IoT-Enabled Smart City Framework https://pages.nist.gov/smartcitiesarchitecture/

Pollak, B (Ed.), Feiler, P., Gabriel, R., Goodenough, J., Linger, R., Longstaff, T., Kazman, R., Northrop, L., Schmidt, D., Sullivan, K., Wallnau, K. (2006). Ultra-Large-Scale Systems: The Software Challenge of the Future. Software Engineering Institute. Retrieved from: http://resources.sei.cmu.edu/asset_files/Book/2006_014_001_30542.pdf

Securing Smart Cities, https://securingsmartcities.org/?page_id=2

Tech Republic, “15 hot tech jobs for smart cities in 2018 and beyond”, https://www.techrepublic.com/article/15-hot-tech-jobs-for-smart-cities-in-2018-and-beyond/

UrbanTide and Scottish Government (2014). “The Smart City can be defined as the integration of data and digital technologies into a strategic approach to sustainability, citizen well-being and economic development”