A set of Good Practices and Recommendations for Smart City Resilience Engineering and Evaluation

Sandro Bologna, Glauco Bertocchi, Luigi Carrozzi, Donato Di Ludovico, Donatella Dominici, Priscilla Inzerilli, Luisa Franchina, Alberto Traballesi

s.bologna@infrastrutturecritiche.it

Abstract

Aim of the paper is to report the scouting activities performed by some Members of the Italian Association of Critical Infrastructures Experts (AIIC), addressing the state of the art in the area of Smart City Resilience, with a special emphasis on the relation between "smartness" and "resilience".
The justification for the research activity dealing with urban resilience and smartness is clear: urban areas, the engines of economic growth, are projected to provide the living and work environment for two-thirds of the global population of close to 10 billion by 2050. The concepts of smart city and resilient city go hand in hand with each other and thus are interrelated.
The AIIC Document, on which is based this paper, is primarily intended for use by organizations with responsibility for urban governance. However it is equally applicable to all types and sizes of organizations that represent the community of stakeholders, and in particular those organizations that have a role in urban planning, development and management processes in urban areas around the world.
The Document describes a framework and principles that want to be coherent with the entire UN Agenda 2030, in particular to goal 11 Sustainable Cities and Communities, to make cities and human settlements inclusive, safe, resilient and sustainable.

Introduction

There have been numerous studies attempting to define the Smart City concept, but it is still a difficult challenge to tackle. It is a multidisciplinary concept and to define '*Smart*' is difficult. The first attempts to define the concept were focused on the smartness provided by information technology for managing various city functions. Lately the studies have widened their scope to include the outcome of the Smart City such as sustainability, quality of life, and services to the citizens.

A good conceptualization of Smart City is represented by Figure 1.

The first appearance of the concept *resilience* in connection with urban policy dates to 2002. However, only not earlier than 2012 the frequency of searches in Google for Resilient City started to boom[1]. For the cities of the future to be smart, urban resilience must first be achieved.

In contrast with Smart City, the number of definitions of Resilient City is limited. Cities who call themselves resilient, like Rotterdam and The Hague in The Netherlands, claim to build capacity within individuals, communities, institutions, businesses, and systems to survive, adapt, and grow; no matter what kinds of chronic stresses and acute shocks they experience.

[1] http://smartcityhub.com/collaborative-city/smart-cities-resilient-cities-make-difference/

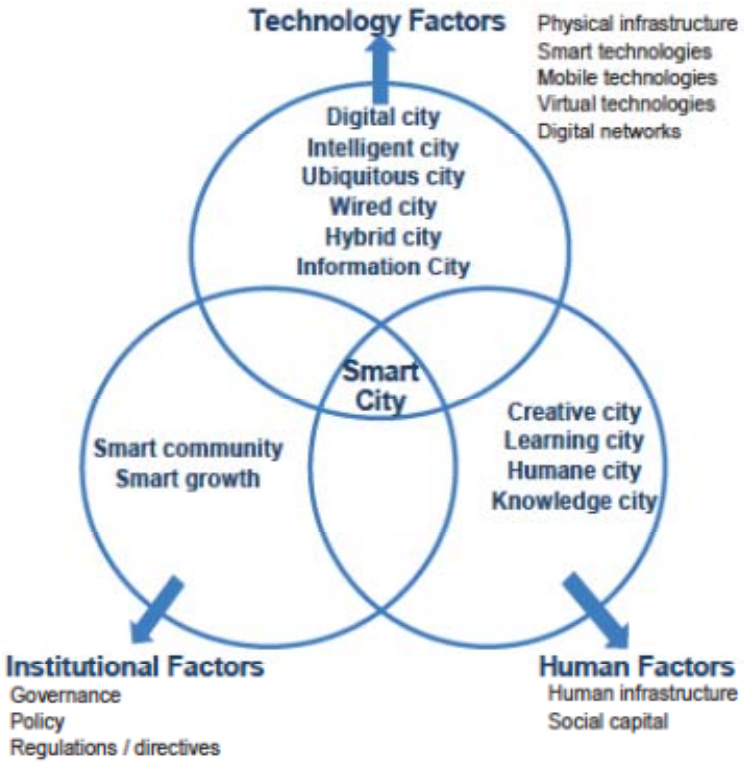

Figure 1. Conceptualization of Smart City

(*Source: Towards Smart and Resilient City: A Conceptual Model Y Arafah et al 2018 IOP Conf. Ser.: Earth Environ. Sci.* ***158*** *012045*)[2]

Resilience is an important factor as we are facing rapidly changing natural and social conditions, which require cities to be more resilient. The resilience concept in the context of a city refers to the city's ability to absorb, adapt, and respond to any changes in urban system. Therefore, a Resilient City is able to withstand the impact of shocks, hazards, and pressures through adaptability or transformation to ensure the long-term sustainability, basic functions, characteristics and the structure of a city (UNISDR, *How To Make Cities More Resilient A Handbook For Local Government Leaders*. Geneva: United Nations, 2012)[3]. Resilience cannot be reached in one step, it is a new approach to city design and implementation[4].

Smart Cities are powered by networks. Devices, people, businesses, and governments must all be able to connect securely, reliably, and quickly in order to share data to improve how people live, work, and manage their daily activities. Even while adopting the most current state of the art telecommunications and network technologies, a meaningful "Smart Cities" strategy must also pave the way for the integration of the next generation of wireless networks and services. This will have to occur not only in the telecommunications companies themselves but in all participating sectors of the economy. Additionally, inherent to any interconnected ecosystem, there are security challenges and altered expectations of privacy[5].

A Smart City approach must ensure that the increase in smart technology is accompanied by strategies to enhance cyber and physical security. As with any complex project, security and privacy

[2] http://iopscience.iop.org/article/10.1088/1755-1315/158/1/012045/meta
[3] https://www.unisdr.org/files/26462_handbookfinalonlineversion.pdf
[4] https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/smart-city-resilience-digitally-empowering-cities-to-survive-adapt-and-thrive
[5] Clinton A. Vince and Jennifer Morrissey "Smart Cities – Modernizing Our Infrastructure as a Platform for Exciting Technology" IEEE Smart Grid Newsletter, March 2018

must be baked in. That's especially so when a government agency and/or public institution works with vendors and contractors to get the work done - and usually, they do. Having a third party involved raises another level of security awareness to any IT project, even the most trivial. It opens the network to whatever malware infections the contractor brings-in, whether it's cash registers or smart streetlights. Adding the IoT, sensors, GPS, and lots of new stuff is the rule. That type of infrastructure is especially vulnerable to hacking, due to ill-thought-out IoT security. That's because there's been a big push to do IoT cheap and get Internet-enabled devices to market quickly. Developers rely on specific functions in open Source code to do that.

These sensors and smart devices can allow government agencies to not only capture data through IoT-enabled sensors, but to deliver that data to an Intelligent Infrastructure Management (IIM) system. This system performs real-time monitoring of the condition of assets, as well as predicts their condition over time, by applying algorithms that make use of Artificial Intelligence and Big Data Analytics. Armed with this real-time and predictive data, government officials can take immediate action, such as dispatching road maintenance crews, rerouting traffic or deciding whether to repair something, tear it down or invest in new assets.

Smart City Security and Privacy Concerns

Smart City technologies also open new vulnerabilities. Cyber-attacks can bring these thriving Smart Cities to a standstill and create total chaos. Ensuring cyber-physical security against local and foreign adversaries is the new challenge for today's city planners. However, some of the smart devices used for implementing Smart City cyber-physical solutions are not sophisticated and they lack basic security safeguards. Cybercriminals are aware of the various weak points and they are ready to exploit the weaknesses.

Naturally, urban planners and Smart City governments are proactively seeking ways to make their cities infrastructure and their Industrial Control Systems (ICS) safe from potential threats. Smart cities must look at their security needs both at the macro and the micro levels[6].

There are no doubt Smart Cities are the wave of the future, but in their rush to become smart, cities need to think about a total security program and ensure security is built into devices.

The paper "*Cyber security challenges in Smart Cities: Safety, security and privacy*"[7] examines two important and entangled challenges: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go together with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live. The interactions between person, servers and things are the major element in the Smart City and their interactions are what we need to protect.

The security and privacy of information in a Smart City has been interest of researchers. The reason behind it is that, in order to ensure the continuity of critical services like health care, governance and energy/utility issues in a Smart City, the information security must be fool proof. The factors that are taken under consideration in order to identify the issues in information security in a Smart City include governance factors, social/economic factors and most importantly economic

[6] Automation, September 24, 2018: How ICS Security Attacks can Cripple Smart Cities
[7] https://www.sciencedirect.com/science/article/pii/S2090123214000290

factors. These factors are elaborated in the paper "*Smart Cities: A Survey on Security Concern*"[8]. In our Report, we have specific sections dealing with security and privacy, also in the light of using new technology solutions like Artificial Intelligence.

Smart City as a complex System-of-Systems

A Smart City constitutes a "System of Systems" and a set of private and public systems that the city integrates for good governance and to achieve better services for citizens. Further, as being key criteria of ideal system all major components of Smart City i.e. education, transportation, energy and water, healthcare, other ICT systems must be planned and completed simultaneously as each element of process does not appear feasible when considered separately but becomes feasible when considered collectively, see Figure 2 from "*Conceptualizing Smart City with Dimensions of Technology, People, and Institutions*"[9].

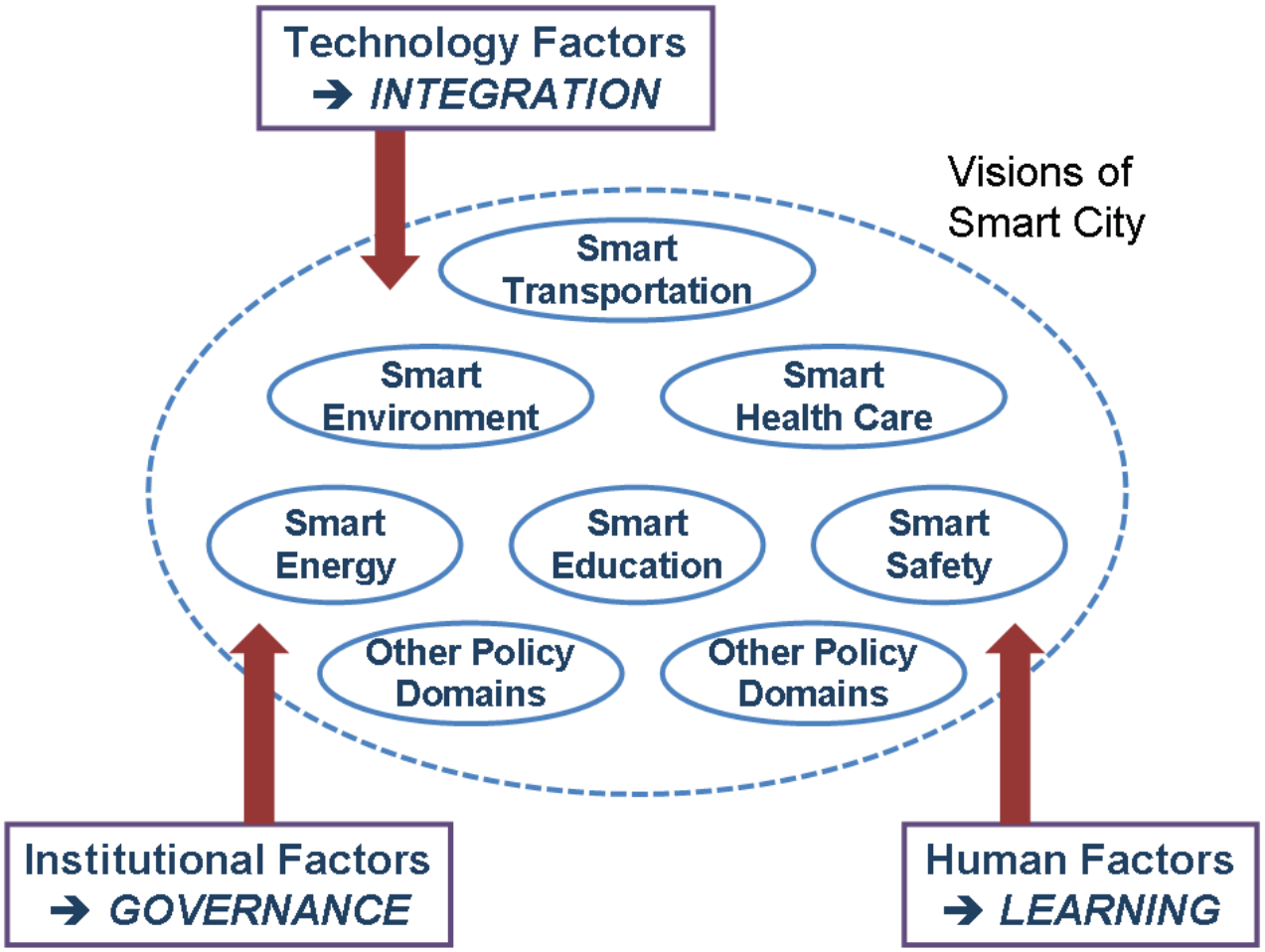

Figure 5. Conceptualization of Smart City

(Source: Conceptualizing Smart City with Dimensions of Technology, People, and Institutions)

[8] http://thesai.org/Downloads/Volume7No2/Paper_77-Smart_Cities_A_Survey_on_Security_Concerns.pdf
[9] https://inta-aivn.org/images/cc/Urbanism/background%20documents/dgo_2011_smartcity.pdf

To date, systems in Smart Cities have been often developed and deployed in significant fragmentation and isolation, each one responsible for tackling specific areas, concerns, and problems in the city. This might be explained by the fact that these systems are often complex enough in their own right, even before starting the exploration on how they can interact with each other in the daily life of a city. As a result, some implementations of the Smart City concept in urban agglomerations around the world have been done in a bottom-up approach. In this sense, cities would become smarter through decentralized initiatives and gradual implementation of successive projects, each one focusing on a specific objective. Although these applications and systems may be relatively mature in some specific fields, it is easy to observe that collaboration and coordination among them are missing. This type of situation may lead to an unmanageable and unsustainable sea of systems, thus preventing solutions of becoming more efficient, scalable, and suitable to support new generations of systems and services that are not envisaged yet (*Challenges to the Development of Smart City Systems: A System-of-Systems View*)[10].

Figure 3 gives an idea of the interconnection and permanent information of each point of the city thanks to **Internet of Things** and the need of permanent interpretation of data for the evaluation and evolution of the state of the city making **Big Data Analytics** essential.

For a comprehensive presentation about the different Systems making a Smart City, the reader can refer to "*IEEE 9th International System of Systems Engineering Conference - John Fennell Lead, Smarter Cities IBM ANZ – 2014*"[11]. The presentation gives a bright view of the different Systems making a Smart City a System-of-Systems.

The issue of how to model interdependency among different infrastructures is very challenging. In literature, different techniques are available for modeling lifelines interdependencies, see Eusgeld et al. 2011[12],

[10] http://www.dimap.ufrn.br/~everton/publications/2017-SBES.pdf

[11] http://sosengineering.org/2014/wp-content/uploads/2014/05/Smarter-Cities-System-of-Systems-Fennell.pdf

[12] http://webarchiv.ethz.ch/lsa/people/phd/cnan/sos.pdf

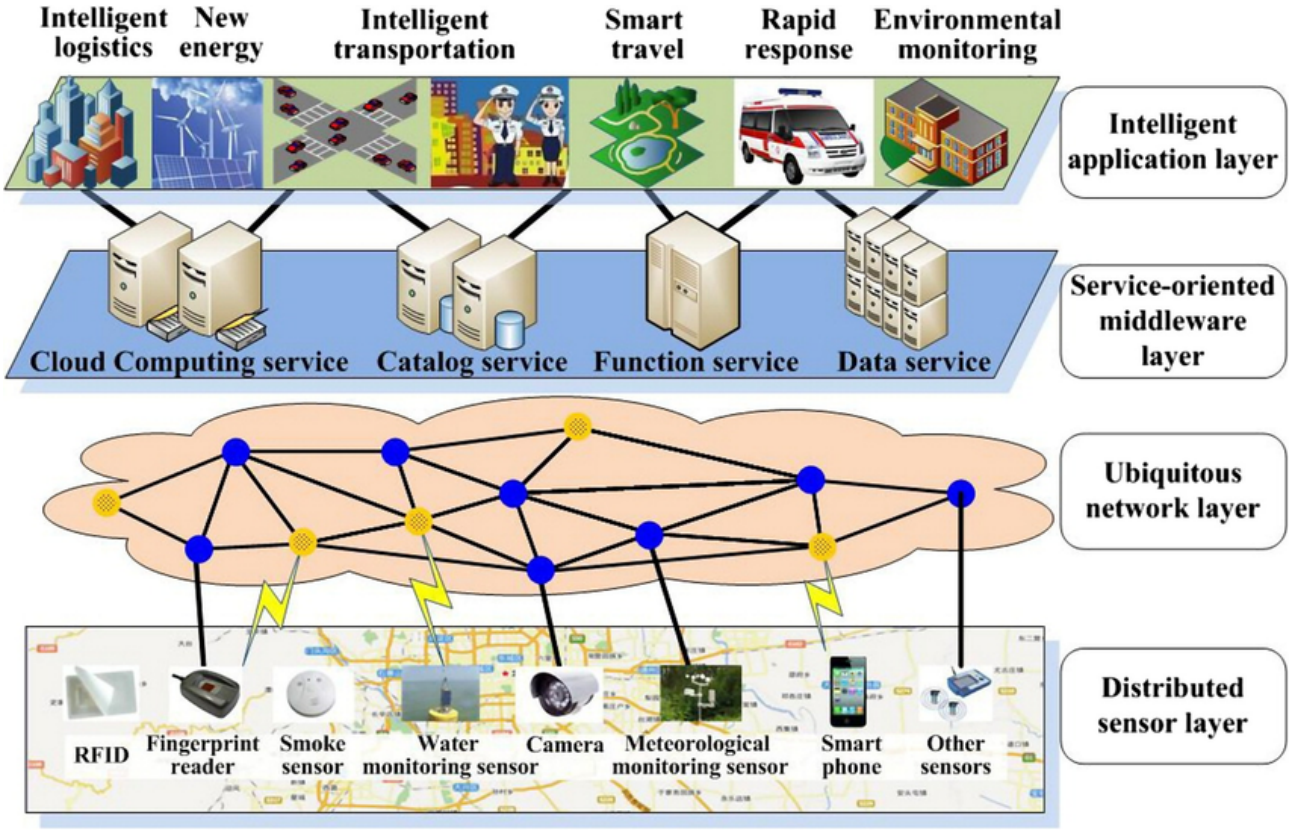

Figure 3. Smart City Layers – How difficult will be to manage a Smart City
(*Source WEB*)

The role of IoT and Big Data in the Smart City Resilience

The implementation of the concept of Smart City Resilience will benefit of the two most disruptive technologies of these last years:
Internet of Things: Interconnection and permanent information of each point of the city.
Big Data: Permanent interpretation of data for the evaluation and evolution of the state of the city.
This is well illustrated in the following Figure 4.

Although there is no standard model for IoT architecture, particularly with respect to network architecture, there are recently published studies in which propose some new IoT model are discussed in their applicability to Smart Cities' resilience. In a context of a (smart) city development, we have to consider the necessity to manage and process thousands and thousands of data generated by various Sources (as shown in Figure 4) through IoT devices interconnecting and communicating with each other in the most efficient way.

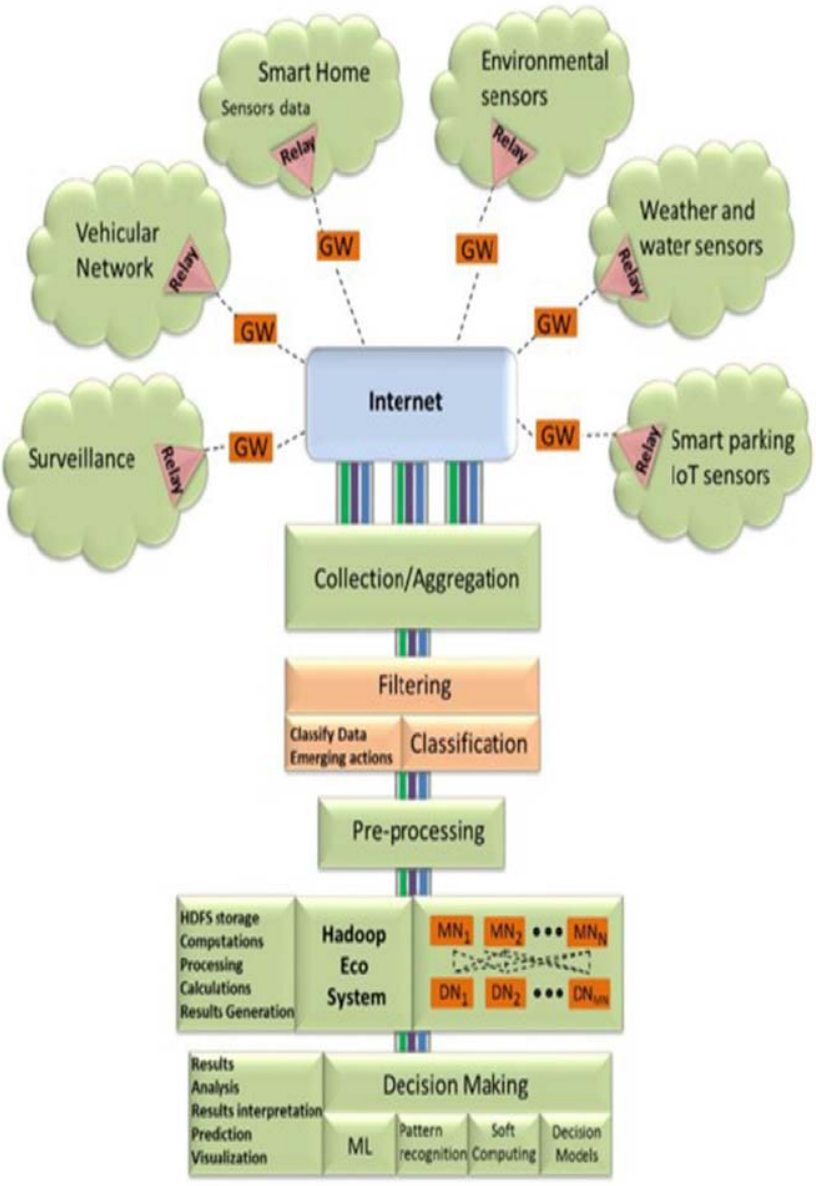

Figure 4. Sensors deployment.
(Source: Development of SMART CITY Using IOT and BIG Data)

How to combine the Smart City and the historic centre: suggestions from a case study

An example comes from the post-earthquake reconstruction of the City of L'Aquila and its historic centre, which is suffering the lack of urban planning and urban design. Faced with this problem, the acceleration of urban transformation resulting from reconstruction is producing widespread experiments in advanced technologies in the renewal of infrastructures, services and mobility, supported by significant public and private investments. These are innovations that often concern the historic centre and sometimes the periphery, ongoing experiences that invest first the field of knowledge that in L'Aquila assumes a role of absolute importance in relation to the innovation of survey techniques and of investigation that concerned most of the buildings inside the medieval walls. Then there are interventions that can be included in the "Smart" context, such as the Smart Ring, the technological tunnel, the structural monitoring through the sensors, the augmented reality, the 5G for which L'Aquila is one of the cities of experimentation and which will make it

possible to significantly improve the capabilities of mobile broadband and to address the new needs of the online society. All these innovations, which concern the context of resilience, are taking place on an urban settlement form deconstructed by the earthquake and reconstruction. The danger is that these technological innovations, particularly aimed at increasing safety and the level of urban services, in the absence of a comprehensive and articulated urban regeneration project that connects them with the reorganization of urban components and their negative dynamics, are likely to have a reduced effectiveness. Among other things, these are innovations disconnected from a coordinated program.

The scientific research of the University of L'Aquila and its Laboratories is addressing these issues, connected to historic contexts, bringing them back within the framework of innovative tools of urban knowledge and urban design oriented towards resilience, a study in which the L'Aquila case is considered paradigmatic.

The reconstruction of L'Aquila began based on an intentionally 'ordered' model, the outcome of a disciplinary rationality substantially restrained to functionalist planning applied to the modern city and of an institutional rationality optimistically projected towards inter-institutional governance, blocked however by a comparison-clash between local powers and central administration. In L'Aquila prevailed a 'structural' and static vision of the territory, linked to the great road system, to the geomorphological constraints, to the landscape and historical monumental constraints. But above all, a concept linked to the survival of the two models that have always characterized the territory of L'Aquila, the urban-centred one focusing on the functions of the historic centre, and the polycentric one built on a diversification of the functions of the hamlets. The earthquake not only heavily modified this settlement structure producing new temporary aggregations (CASE Projects, MAP and DCC houses 58/2009) with a substantial consumption of soil but has relocated new centralities and with them has produced a shift of residences and a variation of flows determining in substance a porous and widespread city which corresponds to a new citizenship that manifests predominantly individualistic behaviours.

But if any form of programmatic rationality and urban planning has disappeared, experiments of advanced technologies in the renewal of infrastructures, services and mobility have been widespread, supported by significant public and private investments. These are innovations that almost exclusively concern the historic centre, realizations in progress and rapid evolution that can be summarized with the following points:

- The Smart Tunnel (Figure 5), a tunnel in which the underground networks are housed in a single location under the road surface of the historic centre[13].
- L'Aquila Smart Grids, which empowers technologies and services for the Smart City that arises from an agreement protocol between ENEL (National Electricity Agency) and the Municipality of L'Aquila signed in 2013. It is a series of interventions on the electricity distribution network aimed at implementing capabilities of smart energy networks.
- Structural monitoring, through sensors for assessing the vulnerability of structures and for planning maintenance activities (a University of L'Aquila experimentation[14]).
- Augmented reality (Figure 5), through which to represent new levels of information and keep the memory of the reconstruction phases of the city but also of its history (a University of Aquila experimentation[15]).
- The 5G, for which L'Aquila is one of the cities of experimentation and which will greatly improve the capabilities of mobile broadband and address the new needs of the network society,

[13] Si veda http://www.sottoserviziaq.it/

[14] Potenza F. et alii, *Long-term structural monitoring of the damaged Basilica S. Maria di Collemaggio through a low-cost wireless sensor network*, Journal of Civil Structural Health Monitoring, 2015, 5(5):655-676, doi: https://doi.org/10.1007/s13349-015-0146-3.

[15] Brusaporci S. et alii, *Augmented Reality for Historical Storytelling. The INCIPICT Project for the Reconstruction of Tangible and Intangible Image of L'Aquila Historical Centre*, Proceedings, 1, 1083, 2017, 1-20, doi: https://doi.org/10.3390/proceedings1091083.

such as Self Driving Car, Work & play in the cloud, Augmented reality, Sensor NW, etc.[16] (University of L'Aquila / ZTE agreement).

Figure 5. Historic centre of L'Aquila. On the left the areas where the Smart Tunnel is made. On the right the experimentation of augmented reality on monuments.
(Source: on the left "L'Aquila un centro storico ricostruito smart" - Urbanpromo 2016; on the right[17])

These innovations are taking place on a destructured urban settlement and on a territory that the 2009 earthquake and subsequent reconstruction have radically changed, putting all the urban, social and economic components at stake and therefore presenting a very particular condition in which an acceleration of processes allows to experiment and verify new forms of spatial organization and of their governance. This experimentation, which leads back to the Smart and Resilience principles, allows us to have an idea of what will be the new drivers for the growth of areas of high historical value, with the aim of relaunching urban parts of significant dimensions where today the quality of life has several elements of criticality. However, some open questions remain related to the conservation purpose of historic buildings that, in the historic centre of L'Aquila, for example, did not allow the installation of technological plants to produce energy from renewable Sources[18]. In a historic centre like L'Aquila, 160 hectares large with the potential to house up to 20,000 inhabitants, the theme of clean energy is fundamental and must necessarily be addressed to meet the new needs of the contemporary city.

Smart City Security and Privacy Concerns

Smart City technologies also open new vulnerabilities. Cyber-attacks can bring these thriving Smart Cities to a standstill and create total chaos. Ensuring cyber-physical security against local and foreign adversaries is the new challenge for today's city planners. However, some of the

[16] IEEE, *ITU-R agrees on key performance requirements for IMT-2020="5G"*, 2017, in: http://techblog.comsoc.org/2017/03/02/itu-r-agrees-on-key-performance-requirements-for-imt-20205g/, last access: 25.01.2019.
[17] Brusaporci S. et alii, *Augmented Reality for Historical Storytelling. The INCIPICT Project for the Reconstruction of Tangible and Intangible Image of L'Aquila Historical Centre*, Proceedings, 1, 1083, 2017, 1-20, doi: https://doi.org/10.3390/proceedings1091083.
[18] SBAP, *Prescrizioni per gli interventi nei centri storici di L'Aquila e frazioni*, Comune dell'Aquila, Soprintendenza per i Beni Architettonici e Paesaggistici per l'Abruzzo, 2011, in: http://www.comune.laquila.it/moduli/output_immagine.php?id=1877, last access: 25.01.2019.

smart devices used for implementing Smart City cyber-physical solutions are not sophisticated and they lack basic security safeguards. Cybercriminals are aware of the various weak points and they are ready to exploit the weaknesses.

Naturally, urban planners and Smart City governments are proactively seeking ways to make their cities infrastructure and their Industrial Control Systems (ICS) safe from potential threats. Smart cities must look at their security needs both at the macro and the micro levels[19].

There are no doubt Smart Cities are the wave of the future, but in their rush to become smart, cities need to think about a total security program and ensure security is built into devices.

The paper "*Cyber security challenges in Smart Cities: Safety, security and privacy*"[20] examines two important and entangled challenges: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go together with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live. The interactions between person, servers and things are the major element in the Smart City and their interactions are what we need to protect.

The security and privacy of information in a Smart City has been interest of researchers. The reason behind it is that, in order to ensure the continuity of critical services like health care, governance and energy/utility issues in a Smart City, the information security must be fool proof. The factors that are taken under consideration in order to identify the issues in information security in a Smart City include governance factors, social/economic factors and most importantly economic factors. These factors are elaborated in the paper "*Smart Cities: A Survey on Security Concern*"[21]. In our Report, we have specific sections dealing with security and privacy, also in the light of using new technology solutions like Artificial Intelligence.

In a Smart City the attack surface is an extended one, because of the great number of interconnected cyber-physical things, spaces, infrastructures and users. Violations of data security can provoke the compromising of entire system, and an infection can be easily transmitted between systems.[22].

[19] Automation, September 24, 2018: How ICS Security Attacks can Cripple Smart Cities
[20] https://www.sciencedirect.com/science/article/pii/S2090123214000290
[21] http://thesai.org/Downloads/Volume7No2/Paper_77-Smart_Cities_A_Survey_on_Security_Concerns.pdf
[22] Daniela Popescul and Laura-Diana Radu " *Data Security in Smart Cities: Challenges and Solutions*" *Informatica Economică* vol. 20, no. 1/2016.

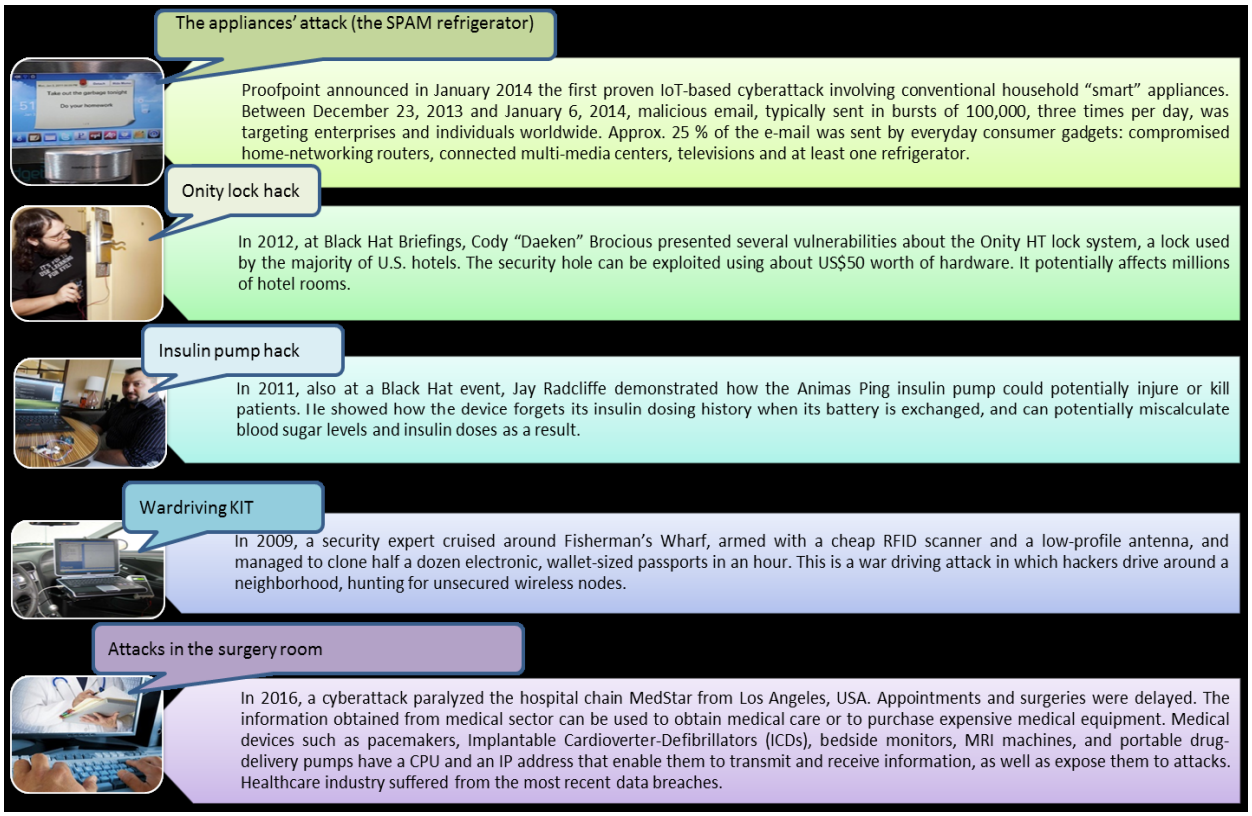

Figure 6. Attacks in a Smart City – some examples

(*Source: Daniela Popescul and Laura-Diana Radu* " *Data Security in Smart Cities: Challenges and Solutions*" *Informatica Economică* vol. 20, no. 1/2016)

As already previously stated, a Smart City can be modelled as system of systems and this consideration can drive a possible approach to cyber security.

We can consider that there are 3 types main components to be considered: 1) the networks that connect the devices and the systems; 2) the systems that provide services used by other systems or by one or more users; 3) the data used by systems to provide services and information to systems and users.

All these types of components must be secured against attacks and/or errors and this goal can be achieved using technical and organizational means that are appropriate to type and relevance of the objects to be protected.

It is beyond our scope and our capabilities, to provide a "complete and exhaustive" review of the very huge landscape of the feasible solutions. Our concern is to focus on some points we consider crucial and suggest a possible approach.

A first general consideration is that a cyber security system must be managed in order to keep the desired level of defence. A security system that is not managed became obsolete or ineffective in a very short time and all previous investments can be voided.

Consequently, you should identify and acquire the resources (financial, human, skills, etc.) needed to keep your security systems up to date and well managed.

A second general consideration is that "human factor" is one of the most relevant weakness in security (not only cyber) systems. People must be informed and trained to be aware of the risks related to cyber world. Users are probably the worst threat and the biggest opportunity; they can "destroy" your systems or help to keep a good level of awareness and security. Involvement of people is a difficult but rewarding task, many situations can be better approached with

organizational solutions instead of technical ones and people are the main component of every organization.

Another general consideration is to apply the "defence-in -depth" concept whenever and wherever is possible. In a system of systems this model can be viewed as a distributed defence where each component is protected against threats from "outside". A simple improvement of this model would include protection from "inside" to bound and prevent the spread of menaces to other systems.

Regarding networks one of the main concerns is to keep the bandwidth available, e.g. assurance of effective connections, and avoid the propagation of threats. Segregation of sub-networks can a possible solution that must be balanced with the capability of effective connection among end points in different subnetworks.

Systems that provide services are one of the main targets of threats focused on blocking or altering their functioning. They are also objectives of malware for data exfiltration. Cyber defence against these threats is a difficult and complex task and can be approached using multifaceted solutions (Intrusion Detection Systems on systems and on the network, specialized appliance or programs to identify Advanced Persistent Threats -APT-).

Data are the fundamental component of ICT world and consequently of a Smart City. Without data there are not services (smart or not) and information. Protection of data (confidentiality, integrity, availability) secure access to data is essential to functioning of a Smart City. The following paragraphs are focused on this aspect.

Need for Governance framework

The Smart City could be considered as an "enabling platform for the activities that citizens are able to develop, linking those inherited from the past to those that can be realized in the future, so it is not focused on just applications but on the possibility that citizens realize them"[23]
A Smart and Resilient City therefore is a very long, more correctly never ending program, composed by main relevant projects with a duration measured in many years (more than 5 e possibly within 15 years). During this time period many things can change (city political management, budget of the city, technology available, population variation in number and establishment, etc.).

It seems relevant to define what is a program and a project. *"At the most basic level, a project is created to deliver a specified 'deliverable' as efficiently as possible. Programs focus on the coordination of a number of related projects and other activities, over time, to deliver benefits to the organisation "*[24]

It is also useful to define governance in terms of setting strategic goals and monitoring their accomplishment when management is responsible of converting strategic goals in programs and projects and accomplish them in an effective and efficient way. [25]

A more comprehensive definition of Governance framework can be excerpted from Wikipedia:
Governance frameworks are the structure of a government and reflect the interrelated relationships, factors, and other influences upon the institution. Governance structure is often used interchangeably with governance framework as they both refer to the structure of the governance of the organization. Governance frameworks structure and delineate power and the governing or management roles in an organization. They also set rules, procedures, and other informational guidelines. In addition, governance frameworks define, guide, and provide for enforcement of these

[23] De Biase, L." *L'intelligenza delle Smart Cities (2012)*", http://blog.debiase.com/2012/04/intelligenza-delle-smart-city/
[24] https://mosaicprojects.com.au/WhitePapers/WP1002_Programs.pdf
[25] https://mosaicprojects.com.au/WhitePapers/WP1084_Governance_Systems.pdf

processes. These frameworks are shaped by the goals, strategic mandates, financial incentives, and established power structures and processes of the organization.

A Governance framework is needed to maintain consistency during the time period and make inevitable changes within the objectives. This concept can be passed on different elements, pillars to be organized and linked together[26]. In synthesis they can be summarized in three main pillars, as explained in Fig. 7.

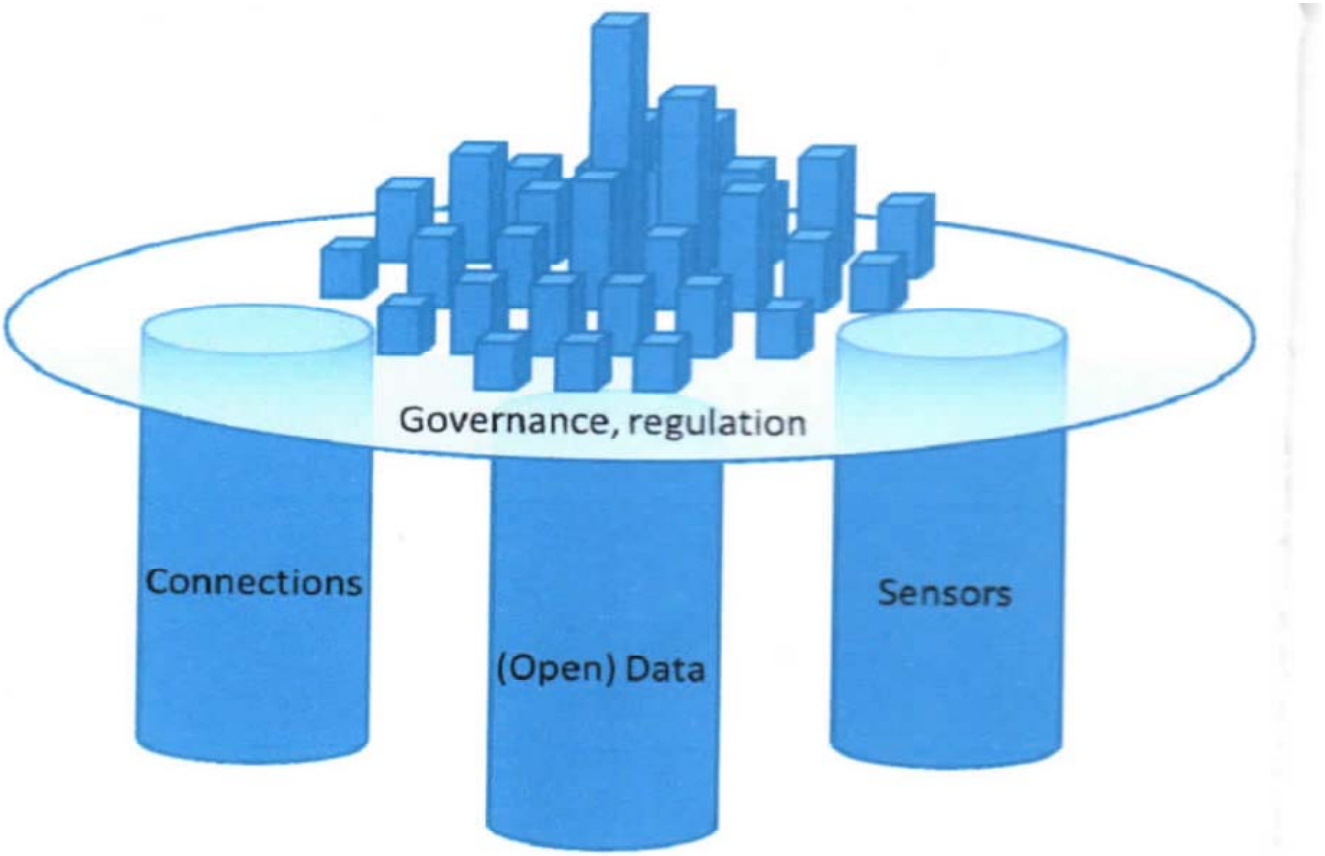

Figure 7. The pillars sustaining the Smart City and its Governance
(Source: Graphical elaboration, after concepts in De Biase, 2012)

These pillars must be combined with a governance able to link them together, giving a direction and a vision to the city.

As a consequence, a Smart City is an environment where a group of elements, as the ones above reported – sensors, data and connections – in combination with a collection of fundamental rules, gives public bodies, citizens, enterprises the possibility of developing applications and solutions able to improve life of the city itself, allowing also to create new markets and solutions also where the public sector is not able to make progress.

To support the city Governance framework a Management system is needed. Executive management is responsible for creating an organisation capable of achieving the objectives defined by program and projects and capable of providing assurances to the Governance that resources of all types are being effectively and ethically used in accordance with the organisation's policies.

[26] Beniamino Murgante1 and Giuseppe Borruso *"Cities and Smartness: A Critical Analysis of Opportunities and Risks"*
https://www.academia.edu/people/search?utf8=%E2%9C%93&q=Smartness+and+Italian+Cities.+A+Cluster+Analysis+

Securing supply chains

Supply chain management typically implies a sourcing strategy being aware that a fully integrated lifecycle approach to the product/services is recommended. NIST SP800-53[27] defines Supply Chain as **"***Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer*"

In cybersecurity an aspect whose importance is often underestimated is to provide a secure supply chain to systems. There is a large literature on procurement management and supply chains. The design of a product or a service generally implies an adequate overall control of the procurement process, but this becomes essential in case of cyber systems providing critical services for example to a Smart City and the evaluation of the supply chain risk is a primary activity.

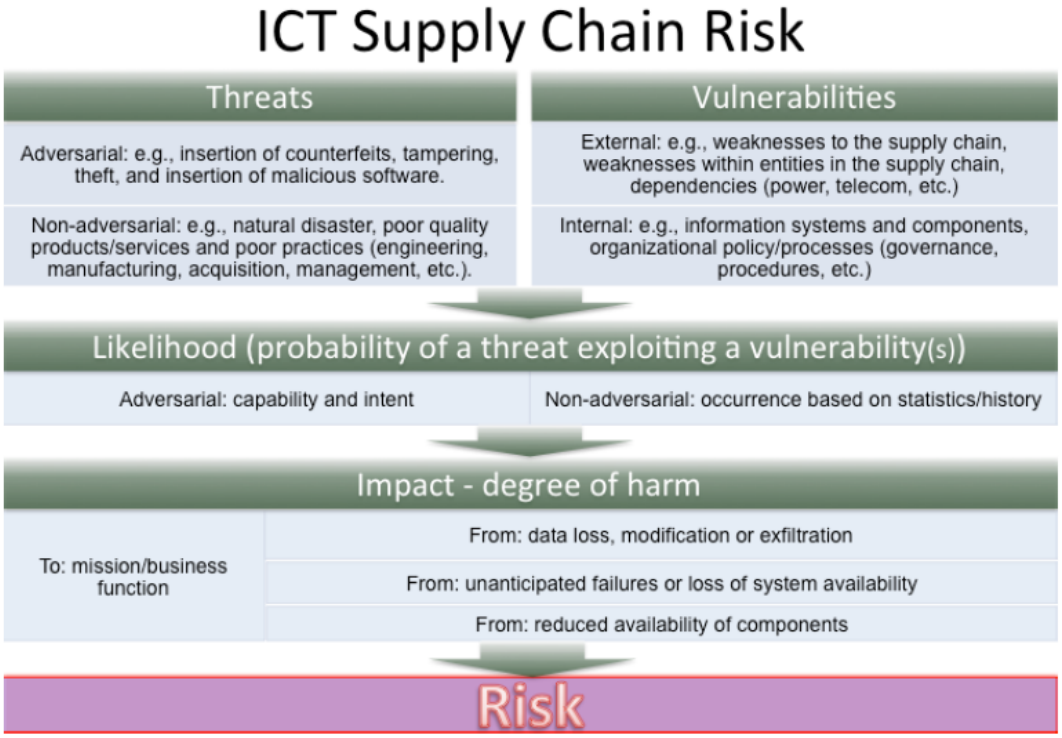

Figure 8. ICT Supply Chain Risk

(Source: NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations[28])

According to NIST[29] Cyber supply chain include risks from:

[27] NIST Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

[28] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

[29] NIST Best Practices in Cyber Supply Chain Risk Management - Conference Materials – Cyber Supply Chain Best Practices
https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

- *third party service providers or vendors - from janitorial services to software engineering - with physical or virtual access to information systems, software code, or IP,*
- *poor information security practices by lower-tier suppliers,*
- *compromised software or hardware purchased from suppliers,*
- *software security vulnerabilities in supply chain management or supplier systems,*
- *counterfeit hardware or hardware with embedded malware,*
- *third party data storage or data aggregators;*

and the best practices adopted by organizations to manage their cyber supply chain risks are the following:

- *Security requirements are included in every RFP and contract.*
- *Once a vendor is accepted in the formal supply chain, a security team works with them on-site to address any vulnerabilities and security gaps.*
- *"One strike and you're out" policies with respect to vendor products that are either counterfeit or do not match specification.*
- *Component purchases are tightly controlled; component purchases from approved vendors are pre-qualified. Parts purchased from other vendors are unpacked, inspected, and x-rayed before being accepted.*
- *Secure Software Lifecycle Development Programs and training for all engineers in The life cycle are established.*
- *Source code is obtained for all purchased software.*
- *Software and hardware have a security handshake; secure booting processes look for authentication codes and the system will not boot if codes are not recognized.*
- *Automation of manufacturing and testing regimes reduces the risk of human intervention.*
- *Track and trace programs establish provenance of all parts, components and systems.*
- *Programs capture "as built" component identity data for each assembly and automatically links the component identity data to sourcing information.*
- *Personnel in charge of supply chain cybersecurity partner with every team that touches any part of the product during its development lifecycle and ensures that cybersecurity is part of suppliers' and developers' employee experience, processes and tools.*
- *Legacy support for end-of-life products and platforms; assure continued supply of authorized IP and parts.*
- *Tight controls on access by service vendors are imposed. Access to software is limited to a very few vendors. Hardware vendors are limited to mechanical systems with no access to control systems. All vendors are authorized and escorted.*
-

It's clear that the higher is the complexity of the system (i.e. of number of providers, supply chain elements, systems architecture characteristics, etc.) the wider is the attack surface of the system and hence the likelihood to suffering a "supply chain attack"[30] that is the attack to the system occurring through a compromised third party involved in the supply chain.

Sustainable development of AI based Smart Cities respectful of individuals

Artificial Intelligence (AI) Systems are designed to improve efficiency, enable new business opportunities, enhance capabilities to generate value in all sectors of the economy and improve the quality of life of citizens. Smart Cities may take significant advantages from this technology in

[30] The supply chain attack is also known as "value-chain attack" or "third-party attack"

several critical city-life applications[31]. As a matter of fact, there is a remarkable growth of "intelligent systems" developed to support fundamental services such as transportation, mobility management, traffic control, public safety, energy systems and other relevant city management functions.

At the same time high concerns rise on protection of rights, dignity, self-determination and freedom of people. It's important to be aware of such relevant threats in order to identify possible solutions able to prevent harms to individuals thus adopting that "win-win" approach able to combine AI based Smart City applications and personal data protection.

All the potential provided by any AI system must be exploited in order to get beneficial output for individuals and society minimizing the drawbacks such as discrimination, unfairness, inaccuracy and bias when processing personal data.

The keyword for a sustainable Artificial Intelligence System development is the "Human Centered design". This means that when developing systems and services based on somewhat "intelligent function" that may infringe the rights and freedom of natural persons, a robust, preventive, risk management to avoid material and non-material damages to individuals should be put in place. Both private and public sector should design and deploy AI systems and application respectful of dignity, rights and freedom of each citizen. Algorithmic bias, discrimination, non-transparent and non-intelligible logic of algorithms and of the overall purpose of the system, undue profiling and performance non-aligned with the expected behavior by end user, are obstacles to overcome towards an "ethically sustainable" AI systems design. These topics need to forge a new mindset of industry, technology providers, as well as community managers and local authorities in order to drive Smart Cities in the right direction where the primacy of the well-being of population is recognized and every technology becomes an instrument for the achievement of this primary objective.

On these issues Hile Mehr in his paper "*Artificial Intelligence for Citizen Services and Government*"[32] writes about the important role that AI can play in delivering high value services to citizens and calls on government agencies to consider six strategies for applying AI to their work:

1. *Make AI a part of a goals-based, citizen-centric program*
2. *Get citizen input*
3. *Build upon existing resources*
4. *Be data-prepared and tread carefully with privacy*
5. *Mitigate ethical risks and avoid AI decision making*
6. *Augment employees, do not replace them*

[31] Examples of application of AI in smart cities can be found in the following links:
https://emerj.com/ai-sector-overviews/smart-city-artificial-intelligence-applications-trends/
https://www.automotiveworld.com/articles/artificial-intelligence-in-smart-cities-whats-the-link/

[32] Hila Mehr : Artificial Intelligence for Citizen Services and Government - Harvard Ash Center Technology & Democracy Fellow - https://ash.harvard.edu/files/ash/files/artificial_intelligence_for_citizen_services.pdf

Figure 9. Navigating AI in Government

(Source: Ash Center for Democratic Governance and Innovation - Harvard Kennedy School)

Conclusions

Resilience of a Community (a City is a Community) has been already investigated by our AIIC group among others and some concepts have been recalled in previous chapter 3. It depends on many factors, (see figure 6,7,8 of Guidelines for Community Resilience Evaluation[33]) and is based on a layered model (see figure 11 of chapter 3) that shares, obviously, most of the key infrastructures and functions with a Smart City.

A first question is: which is the most relevant aspect to be considered for a City, Resilience or Smartness?

In our opinion a strong synergy among the two aspects is the most appropriate answer but the two factors are not equivalent.

Smartness, if resilient, can give a big contribution to resilience in terms of communication, emergency management, time for recovery.

Smartness without resilience can worse an emergency making everything more complex due to sudden lack of complex and valuable resources.

In our opinion a Smart City must be designed and built using “smart” solutions that improve or, at least. do not decrease resilience, in fact smartness can improve daily life but resilience is essential to “survive” adverse events.

[33] http://www.infrastrutturecritiche.it/new/media-files/2017/03/COMMUNITY_Resilience_AIIC.pdf

References

Guidelines for Critical Infrastructures Resilience Evaluation
http://www.infrastrutturecritiche.it/new/media-files/2017/03/RESILIENCE_Guidelines_AIIC.pdf

Guidelines for Community Resilience Evaluation
http://www.infrastrutturecritiche.it/new/media-files/2017/03/COMMUNITY_Resilience_AIIC.pdf

Good Practices and Recommendations on the use of Big Data Analytics for Critical Infrastructure Resilience
http://www.infrastrutturecritiche.it/ new / media-files /2018/04/AIIC_BigDataCIPR_FINALE.pdf

A set of Good Practices and Recommendations for Smart City Resilience Engineering and Evaluation
https://www.infrastrutturecritiche.it/wp-content/uploads/2019/06/SmartCity-convertito-unito.pdf