EUROCITIES statement on the contractual public-private partnership on cybersecurity

Cybersecurity risks are one of the most serious economic and security challenges. Rapid urbanisation, increasing use of digital technologies and interconnected devices (Internet of Things, IoT) in sectors such as transport, communications, energy, healthcare, as well as public safety and security, have made cities targets of cyber attacks. The failure of information systems can have a considerable impact on the functioning of critical public services resulting in significant economic and social consequences for citizens and businesses.

Preventing or withstanding cyber attacks is a prerequisite for our cities to become smarter. The EU should fully recognise the issues at stake for cities as public authorities as the level of government closest to the citizens, and as service providers. The Commission should involve city authorities in developments aimed at boosting the level of cybersecurity in Europe to make the most of the benefits of a digital economy and society.

We support the European Commission's efforts to establish a contractual public-private partnership on cybersecurity (cPPP)[1] but recommend that training activities for citizens aimed at recognising and avoiding digital threats should also be included in the scope of the measures.

Our city experts have previously been involved in the Network Information Service (NIS) platform. It has been useful to bring in cities' views and concerns on cybersecurity risks but also share best practices examples. We remain committed to contributing to the cPPP from a city perspective and look forward to participating in its development.

Cybersecurity services and application areas

IT security measures need to be assured to create a secure, reliable and resilient smart city environment. City authorities are increasingly sharing responsibilities with national administrations for a number of specific cybersecurity services to be applied in different areas:

- Cybersecurity services provided by cities: identity and access management; security of data, applications infrastructures and hardware; IT security audit, planning and advisory services; IT security training (in certain cases)
- Application areas with demand in cybersecurity services: critical infrastructures;

[1] We refer to the European Commission roadmap 'Public Private Partnership on Cybersecurity', http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf

energy[2]; transport; public administration; smart cities; protection of data of individual users; local administration and finance

- Specific IT technology areas: cloud computing; Big Data; smartphones; software; hardware engineering

The challenges and risks for cities in cybersecurity

Smart grids and traffic control sensors are key targets for cyber attacks. The manipulation of those systems, e.g. traffic lights or electronic road signs, can have serious implications and lead to public safety issues.

City authorities are responsible for collecting and managing a great deal of data. They are also users of that data. Smarter cities are increasingly opening their data to promote transparency, business opportunities and citizens' participation. However, much of that data, for example on citizens' health or social identity, requires high levels of protection. *Extracting and using identity data for fraud* and *Intrusion in privacy* are pressing challenges for many cities. City authorities are increasingly experiencing 'phishing' i.e. the attempt to acquire sensitive and private information such as username, password or financial data via email.

Disrupting or slowing down network and computer functioning and distributed denial of service (DDoS) attacks are also common types of cyber threats for local administrations. Launched from multiple connected devices that are distributed across the Internet, these attacks are generally hard to deflect, mostly due to the sheer volume of devices involved, causing problems for undefined time. For example, following the Charlie Hebdo terrorist attacks in Paris in early 2015, several local authorities' websites in France were hacked and replaced with the ISIS flag and messages of terror.

Cities at work

City authorities are increasingly developing strategies and programmes aimed at preventing and mitigating cyber threats often in coordination with regional and national authorities and with the involvement of local private actors.

The adoption of cybersecurity standards and interoperability of solutions are part of those strategies. Common, open standards for cybersecurity, updated regularly (at least every 1 or 2 years) are a key priority for our cities[3] to establish an appropriate level of security in public sector information systems.

Example: implementation of cybersecurity standards in cities – Estonian national and local public administrations

ISKE is an information security standard developed for the Estonian public sector based on German information security standards – IT baseline protection catalogues. It is aimed at ensuring a sufficient level of security for the data processed in IT systems by implementing standard organisational, infrastructural

[2] Only in those cities where the management of smart energy grid and meters is a local competence.
[3] For more information please refer to the EUROCITIES statement on standards: http://bit.ly/1QvXTut

and technical security measures. Since 2000, national and local public authorities processing registers and databases must implement ISKE[4].

Example: The city of Stockholm implements guidelines for information security

Stockholm has been implementing mandatory internal guidelines for information security since 2010. The guidelines follow the internationally recognised standard ISO/IEC 27002:2005[5] and provide system owners in the city with an information classification model. By using this model when establishing a new information system, city officers can easily identify which level of security is required. These security measures are then incorporated in the new system.

As part of their digital strategies, city authorities are also engaged in awareness raising activities concerning cybersecurity as well as in education and training programmes for the next generation of cybersecurity professionals. The demand for cybersecurity experts is constantly rising. City authorities contribute to stimulating education and research in this field by supporting the creation of research centres and innovation labs for promising start-ups, involving also large companies and SMEs. However, such investments are costly and should be supported also through more funding opportunities at EU level focused on developing and testing cybersecurity measures locally, for the benefit of all.

Example: Start-up acceleration and business development programme - Rennes Metropole

After being certified with the 'French Tech' label[6] in November 2014, Rennes launched 'La French Tech Rennes St. Malo' programme aimed at accelerating local start-ups and promoting them internationally.

Cybersecurity is among the four[7] areas of expertise. The programme, overseen and partly financially supported by Rennes Metropole and Saint-Malo Agglomeration, gives opportunities to young entrepreneurs to learn and develop e-security solutions. It also promotes the development of the local ecosystem through partnerships and collaborations with large companies, research centres, universities and public institutions.

[4] More information on the ISKE standard are available here: https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf
[5] The ISO/IEC 27000-series comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).
[6] The French Tech label is assigned to French metropolises recognised for their startup ecosystem. It is also a name used by technologically innovative French businesses in all continents. The French Tech aims to provide a strong common visual identity to French startups as well as to promote entrepreneurial exchange between them; http://en.lafrenchtech.com/
[7] Together with audiovisual content production, online health information and smart cities and smart devices; http://lafrenchtech-rennes.fr/language/en/home-3/