European Committee of the Regions

Commission for Economic Policy

ECON

Digital Resilience

More information on the European Union and the Committee of the Regions is available online at http://www.europa.eu and http://www.cor.europa.eu respectively.

QG-05-23-158-EN-N; ISBN: 978-92-895-2664-7; doi: 10.2863/5099

This report was written by Simona Cavallini, Rossella Soldi (Progress Consulting S.r.l.), Gabriele Casalini, Giorgos Verdi, Antonio Grasso (European DIGITAL SME Alliance).

Edited by Ruth Harland

Table of contents

List of acronyms

COVID-19	Coronavirus Disease 2019
CEO	Chief Executive Officer
CEF	Connecting Europe Facility
CISO	Chief Information Security Officer
CSIRT	Cyber Security Incident Response Team
DCC	Digital Cities Challenge
DEP	Digital Europe Programme
DIH	Digital Innovation Hub
EaSI	Employment and Social Innovation
EC	European Commission
EDIHs	European Digital Innovation Hubs
ERDF	European Regional Development Fund
ESF+	European Social Fund+
EU	European Union
GDPR	General Data Protection Regulation
GHG	Greenhouse Gas
HE	Horizon Europe
ICC	Intelligent Cities Challenges
ICT	Information and Communication Technologies
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
JTF	Just Transition Fund
LRAs	Local and Regional Authorities
MMF	Multiannual Financial Framework
NRRPs	National Recovery and Resilience Plans
NUTS	*Nomenclature des Unités territoriales statistiques*
RIS3	Regional Smart Specialisation Strategy
RRF	Recovery and Resilience Facility
SGEIs	Services of General and Economic Interests
SGIs	Services of General Interests
SMEs	Small and Medium-sized Enterprises
5G	5th Generation

Executive summary

In the spring of 2007, Estonia's public services were under cyber-attacks for three weeks. This event is likely to have alerted several EU national governments on the vulnerability of their internet-based services. The 'spring' of digital resilience for public authorities began when it became evident that there was a need to associate digitalisation with information security. Nowadays, this need in the public sector is even more urgent and driven by increased digitalisation, growing interconnection and the mounting occurrence of cyber-attacks. EU legislation has been an important lever of change in public administrations, for example with the GDPR. In future years, it will continue to play this key role. The Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) and the Interoperable Europe Act are examples of legislation that will drive change in the digital resilience of public administrations.

This study is a pioneer in the investigation of the state of play of digital resilience of local and regional authorities (LRAs) across the EU. A primary drawback was the lack of a definition, in the literature, of the public sector's digital resilience. Bearing in mind that European LRAs provide a large variety of eGovernment services and that some LRAs are also responsible for services of general and/or of economic interests, the digital resilience of public authorities certainly encompasses the capacity to cope with threats affecting the provision of public services and the integrity of data. Thus, 'digital resilience' goes beyond the protection of ICT assets. It implies prevention and preparedness measures. If in place, it also ensures timely response and recovery actions from incidents.

Our first task was the identification of the main components of digital resilience. The study identifies 'legislative framework', 'infrastructures' and 'human factor' as equally important and complementary components in achieving digital resilience. Accordingly, digital resilience is defined as LRAs' ability to resist, absorb and recover from the disruption caused by external digital threats or natural disasters through the enforcement of legislation on cybersecurity and cyber resilience, the availability of solid and reliable critical infrastructures and the use of appropriate digital and cybersecurity skills.

Among the most important findings of the study are:

- Cyber-attacks occur frequently and increasingly, the public administration/government sector is the most targeted in terms of the number of incidents (ENISA, 2022) and there is some evidence that **local authorities are amongst the most vulnerable and preferred targets of hackers**.

- There is a **huge variation in the level of digital resilience across European LRAs**. Some public authorities began to invest in their digital resilience up to fifteen years ago, but others only just started or are still unaware of its importance.
- **Political will is a prerequisite** for prioritising investments in digital resilience, but there is low awareness of the importance of digital resilience among leaders, especially at the local level.
- The **main obstacle to increasing digital resilience** in LRAs is the **lack of funding.** This occurs even if the range of EU funding sources, including those channelled through the National Resilience and Recovery Plans (NRRPs), is varied.
- The second most important obstacle to increasing digital resilience in LRAs is **the lack of in-house technical know-how and experience**. For regional authorities, an important challenge is also the complexity of their organisational structure, as pursuing digital resilience requires **internal re-organisation**.
- **Multi-level cooperation across administrative levels** is the most needed type of support for enhancing LRAs' digital resilience. Technical assistance and best solutions sharing across LRAs follow.
- **Investments** in terms of digital resilience **prioritised most** by LRAs relate to **digital infrastructure, equipment and tools** as well as **security and protection of access to data.** The need to invest in systems/tools guaranteeing the continuity of services and in personnel training/awareness-raising follow. LRAs usually use a mix of funds for their investments.
- **Funds made available to regions and cities through the NRRPs are evidently important** in accelerating reforms and strengthening the infrastructure and skill components of digital resilience.
- **Different paths to digital resilience are feasible for LRAs.** Concrete examples are presented through case studies in Part 2.
- **LRAs' choice to invest in digital resilience or to bear the cost of digital non-resilience depends on a number of factors.** These factors are thoroughly discussed in Part 3 with supporting evidence.
- Although there is a 'general perception' of the impacts caused by incidents affecting digital infrastructures (i.e., digital incidents), LRAs' choice to bear the cost of digital non-resilience is affected by a **lack of awareness, capacities and methods to assess these impacts**.
- **Digital non-resilience** is a concrete **risk for smaller local authorities** (highlighted by the most likely scenario developed through a foresight exercise in Part 3) and tailored actions are needed to ensure that they do not lag behind.
- **Wild cards** such as *Artificial Intelligence out of control* and *Extreme automation in public administration* **may threaten LRAs' achievement of digital resilience by 2030**.

Our suggestions are structured around four main steps of a theoretical path leading to a reasonable level of digital resilience in LRAs. Suggestions address a wide range of actors, from EU institutions to local and regional administrations. The first step relates to the achievement of political awareness on the relevance of digital resilience. This is essential to proceed to the next steps. The second step relates to the definition of the most feasible governance model for digital resilience by the concerned authority. We identify at least five models in this study, based on the evidence collected. The third step relates to the choice of investment strategy and the identification of funding sources. In the last step, digital resilience goes beyond individual public authorities, pervades the ecosystem and is embedded in the resilience of territories.

From the methodological point of view, the study is based on a variety of approaches, including desk research, the development of case studies, interviews with experts and the design and implementation of an online consultation. The consultation ran from 19 January to 24 February 2023 and collected the validated contribution of 64 LRAs from 23 EU countries. Interviews were undertaken in January and February 2023 using a semi-structured approach and involved ten representatives from academia and think tanks, industry and the public sector.

Finally, the study is structured into five parts. The **introductory part** provides details on the definition of digital resilience and its components and an overview of how digital resilience is fostered by EU countries with a focus on the measures envisaged in the NRRPs. **Part 1** provides an overview of the state of play of digital resilience in cities and regions, according to the results of the online consultation and the findings of the interviews. The overview is complemented by desk research on investments made at a territorial level further to the implementation of the NRRPs and by a mapping of financial opportunities for digital resilience provided by the main EU funding instruments and programmes under the cohesion policy. **Part 2** is dedicated to deepening an understanding of the state of play of digital resilience at the local and regional level through the development of eight case studies on European regions and cities. **Part 3** explores a concept that is also pioneered in this study: the cost of digital non-resilience for LRAs. This part concludes with two foresight exercises to define scenarios of European LRAs' digital resilience by 2030 and to assess the relevance of wild cards on the evolution of this digital resilience. **Part 4** includes recommendations to facilitate the achievement of a reasonable level of digital resilience by LRAs.

Introduction

During the COVID-19 pandemic, societies and economies became more digital than ever as governments sought to harness the power of digital technologies in order to prevent the spread of coronavirus (Courtney, 2020). Whereas the pandemic crisis accelerated a digital transformation in Europe, the invasion of Ukraine by Russia with the emergence of a new geopolitical landscape highlighted new challenges to the use of digital technologies, such as the cyber intrusions by Russian nation-state cyber actors against Ukraine's government (and military) functions during the ongoing conflict (Microsoft, 2022).

This is not the first time that vulnerabilities associated with the digitalisation of services and processes have generated broad societal disturbance. There are well-known examples demonstrating how the integration of ICT systems into the functions of public authorities, de-facto, implied higher risks of disruption generated by cyber-attacks, or by other external shocks such as natural disasters. For example, in 2007, cyber-attacks launched against Estonia amidst disagreements with Russia on the relocation of a Soviet statue disrupted the functioning of the national government, the Parliament and local governments for some time (Ottis, 2008). In July 2021, the flooding affecting Germany, Belgium and the Netherlands caused, among several other impacts, the disruption of mobile and telecommunication networks. In the Rheinland Pfalz region, it took one month to fully restore the mobile network and four months to restore broadband (Koks *et al.*, 2022). According to ENISA, the European Union Agency for Cybersecurity, the public administration/government sector was the most targeted in terms of the number of incidents (24% of all incidents). It was also the second most impacted in terms of economic losses after finance/banking (ENISA, 2022).

A definition of digital resilience.

This study focuses on the digital resilience of local and regional public authorities. As a first step, it is thus necessary to define what digital resilience is and what its core components are. Existing literature does not define digital resilience in the specific context of the public sector, but definitions are given in other contexts and are here used in order to extrapolate a definition that fits the study's scope. According to the UK Council for Internet Safety, '*Resilience can be defined as 'a process to harness resources to sustain wellbeing', and digital resilience as the application of this concept to technology, the internet and the digital age*' (UKCIS, 2019, p.1). DigitalEurope (2023) indicates that *'digital resilience refers to our ability as a society to use digital technologies to prevent and face crises like pandemics, natural disasters, cyberattacks and hybrid wars, while sustaining our financial and security assets'*. Furthermore, in the context of Regulation (EU)

2022/2554 on digital operational resilience for the financial sector, digital operational resilience is defined as '*the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions*' (Art. 3). Notably, the operational aspect of this definition refers to the continuity of access to services.

The above definitions offer glimpses of how digital resilience can be understood in the context of local and regional public administrations. Digital resilience evidently depends on secure infrastructures necessary for the delivery of essential services. Furthermore, it depends on the presence of digitally skilled individuals who can take action to counter, absorb and recover from incidents. These two aspects are necessarily framed in existing regulations and laws. More specifically, at a local and regional level, we consider the concept of digital resilience to be comprised of three components:

- A comprehensive legislative framework, that sets minimum cybersecurity and cyber resilience requirements, for example, for networks and information systems.

- Solid and reliable critical infrastructures, here meaning both the external infrastructure necessary for the delivery of public services (among which are, for example, power distribution networks) and LRAs' digital infrastructures, i.e., communication networks and information systems with their hardware and software.

- Appropriate digital and cybersecurity skills to understand and deal with risks, manage the consequences of incidents, contain damage and the spreading of outside attacks in local and regional authorities.

Hence, in this study, **digital resilience for LRAs** is defined as their ability to resist, absorb and recover from the disruption caused by external digital threats or natural disasters through the enforcement of legislation on cybersecurity and cyber resilience, the availability of solid and reliable critical infrastructures and the use of appropriate digital and cybersecurity skills.

With respect to the **first component**, LRAs are responsible for the adoption of EU and national legislation or standards which may also be added to other regional or local requirements. Legislation relevant to digital resilience may, for

example, determine how secure products, systems, networks, infrastructures and processes must be. Hardware and software products have increasingly become the subject of cyber-attacks, with the global cost of cybercrime rising to €5.5 trillion at the end of 2020, double that in 2015 (EC, 2021). Cyber-attacks can significantly impact the entire supply chain since one incident in a specific product propagates across systems and state borders in a matter of minutes. Notably, connected devices are forecast to rise to 25 billion units by 2025 (EC, 2021). This situation increases the potential attack surface for cyberthreats, particularly because connected devices are often shipped to customers with known vulnerabilities. So, legislative initiatives setting minimum secure product requirements in the Single Market contribute to reinforcing the digital resilience of all actors (i.e., citizens, businesses and public administrations).

At the EU level, there are several pieces of legislation addressing digital resilience. In 2019, the Cybersecurity Act (Regulation (EU) 2019/881) entered into force aiming to enhance the security of ICT products, processes and services by introducing a voluntary European cybersecurity certification framework. In 2022, the European Commission (EC) proposed the Cyber Resilience Act[1]. The proposal aims to create the conditions for the development of secure products, by ensuring that when hardware and software products are placed on the market they have as few vulnerabilities as possible and that manufacturers take security seriously throughout the life-cycle of their products (EC, 2022a). Once approved and enforced, these requirements are expected to ensure increased security/resilience performance of digital solutions procured by local and regional authorities, hence reducing vulnerabilities and risks. In terms of critical and digital infrastructures, EU rules are very recent and include the Directive on the Resilience of Critical Entities (CER Directive (EU) 2022/2557) and the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive (EU)2022/2555). The CER Directive replaces the 2008 Directive on European critical infrastructure, while the NIS2 Directive replaces the 2016 NIS Directive. These updates were necessary to address the integration of new technologies, such as 5G, and the increased interconnections between operators, networks and services (EPRS, 2022). In light of the rapidly evolving landscape of disruptions, the accelerated enforcement of this new legislation will be crucial. Under the CER Directive, Member States will adopt a national strategy to enhance the resilience of critical entities and carry out risk assessments at least every four years. The NIS2 Directive will set minimum risk management requirements that apply to public administration entities at a central and regional level. Member States may also rule that the Directive applies to public administration entities at a local level.

[1] COM(2022) 454 final.

The **second component** of digital resilience concerns solid and reliable critical infrastructures. Infrastructures in Europe are more interconnected and interdependent than ever; while this increases their efficiency, it also increases the risk of higher impact in case of incidents. Critical infrastructures are primarily those providing essential services and are found in sectors such as energy, finance, health, transportation and public administration. European citizens depend on the seamless functioning of these critical infrastructures to access public services and maintain their social and economic activities. It is therefore clear that in the event of an incident, the bedrock of services offered by local and regional authorities is affected by the disruption of these infrastructures. Instead, LRAs manage their own digital infrastructures, i.e., fixed and mobile communication networks and information systems, through which most public services are delivered. These comprise hardware, software and data centres that enable the adoption of new technologies (e.g., artificial intelligence, blockchain).

The **third component** of digital resilience concerns skills, comprising digital and cybersecurity skills. The digital skills gap affecting the EU's workforce has been well documented (Anderson, 2022). Looking at cybersecurity skills in particular, ENISA specifies that two situations may occur: a cybersecurity skills gap, i.e., '*a lack of appropriate skills in the workforce to perform cybersecurity tasks within a professional setting*', and a cybersecurity skill shortage, i.e., '*a lack of cybersecurity professionals to fill cybersecurity roles or, as aptly defined, the 'unfilled or hard-to-fill vacancies that have arisen as a consequence of a lack of qualified candidates for posts.*' (ENISA, 2021, p.5-6). It is reasonable to assume that LRAs may be affected by both. In addition, it can be assumed that competition between the public and private sectors for the hiring of cybersecurity professionals will rise. In 2019, Eurostat statistics show that 58% of European private firms found it hard to recruit ICT specialists notwithstanding a growth of 51% in the number of specialists over the last decade (Anderson, 2022).

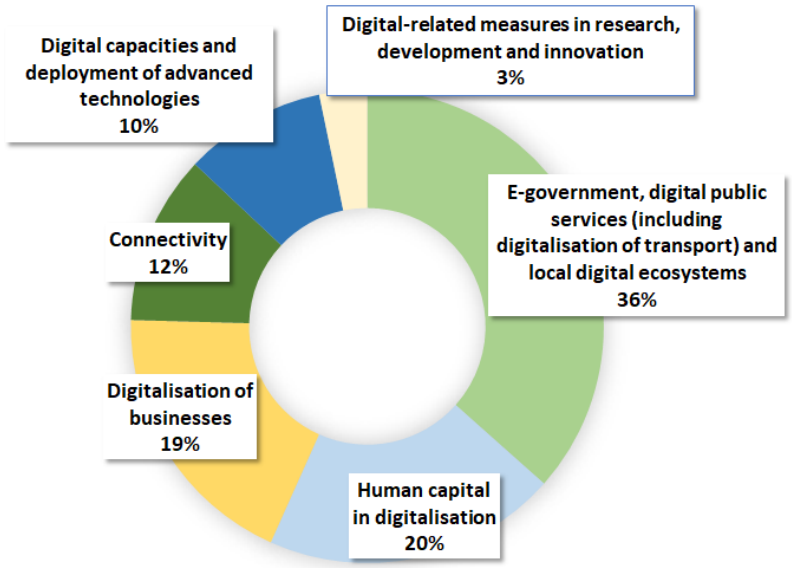
The definition adopted in this study clearly points to the fact that digital resilience extends beyond cybersecurity and the protection of ICT assets. It is only in the interplay of the three components above that LRAs can act and guarantee the functioning of their services thereby continuing to address the needs of citizens.

Member States' actions to support the digital resilience of public administrations.

Since 2021, the establishment of the Recovery and Resilience Facility (RRF) at the EU level offered ample possibilities to governments to invest in digital transformation, including for enhancing the digital resilience of their public administrations. The RRF Regulation (Regulation (EU)2021/241) identifies

digital transformation as a key policy area and a pillar (Art. 3) that guides the National Recovery and Resilience Plans (NRRPs). At an aggregated level, over 25 approved plans, the first annual report of the EC on the implementation of the RRF shows that 26% of the total RRF expenditure, or some €127 billion, were allocated to the digital transformation pillar (EC, 2022b). However, despite Member States exceeding the minimum requirement (20%), individual allocations diverge significantly. For example, Germany and Austria plan to invest 53% of their allocations to digital objectives; for Luxembourg, Lithuania and Ireland this figure is 32%; and for several other countries it is between 20% and 22% (Croatia, Estonia, France, Latvia, Poland, Romania, Slovakia, Slovenia and Sweden) (EC, 2022b).

Figure 1. Allocations under the digital transformation pillar (25 RRPs)



Source: data from the Recovery and Resilience Scoreboard.

The overview of the allocations made in the RRPs by policy area (Figure 1) clearly indicates that the digitalisation of public administration is a priority in Member States accounting for 36%, or €47 billion, of the total amount allocated in the NRRPs under the digital transformation pillar (EC, 2022b).

The other policy area used to support public administration's transformation and digitalisation is that of 'Digital capacities and deployment of advanced technologies' which accounts for 10% of the budget of the digital pillar. Investments for the skilling or upskilling of civil servants are made under this area, but also under the 'Human capital in digitalisation' area, which accounts for 20% of the budget of the digital pillar.

With reference to the first component of digital resilience outlined in our definition, **'enforcement of legislation'**, there is ample evidence that the RRF is used to pass reforms and implement new and existing legislation. Examples specifically referring to the enforcement of legislation related to digital resilience include (EC-DG DIGIT, 2022 – unless otherwise specified):

- the **Czech Republic** plans a €106 million investment for an initiative aimed at increasing the cybersecurity of public authorities and other entities under the country's Cybersecurity Act and related regulations.
- **Germany** allocated €3 billion to the implementation of the Online Access Act 'Onlinezugangsgesetz'. The law aims at deploying fully digital public services at all administrative levels (central, regional and local).
- **Greece** allocated €16 million to the deployment of big data management and analysis nodes to support its 'Management and governance of public sector data and ensuring compliance with GDPR' reform.
- **Slovakia** plans to invest almost €36 million in strengthening its capacity to prevent cyber incidents and to speed up the process for their detection and resolution. This investment contributes to implementing the reform '*on the standardisation of technical and procedural solutions for cybersecurity, which also implies the adoption of the National Concept of Informatisation of Public Administration for 2021-2030*' (EC-DG DIGIT, 2022, p.196).
- **Slovenia** allocated €10 million to support cross-border and multi-country projects on the development of digital infrastructures such as a European Common Data Infrastructure and the European Blockchain Service Infrastructure, with the aim of increasing security and integrity of data as well as of public service provision. These investments contribute to implementing the reform on the 'Development of economic data and digital services' and on 'Ensuring cybersecurity'.

With regard to the second component of digital resilience, '**infrastructures'**, NRRPs are populated by planned investments aimed at the enhancement of digital infrastructures and the deployment of advanced digital technologies. In some cases, these investments are explicitly linked to achieving digital resilience. For example (EC-DG DIGIT, 2022 – unless otherwise specified):

- **France** plans to invest €136 million in strengthening the cybersecurity of the public sector and, in particular, of the digital systems of national and regional administrations and public institutions.
- **Luxembourg** allocated €10 million to the development of a communication infrastructure based on quantum technology, with the aim of improving the security of public sector communications.
- **Poland** plans to invest €443 million in enhancing its national cybersecurity capacity and securing a data processing infrastructure (EC webpage on Poland RRP accessed in February 2023).
- **Portugal** allocated €47 to strengthening its overall cybersecurity framework. This allocation covers strengthening capacities in cybersecurity and information security; increasing security in the management and organisation of data; reorganisation of the coordination model for cybersecurity within the

public administration; and creation of the necessary physical and technological conditions for the implementation of the model.
- **Romania** allocated almost €375 million to the deployment of government cloud infrastructure that is cyber secure, energy efficient and based on latest technologies. The country plans several other investments related to the resilience and cybersecurity of digital infrastructure, including those of external providers to the public sector.

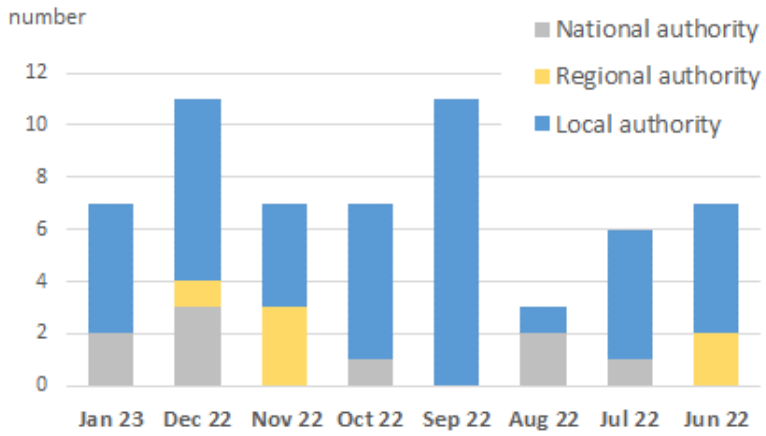
When considering the third key component of digital resilience, '**human capital'**, increasing civil servants' expertise in ICTs is expected to improve the efficiency and security of eGovernment services and processes and to take advantage of the benefits introduced by digital transformation. Examples of allocations made by EU countries for the upskilling of civil servants in digital and information security include (EC-DG DIGIT, 2022):

- in **Latvia**, around €8 million are earmarked for the strengthening of the digital capacity of public administrations. More specifically, investments target the training of 62,900 public administration employees and the development of self-learning and online learning material;
- in **Italy**, €490 million will be invested in strengthening the competencies and capabilities of public servants, including through online courses and communities of practices where experiences are shared within public administrations;
- in **Portugal**, €88 million are dedicated to the training of the public administration, in terms of both management (adoption of agile methods for delivering public functions) and technology (digital skills). This is part of a public administration empowerment policy aimed at creating 'public value' from the investments made in digital transition;
- **Romania** allocated €20 million to the training of civil servants in digital skills, with a view to supporting the digital transformation of the public administration and promoting a concept of life-long learning for public sector employees.

Embedding digital resilience at the local and regional level has become a necessity for Member States as regions and, more specifically, municipalities, are often targeted by cyber-attacks. For example, since Russia´s invasion of Ukraine and the related cyberthreats, Denmark has been making efforts to ensure the protection of the municipalities' digital systems and encouraging preparations for eventual emergencies (EC, 2022c). The same occurred in the Netherlands, where a list of basic cybersecurity measures to prevent a cyber-attack was prepared (EC, 2022d). Global cybersecurity industry player Kaspersky indicates that a higher vulnerability of municipalities is determined by the municipalities' services being interconnected to other entities (Kaspersky, 2019). Thus, the disruption of their

systems and services is more likely to damage several actors and/or sectors simultaneously, which is indeed an advantage for hackers. On the basis of the information collected on cyber-attacks by market research company konbriefing.com based in Germany, data related to public authorities in the EU27 countries and compiled from June 2022 to January 2023 clearly shows that local authorities (including forms of associated municipalities) are most targeted (Figure 2).

Figure 2. European public authorities suffering from cyber-attacks



Source: information gathered from konbriefing.com. Data handled by the authors.

Cyber-attacks were reported over the given period for 13 EU countries. Countries with the highest number of cyber-attacks were France (19 attacks out of which 13 were against local authorities), Italy (11 attacks out of which 8 against local authorities) and Germany (10 attacks all of which were against local authorities).

Links between green and digital transitions.

The relevance of green and digital transitions in EU policies is mirrored in the rules for budget allocation applying to the NRRPs. Each NRRP had to allocate at least 20% of the funds to digital transformation and at least 37% of the funds to climate actions (EC, 2022b).

The green and the digital transitions are often referred to with the term 'twin transition' meaning not only two concurrent transformations, but also a united process, ideally mutually reinforcing, intended to accelerate necessary changes and bring societies closer to the level of transformation needed (Muench *et al.*, 2022). Neither can succeed in the long term without the other, so the EU considers they are equally fundamental and instrumental to the goal of transforming Europe into a globally competitive, climate-neutral and digitalised economy and society.

In December 2020, the Council of the EU emphasised that the digital component will be key in reaching the ambitions of the European Green Deal and the Sustainable Development Goals. It also acknowledged that digitalisation is an

excellent lever to enhance environmental sustainability (Council of the EU press release dated 17/12/20). The Council's conclusions gave political guidance to the EC to exploit the opportunities offered by digitalisation for environmental protection and climate action, and to reduce the environmental impact of digitalisation itself.

Furthermore, evidence shows that the digital and green transitions are instrumental to each other because **accelerating the digital transformation of our societies can help to reduce the overall carbon footprint**. It is estimated that digital solutions can reduce global emissions by at least 20% by 2050 (George, O'Regan and Holst, 2022). As such, it is acknowledged that digitalisation can contribute to the decoupling of economic growth from the use of non-renewable natural resources and environmental impact. In addition, digitalisation can promote circular business models in the private sector and address important market failures that stand in the way of scaling up the circular economy (OECD, 2022). To promote such processes, it is crucial to ensure that digital technologies do not generate more greenhouse gas (GHG) emissions than they save. At present, digital technologies account for between 8% and 10% of our energy consumption, and 2% and 4% of our GHG emissions. It should be noted that although these are small percentages, they have a considerable impact (The Shift Project, 2019).

The EU is launching initiatives such as the European Green Digital Coalition to foster the development and deployment of greener digital technologies as well as methods and tools to measure the net impact of digital solutions on the environment. The Coalition explores voluntary and binding measures to help the private sector become climate neutral and use more renewable resources, and will also serve to develop guidelines for public administrations to buy digital products and solutions that have a minimum possible impact on the environment.

Another important aspect characterising the twin transition is the **relevance of digital technologies to the protection of critical infrastructures**. As emphasised in the Strategic Foresight Report 2022, the cross-dependencies between the digital and green transitions were reinforced by the rapid evolution of the geopolitical context after the Russian aggression on Ukraine. In this scenario, the need for a secure energy supply and the protection of an increasingly digital energy system against cyber-attacks has become a priority (EC, 2022e). Beside the protection of critical infrastructures, advanced technologies offer situational intelligence in warning and response systems that are used to face and respond to natural hazards such as floods. Their cyber protection is thus a prerogative to the maintenance of a country's reaction and response capacity.

Overall, the promotion of the twin transition is a multi-level governance effort currently framed by the RRF Regulation. It is believed that NRRPs, under which investments are due to be completed by 2026, can encourage comprehensive reforms and initiate the long-term measures needed to make the twin transition a success while ensuring social and territorial cohesion across Europe (EPC, 2021).

Part 1. State of play of digital resilience in cities and regions

1.1 Overview of the state of play

In order to provide an overview of the state of play of digital resilience across cities and regions, we designed and implemented an online consultation addressing public authorities at local and regional level. In addition, semi-structured interviews with experts were carried out to gather more information (Box 1). Findings from the online consultation and the interviews are presented in this Part 1 as well as in Part 3 of the study that looks at the cost of digital non-resilience.

Box 1. Online consultation and experts' interviews

LRAs' consultation was based on an online questionnaire implemented using EUSurvey. The consultation was by invitation, meaning that it was not publicly available and could be accessed only by using personal links. This approach made the selection of the 'right person' (e.g., civil servants in charge of cybersecurity and/or information security and/or digitalisation) somewhat complicated and required significant input in terms of searching and networking[2], but was adopted so as to harvest quality results. Approximately 360 invitations were sent out across all EU Member States and 64 valid replies were received, for which participants are hereby thanked. Thus, the response rate is 18%. The survey was online from 18 January 2023 to 24 February 2023. Results are presented in an aggregated and anonymous form.

In January and February 2023, semi-structured interviews were carried out with ten experts[3], who are also hereby thanked, to analyse the digital resilience of LRAs from an external and qualitative perspective. The number of interviews was set with reference to the works of Eisenhardt (1989) and Yin (2003) who demonstrated that replication power can be achieved by collecting data from three organisations. Interviews involved three representatives of academia and think tanks, three industry representatives and four representatives of public authorities. Through this categorisation and whole-of-the-ecosystem approach, insights from the diverse perspectives were obtained to complement

[2] As many cyber-attacks targeting public authorities are perpetrated by email and phishing techniques are becoming increasingly sophisticated, a large number of LRAs across Europe allow contacts to their civil servants/departments only through online forms. In particular, Chief Information Security Officers (CISO) do not usually publicly disclose their emails on the web. The methods used to reach out to the 'right persons' include dissemination to experts' groups of EU networks and associations of LRAs across the EU as well as the use of Linkedin inMail to professionals corresponding to the profiles of interest (e.g., CISO).

[3] Affiliation of interviewed experts: EC-DG Connect, Innova Puglia, Open&Agile Smart Cities (public sector) – the fourth representative from the public sector opted not to disclose the name of the entity; FBK/University of Trento and Inspiring Futures (think tank/academia) – the third representative from think tanks opted not to disclose the name of the organisation; TeamDev, Nextcloud and an independent consultant (industry/private sector).

the findings of the survey. The experts' contributions are used in the report in an anonymous form and only making reference to the respective category.

The online consultation addressing LRAs received **64 contributions** from **23 EU countries**[4]. The consultation was based on a questionnaire comprising four sections. Section 1 was to collect **information on the authority** and the respondent. The **majority of the respondents (81%) are representatives of local authorities**; the remaining respondents (19%) represent European regions[5] (Figure 3). Participating authorities have **variable sizes** in terms of employed civil servants (Figure 4). Local authorities range from very small (0-50 employees) to very big municipalities (over 10,000 employees). A wide variation in size is also observed across participating regions; one-third of the regions have over 10,000 employees. As mentioned above, the geographical coverage of participating public authorities across the EU is very comprehensive. Overall, these authorities serve more than 44 million citizens[6], i.e., about **9.9% of the EU27 population**. We therefore deem the results of the consultation sufficiently representative to provide an overview of the state of play of digital resilience of local and regional public authorities across the EU.

Figure 3. Type of participating authorities

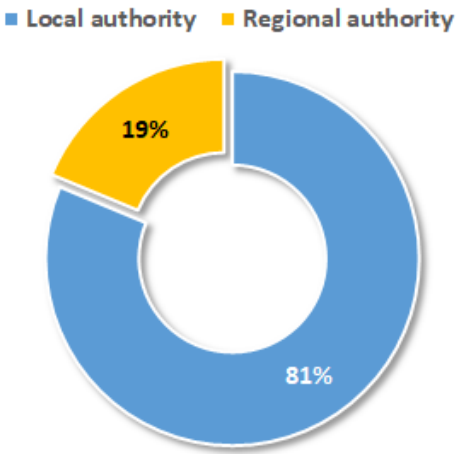
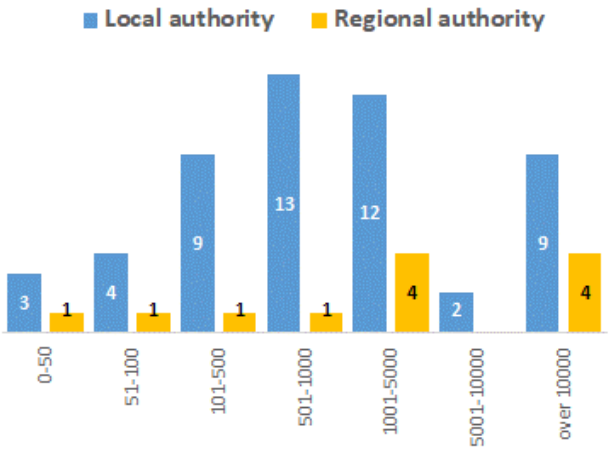


Figure 4. Size of participating authorities according to the number of staff



Source: online consultation

With regard to **cybersecurity management**, all participating authorities have somebody in charge, with the exception of one respondent who is not aware of

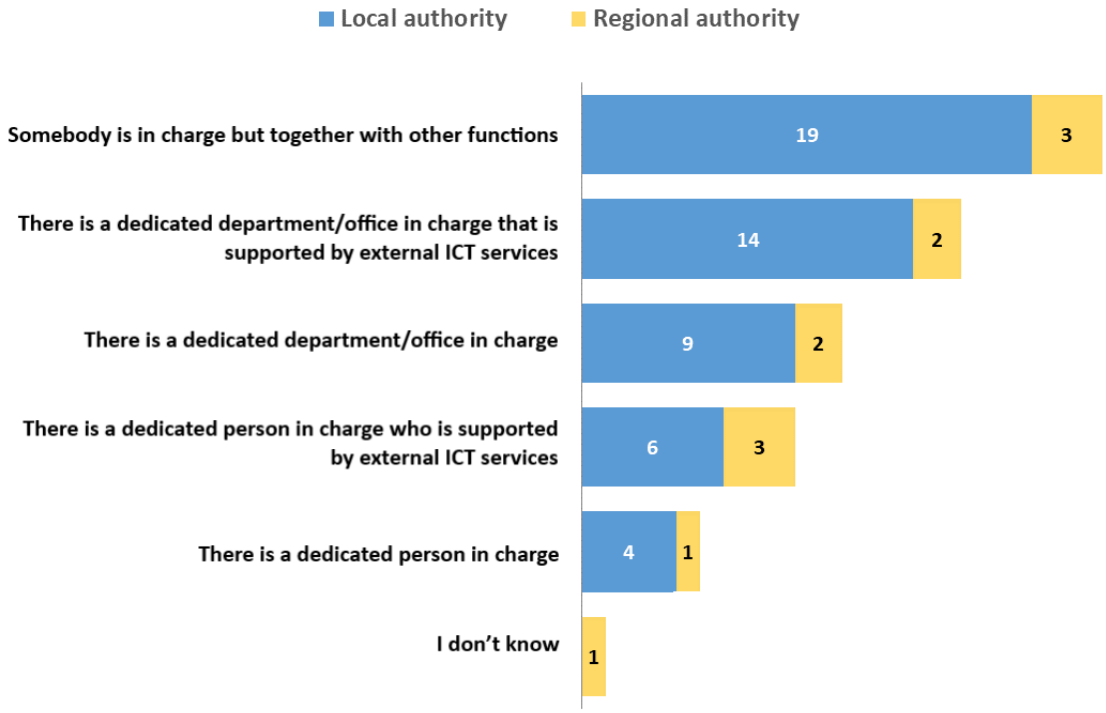
[4] Belgium (6), Bulgaria (2), Croatia (6), Czech Republic (2), Cyprus (1), Denmark (1), Estonia (2), Finland (1), France (4), Germany (4), Greece (3), Hungary (1), Italy (7), Ireland (3), Latvia (1), Poland (1), Portugal (2), Romania (2), Slovak Republic (2), Slovenia (1), Spain (7), Sweden (2), The Netherlands (3).

[5] Regions refer to NUTS1 and NUTS2 level; local authorities refer to NUTS3 and LAU level. In line with this criterion, two replies were re-classified with respect to what was indicated by the respondents.

[6] Authors' gross calculation.

internal responsibilities (Figure 5). In local authorities, the most common form of management for cybersecurity is hybrid, '*Somebody is in charge but together with other functions*' (37% of local authorities). However, a structured form of management where '*There is a dedicated department/office in charge that is supported by external ICT services*' is found in 27% of the local authorities. Across regional authorities, '*Somebody is in charge but together with other functions*' was the most selected option (25% of the respondents) together with '*There is a dedicated person in charge who is supported by external ICT services'* (25% of the respondents).

Figure 5. Cybersecurity management

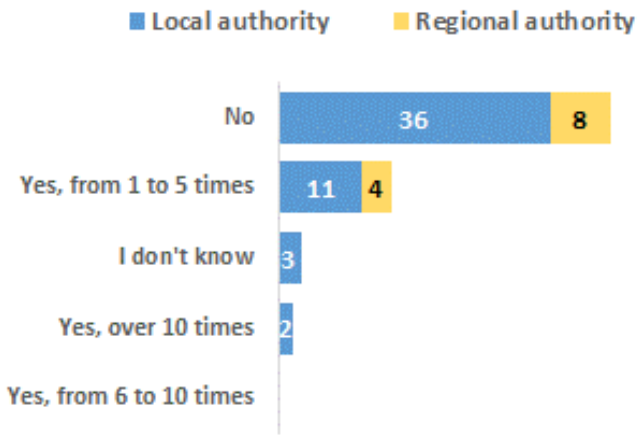


Source: online consultation.

When **analysing replies according to the size of the public authorities**, **it is found that local and regional authorities with more than 10,000 employees have a dedicated department/office in charge**. In fact, they rely primarily on the following two types of cybersecurity management: '*There is a dedicated department/office in charge that is supported by external ICT services*' (i.e., based on structural external support) and '*There is a dedicated department/office in charge*' (i.e., internally managed) (selected by 46% and 31% of the LRAs with over 10,000 employees, respectively). Among the LRAs with less than 100 employees, the most selected form of cybersecurity management is '*Somebody is in charge but together with other functions*' (selected by 78% of the LRAs with less than 100 employees). It is thus clear that **the size of the public authority influences the way cybersecurity management is organised**.

Section 2 of the questionnaire asked **about the authority's recent experience with cyber-attacks.** The majority of the participating authorities (69%) **did not** experience a cyber-attack with significant disruptive effect[7] in the last three years (i.e., from 2000 onwards) while a small share of them (3%) was attacked over ten times (Figure 6)[8].

Figure 6. Has your authority suffered from any cyber-attack having a significant disruptive effect?



Source: online consultation.

Section 3 of the questionnaire was a **self-assessment of the authority's digital resilience in the opinion of the respondent.** The respondent had to score the digital resilience of a **set of given aspects** (e.g., data access, public service provision) from 1 = not applicable/very low, to 10 = very high. The main points relating to the results presented in Figure 7 are:

- Regional authorities assess their digital resilience more positively than local authorities. In fact, given aspects are rarely scored below 5 by regional authorities – the 'below 5' area is shaded in the charts.
- The weakest aspects for both local and regional authorities relate to '*Personnel*', '*In-house ICT specialist staff*' and '*ICT services provided by third parties*' (i.e., shaded areas of these three aspects are the most 'populated' by dots).

[7] Within the NIS Directive (Directive (EU) 2016/1148), Art. 5 indicates the s*ignificant disruptive effects* of an incident on the provision of a service as one of the criteria (to be followed by the Member States) for the identification of operators of essential services. The essentiality of the services of these operators for the maintenance of critical societal and/or economic activities and the dependency of such services on network and information systems are the other two key aspects to be considered.

[8] More results from the consultation on suffered damage, actions taken after the cyber-attacks and perception of damage that may be caused in case of incident (from respondents replying 'No' and 'I don't know) are included in Part 3.

- The strongest aspects for both local and regional authorities relate to '*Digital infrastructure, equipment and tools*', '*Data access*' and 'P*ublic service provision*' (i.e., shaded areas of these three aspects are the least 'populated' by dots).
- Several local authorities have weak '*Decision-making processes*' with respect to digital resilience. For participating regional authorities, this aspect is, with one exception, assessed 6 or above.

The chart on the bottom-right of Figure 7 shows the average score across all the considered aspects, calculated for each respondent. The average may be considered to be an indicator of the self-assessment of overall digital resilience. All regions but one (i.e., 92% of the participating regions) assess their own overall resilience at least 6. This share is 83% for local authorities.

Figure 7. LRAs' self-assessment of digital resilience

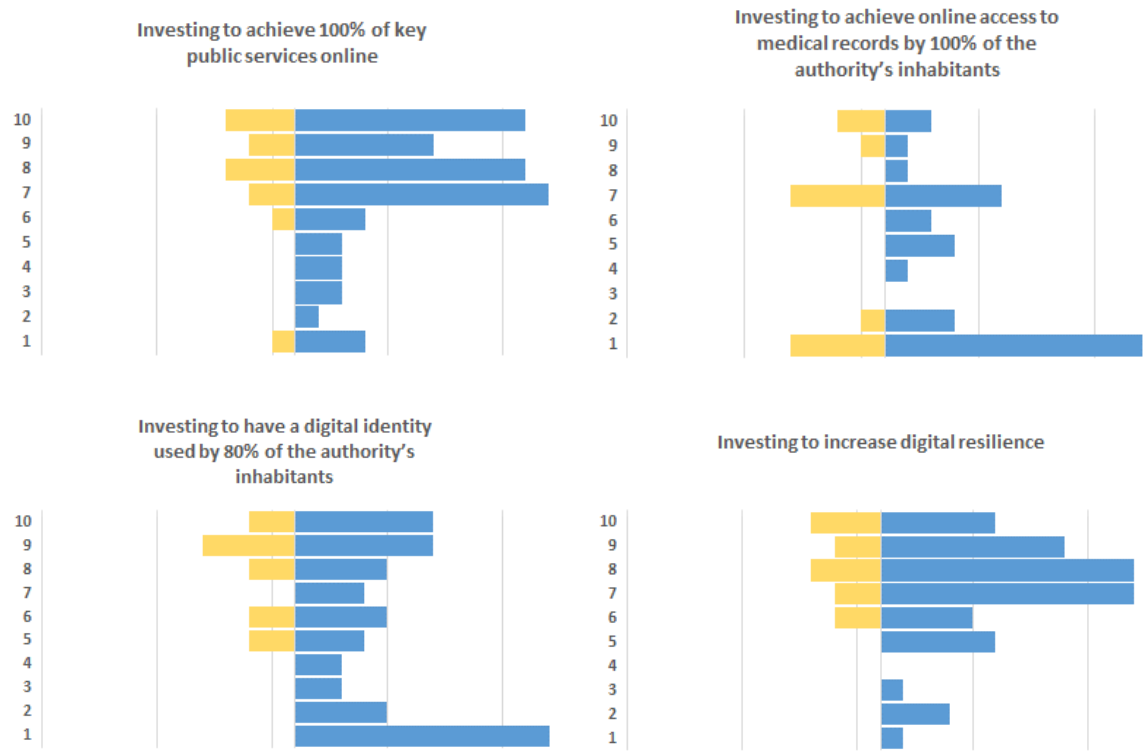
Note: local authorities are represented by blue dots; regional authorities by yellow dots.
Source: online consultation.

Finally, Section 4 of the questionnaire was about **solutions and funds used by local and regional authorities for enhancing their digital resilience**. The first question was intended to understand if priority was given to investments aimed at achieving the EU 2030 targets for the digitalisation of the public sector rather than at strengthening digital resilience. The four types of investments investigated

could be prioritised with scores ranging from 1 = not applicable/very low priority, to 10 = very high priority.

Replies demonstrate that **there is no 'competition' between the two sets of investments**, and that in general high priority is given to investments in digital resilience even if there are no binding requirements set at the EU level. In particular, Figure 8 indicates that digital resilience is as important as achieving 100% of public services online (i.e., one of the targets set by the Digital Decade) in terms of investment priority. Some 83% of the regional authorities score investment priority in digital resilience from 7 to 10 (i.e., from high to very high); the same score is given by 69% of the local authorities. Investing to achieve 100% of key public services online is prioritised with a score from 7 to 10 by 83% of regional authorities and 71% of local authorities.

Figure 8. Investments prioritised by public authorities



Note: the X-axis of each chart reports on the right (blue bars) the number of selections by local authorities, and on the left (yellow bars), the number of selections by regional authorities.
Source: online consultation.

Overall, there is **less interest** in investing to make medical records accessible online to all citizens and to have digital identity used by 80% of citizens, but this **may be explained** by the fact that some of the municipalities have **no**

responsibility in these areas and, accordingly, they rated these investments as not applicable or with low priority.

> **from the interviews** *In the experts' opinion, digital resilience is considered to be a relatively low priority by public administrations. Regional public authorities are considered to be slightly more aware than local authorities on the need to prioritise actions to reinforce digital resilience.*
>
> All experts were asked the following question: '*Based on your experience, nowadays is digital resilience considered a priority by local public authorities (e.g., cities)?'*. The range of responses was set from 1, meaning a very low priority, to 10, considered a very high priority. At an aggregated level, both the average (4.3) and median value (3) of the responses are low. This implies that, from the respondents´ perspective, digital resilience is considered to be a low priority for local public authorities. From the interviews, it was evident that cities are starting to realise the importance of digital resilience and that anyone can be a target of cyber-attacks. In addition, the presence of other priorities and challenges related to the scarcity of resources, both financial and human, contributed to the overall lack of prioritisation of actions related to digital resilience. When asked the same question with regard to regional authorities and given the same assessment framework of the previous question, the average value compiled from the answers is 5.7, while the median is 6. A higher degree of priority on digital resilience is expected from regional public authorities than from local authorities, despite it still not being considered an important priority on the scale. In this case, responses diverged significantly with very low or very high values, which also included a 10 (maximum score), implying digital resilience as one of the highest priorities. Despite acknowledging the heterogeneity between different EU local public authorities, several respondents commented that digital resilience should be further prioritised at both a local and regional level. One respondent also pointed out that priority is higher at an operational level than at the political level. Lastly, one respondent from the public sector highlighted that 'both local and regional authorities have understood the importance of resilience as a much broader category than cybersecurity', citing for example the Resilient Cities Network.

When it comes to the identification of **the main obstacle** to increasing digital resilience, results between local and regional authorities differ slightly (Figure 9). The question allowed the selection of only one reply and thus it is assumed that the most important factor was indicated by respondents. For both local and regional authorities **the lack of funding is the main obstacle to digital resilience**. However, for regional authorities, **the complexity of their organisational structure is as important as funding.** For local authorities, besides funding, other important obstacles are '*Lack of awareness at the top-management level*' and '*Lack of in-house technical know-how and experience*'. 'Other' was never selected. In addition, it is worth noting that seven local and two regional authorities replied that they are successfully pursuing their digital resilience. These authorities are from seven countries (Bulgaria, Italy, Latvia, France, Slovak Republic, Spain and The Netherlands) and have varying sizes from a minimum of 101-500 staff to a maximum of over 10,000 staff.

Figure 9. The main obstacle to increasing digital resilience

Source: online consultation.

❝ **from the interviews**❞ *In the experts' opinion, the lack of financial and human resources are the main obstacles faced by European LRAs to increasing their digital resilience.*

Experts were asked about the main obstacle faced by European LRAs to enhancing their digital resilience. The question was left open-ended, but recurring replies were received, namely: budget and skills (seven selections each); political will, cultural factors, organisational capacity and digital tools (two selections each); bureaucracy (one selection). We can thus see that the main obstacles identified through the interviews are the lack of financial and human resources. Budget represents the first challenge to initiating any policy action to build digital resilience and some of the experts emphasised that, even in cases where there are enough resources, LRAs lack the organisational capacity to use them efficiently. In the experts' opinion, LRAs often need to address conflicting priorities with scarce resources and decide not to prioritise, for instance, investments in cybersecurity programmes even after having upgraded their digital infrastructure. With the same number of mentions, the lack of digital and ICT skills in the public administrations remains a key challenge. The skills gap and shortage have been well documented and several respondents agree that, without digitally trained personnel, or ICT experts, LRAs will not be able to build digital resilience or to ensure the adequate implementation of innovative technologies, even having recognised their potential.

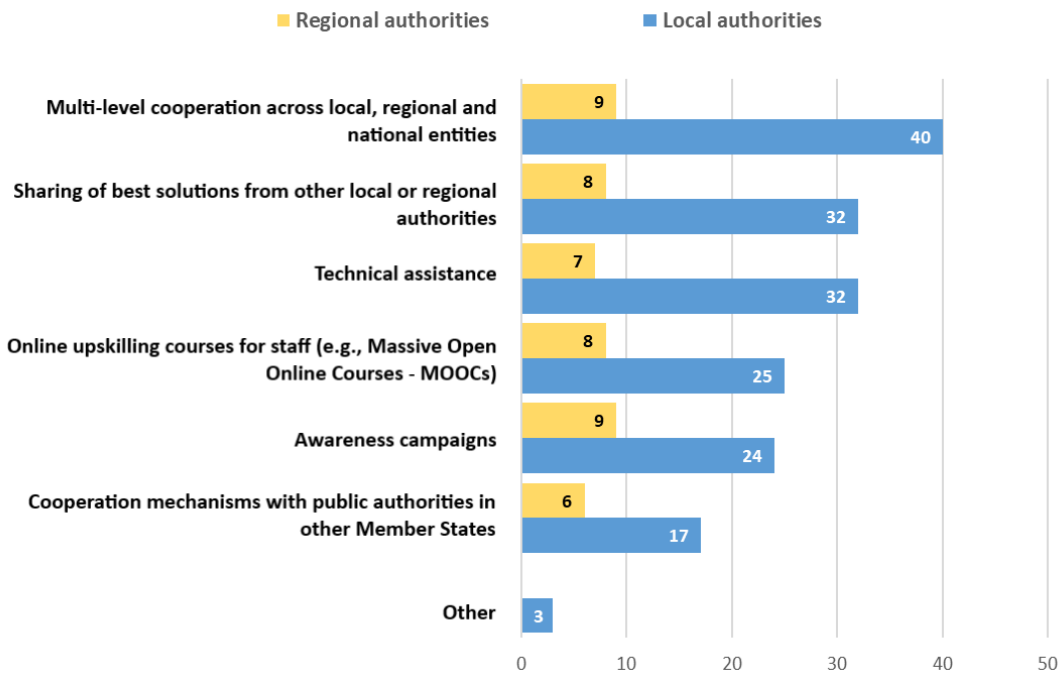
Among other obstacles, the experts identified the lack of political will, limiting cultural factors, lack of organisational capacity and lack of capacity to procure digital goods and services. Some of these challenges remain related to LRAs' resistance to change and to a

subset of citizens, especially the elderly. The need to allocate resources to build digital resilience is still not considered to be a high priority and therefore it lacks the political or cultural motives to prompt changes in the public administration. Lastly, two industry experts highlighted the difficulty for LRAs of procuring goods and services for digital resilience, due to the bureaucratic complexity of the procedures and to the need to find a balance between employing local companies, ensuring quality and maintaining the flexibility of services, especially when procuring off-the-shelf digital solutions from the bigger providers.

When asked if there were differences between the local and the regional level in terms of obstacles to be addressed for pursuing digital resilience, almost all respondents pointed out that regional administrations were in a better position than local authorities. Indeed, the obstacles previously identified are perceived as a greater burden on local authorities that have access to scarcer funding and skilled personnel. For instance, large cities have different challenges due to their urban environment and specific pressures such as immigration or security while smaller municipalities have problems in terms of lack of critical mass and of capacity to address bigger challenges.

In terms of **external support that would help to enhance their digital resilience,** '*Multi-level cooperation across local, regional and national entities*' is the most selected option by local authorities; it is followed by '*Technical assistance*' and '*Sharing of best solutions from other local or regional authorities*' (Figure 10). Regional authorities do not show a specific preference, but '*Awareness campaigns*' and '*Multi-level cooperation across local, regional and national entities*' were selected the most. Few local authorities reiterated under the 'Other' option the need for financial support and subsidies.

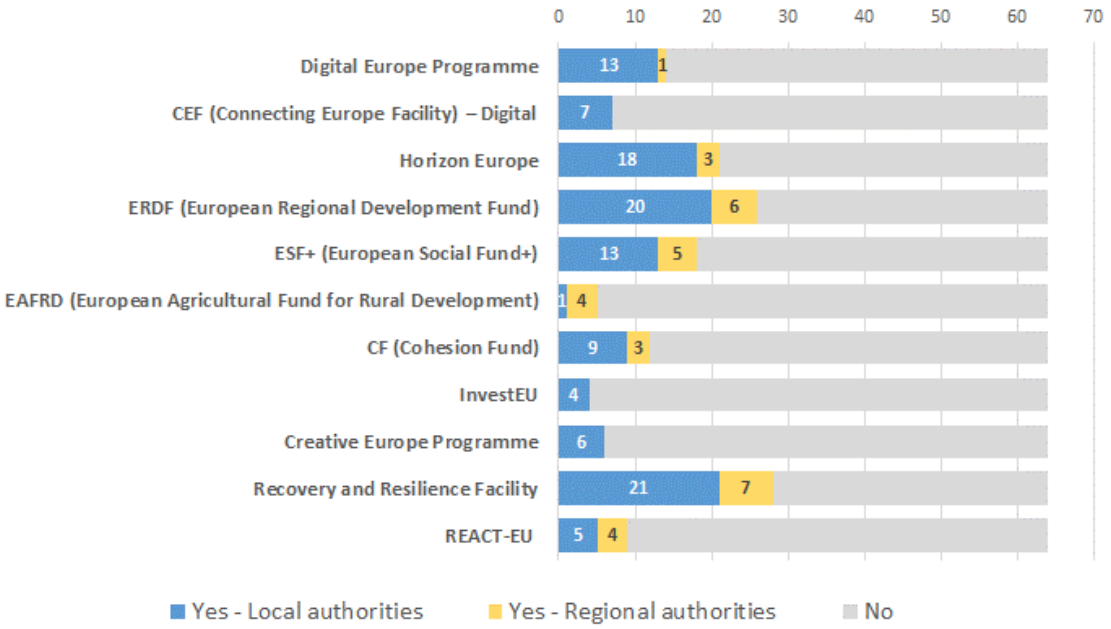
Figure 10. Type of external support needed in order to enhance digital resilience



Source: online consultation.

The results of the consultation **highlight difficulties in accessing EU funds with the scope of enhancing digital resilience.** Public authorities were asked if they were accessing a number of EU funds (Yes/No) (Figure 11).

Figure 11. Access to EU funds with the scope of enhancing digital resilience



Source: online consultation.

The **Recovery and Resilience Facility** is the most important funding source; it is accessed by 44% of the participating authorities. The second most used source is the **European Regional Development Fund** (accessed by 41% of the authorities), followed by **Horizon Europe** (accessed by 33% of the authorities). Overall, all listed sources were selected to a certain extent, indicating that **a variety of European funds is being used** by LRAs. Local authorities access a wider range of funding sources than regional authorities for enhancing their digital resilience. Example of these sources are the Connecting Europe Facility – Digital, InvestEU and the Creative Europe Programme.

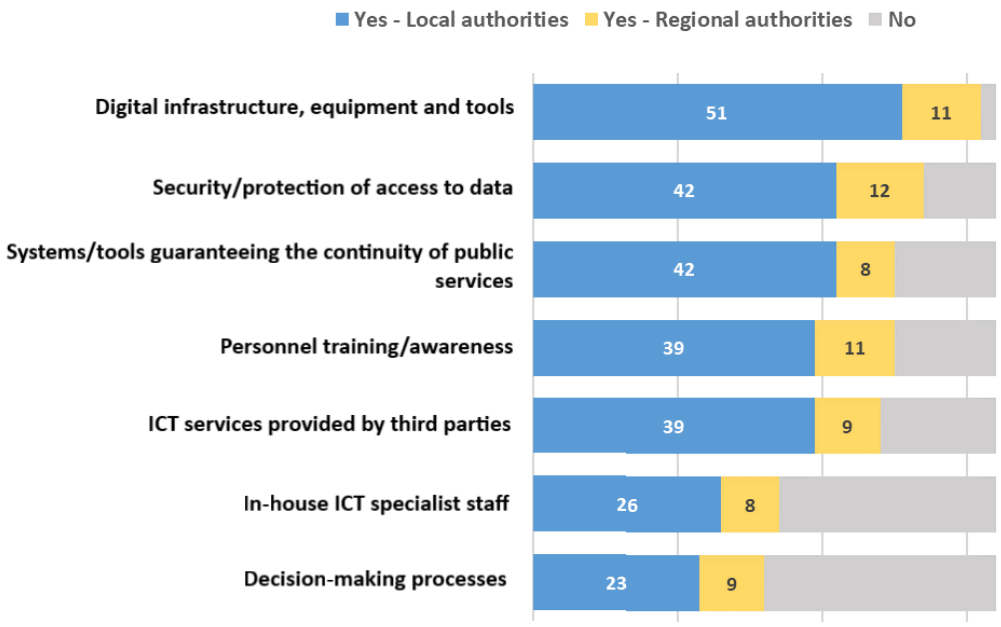
Apart from the frequency of the selections, the **analysis of selection distribution indicates that 40% of the participating local authorities do not access any EU funding source** (i.e., they replied 'No' to all listed EU funds). Among regional authorities, there are two regions, out of twelve, that indicate they do not access any of the listed EU funds.

❞ **from the interviews**👀 *In the experts' opinion, the best approach to funding for LRAs is the reliance on at least two different funding sources.*

Although one digital solution provider expert highlights that some small administrations might be left behind due to difficulties in effectively managing EU funds and projects, most of the experts from all the interviewed categories (including decision-makers, private sector and academia representatives) indicated that at least two different funding sources would be suitable to invest in digital resilience. It is then expected that EU funds are coupled with other available funds (local, regional, national, private or other), and that regional funds coupled with the EU funds is the most recurrent choice. Some experts even clarified that a 'mixed' approach should be taken and that it is not a matter of one or another fund but 'mixed funds' represent the best approach, where different EU funding schemes can be coupled with, for instance, private funds. Finally, a public sector expert also noted that the choice of funds will depend on the type of authority (e.g., their size, capacity, experience with different funds). This opinion was supported by another think tank/academic sector expert who referred to German LRAs, where regional and national funds are more suitable due to the structural peculiarities of the federal system.

Public authorities were then asked if they have plans to invest in areas related to digital resilience in 2023 and 2024 (Yes/No). **Almost all (97%) local and regional authorities are planning to invest in digital infrastructure, equipment and tools** (Figure 12). About 84% of LRAs participating in the consultation are planning to invest in '*Security/protection of access to data*'; this area is followed by '*Systems/tools guaranteeing the continuity of public services*' (78%), '*Personnel training/awareness*' (78%) and '*ICT services provided by third parties*' (75%).

Figure 12. Plans for 2023-2024 investment in areas which are relevant for digital resilience

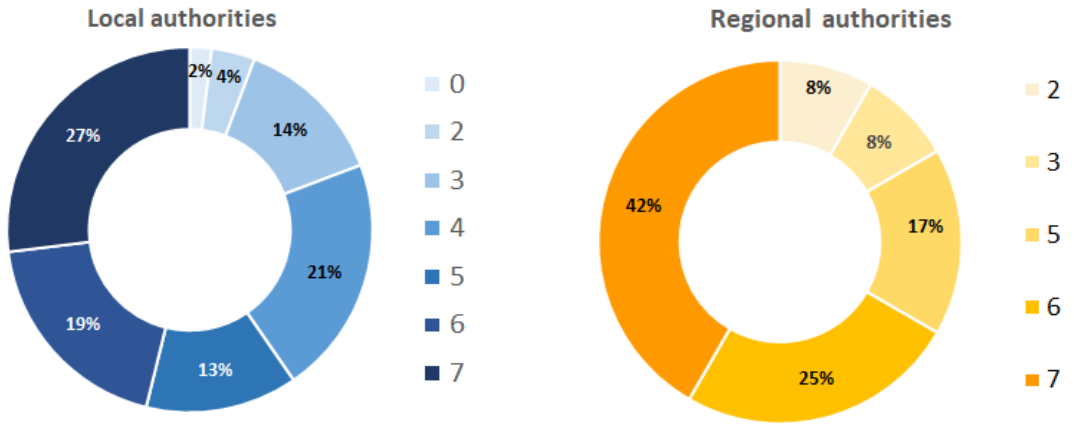


Source: online consultation.

All regions are planning to invest in security/protection of access to data and all but one plan to invest in personnel training/awareness and digital infrastructure, equipment and tools. Investments in decision-making processes are more popular among regions than among local authorities. A couple of local authorities selected 'Other' to indicate their plan to invest in GovTech[9], 5G, IoT and secure messaging tools to communicate with other authorities, companies and individuals.

The analysis of selection distribution indicates that only one small-sized local authority is not planning to invest in any of the listed areas (i.e., it replied 'No' to all investment areas). Figure 13 indicates the share of local and regional authorities per number of selected investment areas.

Figure 13. Frequency class of investment areas, % of public authorities



Source: online consultation.

It can be seen that 27% of local and 42% of regional authorities are planning to invest in seven of the areas listed in Figure 12; 19% of local and 25% of regional authorities are planning to invest in six areas; and 13% of local and 17% of regional authorities are planning to invest in five areas.

from the interviews *In the experts' opinion, upskilling and training should be the main priority investment areas.*

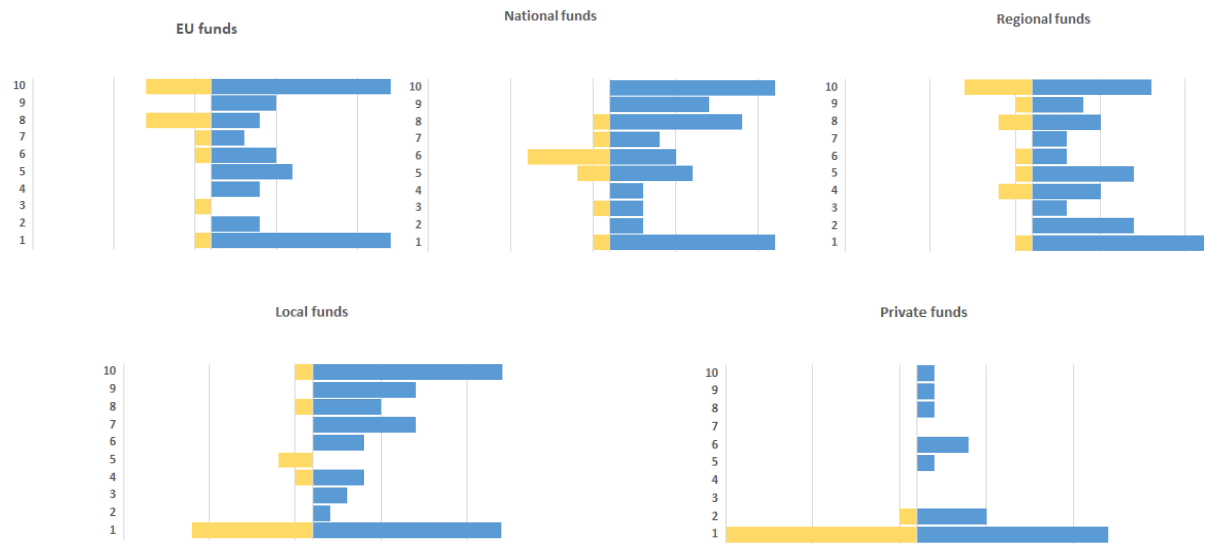
The interviewed experts also see the need to invest in most of the areas indicated by the respondents in the survey. All of the options, except for the one on the decision-making processes, were chosen by the experts when asked which actions LRAs should prioritise to

[9] A whole of government approach to public sector modernisation (World Bank website accessed in March 2023).

enhance their digital resilience. However, most of the experts, from all three interviewed categories, suggested that skills and training should be the main priority for LRAs, by choosing 'Upskilling personnel' and 'Strengthening ICT specialist staff' as the key actions needed. A representative from the public sector noted that the skills of any staff working with digital infrastructures, and not only of the ICT specialists, should be the priority. Additional suggestions of activities to be taken to improve digital resilience also include changes in the organisational culture, definition of the clear requirements for public procurement and prioritisation of a strategic plan for digital resilience, which should be embedded in a wider policy framework of the specific public authority.

In order to invest in the above areas, LRAs were asked to indicate the most likely funding sources, the choice being between EU, national, regional, local and private sources. Respondents could score the likely use of a source from 1 = not likely, to 10 = very likely. Results show that for regional authorities the most likely sources of funding are EU and regional funds (Figure 14).

Figure 14. Likeliness of funding sources for investing in digital resilience



Note: the X-axis of each chart reports: on the right (blue bars) the number of selections by local authorities; on the left (yellow bars), the number of selections by regional authorities.
Source: online consultation.

National funds are the most likely source of funding for local authorities. However, local authorities also frequently select as 'likely' the use of EU and regional funds. With few exceptions among local authorities, the use of private funds is not likely for the majority of the participating public authorities. Few local authorities reiterate in their comments (i.e., the 'Other' reply) the use of their own local budget for investments in areas which are relevant for digital resilience. One local authority considers fairly likely the use of InvestEU and of the European Energy Efficiency Fund.

1.2 Measures financed from programmes under cohesion policy

Despite the fact that funding is considered by LRAs to be the main obstacle for enhancing their digital resilience, relevant support is currently being channelled from the EU long-term budget (i.e., the MMF 2021-2027) and the recovery instrument Next Generation EU - through the Recovery and Resilience Facility (RRF). The diverse EU sources available and accessible by European LRAs are also evidenced by the results of the online consultation.

Funding programmes available under the Cohesion policy are presented in this Section 1.2. Section 1.3 focuses on funding opportunities other than those under the cohesion policy. Finally, referring to the presentation of the RRF in the 'Introduction' of this study, Section 1.4 provides examples of concrete investments made for the benefit of LRAs and falling in the framework of the NRRPs.

There are four funds available for Member States and regions under the EU Cohesion policy: the European Regional Development Fund (ERDF), the Cohesion Fund (CF), the European Social Fund+ (ESF+) and the Just Transition Fund (JTF). Investments from these funds are specified in national, and sometimes regional, programmes. In addition, LRAs benefit from the European territorial cooperation initiative (Interreg) that is supported by the ERDF and external financing instruments.

The information provided hereafter refers to the provisions made for these funds in the respective Regulations and not to the measures actually included in EU countries' national and regional programmes. However, examples of the use of Cohesion policy funds may be found elsewhere in the report, especially in Part 2.

The ERDF supports the economic, social and territorial cohesion of the Union. Its aim is to reduce imbalances among regions. According to the consultation, 41% of the participating LRAs are using this fund to enhance their digital resilience. In the new programming period, the ERDF is the fund with the most explicit reference to measures that are relevant for enhancing the digital resilience of public authorities. One of its priorities in the current programming period is to make Europe and its regions '*More competitive and smarter, through innovation and support to small and medium-sized businesses, as well as digitisation and digital connectivity*' (ERDF webpage accessed in March 2023). Under this priority, one on the specific objectives reads '*Reaping the benefits of digitisation for citizens, companies, research organisations and public authorities*' and a

corresponding output is '*Public institutions supported to develop digital services, products and processes*' (Regulation (EU) 2021/1058). The ERDF is also intended to support '*networking, cooperation, exchange of experience and activities involving innovation clusters including between businesses, research organisations and public authorities*' and '*investment in infrastructure*' and '*technical assistance*' (Regulation (EU) 2021/1058), all of which may be relevant for LRAs to pursue their digital resilience. Another relevant area that may be funded under the ERDF is the development of skills for smart specialisation, including the preparation or updating of smart specialisation strategies. The fund is also suitable for enhancing digital connectivity (see the CF below).

The ESF+ is used by 28% of the LRAs participating in the consultation with the scope to enhance their digital resilience. One of the objectives of the ESF+ is '*promoting lifelong learning, in particular flexible upskilling and reskilling opportunities for all taking into account entrepreneurial and digital skills, better anticipating change and new skills requirements based on labour market needs, facilitating career transitions and promoting professional mobility*' (Regulation (EU) 2021/1057). This objective could potentially cover training addressing civil servants in digital areas. In addition, the EaSI strand of the fund, that is for the most part managed by the EC, supports analytical initiatives such as studies, communication and dissemination activities, and exchange of practices. For this strand, funds are allocated according to calls for projects or through tenders to award service and/or supply contracts.

The CF is used by 19% of the LRAs participating in the consultation with the goal of enhancing their digital resilience. The CF only concerns Bulgaria, Czech Republic, Estonia, Greece, Croatia, Cyprus, Latvia, Lithuania, Hungary, Malta, Poland, Portugal, Romania, Slovakia and Slovenia. In the current programming period, it is specified that *'... based on the experience of previous programming periods, the ERDF and the Cohesion Fund should also support investments in enterprises other than SMEs, including in particular utilities, when they concern investment in infrastructure that ensures access to services available to the public in the field of energy, environment and biodiversity, transport and digital connectivity*' (Regulation (EU) 2021/1058).

According to the Regulation establishing the JTF, the fund '*shall contribute to the single specific objective of enabling regions and people to address the social, employment, economic and environmental impacts of the transition towards the Union's 2030 targets for energy and climate and a climate-neutral economy of the Union by 2050, based on the Paris Agreement*' (Regulation (EU) 2021/1056). If this specific objective is met, the following relevant activities are eligible: '*investments in digitalisation, digital innovation and digital connectivity*'

stemming, among other outputs, in '*new and upgraded public digital services, products and processes*' (Regulation (EU) 2021/1056).

Finally, the European Territorial Co-operation (Interreg) is organised in different strands, depending on the type of collaboration among different regions: cross-border collaboration (Interreg A), transnational collaboration (Interreg B), interregional collaboration (Interreg C) and outermost regions' cooperation (Interreg D). In the 2021-2027 programming period, Interreg has two new specific objectives, one of which is very relevant for LRAs, including with regard to the enhancement of their digital resilience: 'A better Cooperation governance'. Under this objective, funding is intended for enhancing the institutional capacity of public administrations (Regulation (EU) 2021/1059).

1.3 Existing funding opportunities other than those under the cohesion policy

Below is reported an overview of the EU funding programmes/instruments that have a focus on the digital domain and on which LRAs can rely for improving their digital resilience. Notably, programmes that have a digital focus, but do not provide opportunities for LRAs to improve their digital resilience, are not included. For each source, the modalities through which funds can be accessed and examples of uses are specified.

The Connecting Europe Facility (CEF)-Digital. CEF supports the development of high performing, sustainable and efficiently interconnected trans-European networks in the fields of transport, energy and digital services. For the purpose of this study, the facility's digital priority 'CEF-Digital' is of main interest as it contributes to the deployment of safe, secure and sustainable high-performance infrastructure, including Gigabit and 5G networks, with a specific focus on local and regional infrastructures (EC, 2021a). Participation by LRAs: legal entities established in the EU are eligible to apply for funds (Regulation (EU) 2021/1153), but public administrations are specifically targeted through CEF Digital's '5G for Smart Communities' priority, and it is here that the main opportunities for LRAs arise. LRAs can access these funds by participating in the single-stage calls for proposals published by the EC (participation usually requires the formation of a consortium with other entities). Use by LRAs: funds can be used for upgrades/improvements of digital infrastructure, especially when it comes to 5G-based systems.

The Digital Europe Programme (DEP). This is a new EU funding programme focused on bringing digital technology to businesses, citizens and public administrations. As such, it targets public administrations at all levels (local, regional and national) as well as their cross-border collaboration. The DEP

provides strategic funding in five key capacity areas: supercomputing, AI, cybersecurity, advanced digital skills and wide use of digital technologies across the economy and society, especially through the network of Digital Innovation Hubs (DIHs). Participation by LRAs: legal entities established in the EU are eligible to participate and public administrations are one of the three key stakeholders (EC, 2021b). In some of the calls, LRAs are specifically targeted. LRAs can explore open calls for proposals on the EC's Funding & Tender Opportunities platform (most of the calls require the formation of a consortium with other categories of stakeholders). Use by LRAs: potential uses include: improvements of digital systems and infrastructures, in particular focusing on cloud-to-edge technology, AI and blockchain; adoption of, or improvement of, data-driven services within the LRAs or their public enterprises/agencies in relation to Data Spaces development, data sharing, etc.; and digitalisation of services provided by LRAs, especially when it comes to managing citizens' digital identity, personal data and services using such data. Support is also available in other forms such as for the use and adoption of various digital tools/services or as training for advanced digital skills provided by the regional DIH within the EDIHs Network; through the 'Advancing the digital transformation of smart communities' action to develop strategic plans for LRAs' digital resilience and to improve digital infrastructures; and in the procurement of digital solutions through the European marketplaces where validated and compliant resources (e.g., tools, services) are available for LRAs.

Horizon Europe (HE). This is the EU's key funding programme for research and innovation. It facilitates collaboration and strengthens the impact of research and innovation in developing, supporting and implementing EU policies while tackling global challenges. It has a specific focus on digital through the 'Digital, Industry and Space' cluster within its second pillar on 'Global Challenges and European Industrial Competitiveness' and through the 'EU missions' that are meant to support the achievement of EU priorities such as 'Europe fit for the digital age'. Security and resilience aspects are the target of actions in the 'Civil security for society' cluster within its second pillar. In addition, within the Innovative Europe pillar, calls under the European Innovation Ecosystem Work Programme are the most relevant to LRAs, for instance, for capacity building and stimulation of innovation procurement. Participation by LRAs: in principle, it is open to all legal entities, however calls can be restricted to specific categories, so eligibility for LRAs has to be checked for each individual call. In some cases, pre-selection is made through calls for expression of interest. Use by LRAs: LRAs are mostly targeted as the end-users who can serve as demonstrators (demonstration sites) for new innovative technologies. Calls for action usually focus on the services provided by LRAs to citizens or by their public entities/agencies rather than on the authorities' internal digital systems and infrastructures. As such, LRAs can use HE funds to implement pilot projects for the testing and adoption of new

technologies within the programme's priority areas, namely: data and computing technologies, spatial data usage in public service provision and decision-making at LRAs' level. A successful example of using Horizon 2020 (i.e., the predecessor of Horizon Europe over the period 2014-2020) is provided among the case studies in Part 2.

The InvestEU Fund. This is an umbrella scheme for 13 different financial instruments (previously managed separately) expected to stimulate more than €372 billion in public and private investment. It supports financing and investment operations across four EU policy priorities: sustainable infrastructure; research, innovation and digitalisation; SMEs; and social investment and skills. Participation by LRAs: public sector entities (territorial or not) and public-sector type entities are eligible to apply. Use by LRAs: under the research, innovation and digitalisation or social investment and skills priorities, LRAs may fund the uptake of new digital tools/solutions coming from the latest research and innovation activities in their area; the uptake of AI solutions that might be needed to strengthen resilience; and staff training and upskilling.

1.4 Examples of NRRPs' actions involving LRAs and of their actual implementation

Referring to the overview of selected plans provided in the 'Introduction', below are included examples, from a selection of countries, of actual implementation of investments supporting digital resilience. Most of the examples relate to LRAs.

The Czech Republic and Germany provide examples of actual implementation of investments related to the first component of digital resilience, i.e., enforcement of legislation.

- **Czech Republic**

In the 2021-2025 Action Plan for the National Cybersecurity Strategy there is evidence of follow ups to the Act on Cyber Security for which the country made an allocation of €106 million in its NRRP. The Action Plan reflects a comprehensive approach to information security and cybersecurity management. The listed tasks address strategic communication, secure infrastructure, development of capabilities, response and prevention, research and development as well as updates of the regulatory framework. Among the tasks directly addressing public authorities are the search for faults and vulnerabilities in their information systems and networks, the design, organisation and implementation of technical, non-technical and combined cybersecurity exercises and the training in cybersecurity of public administration employees (Government of the Czech Republic, 2021).

- **Germany**

The German Online Access Act came into force in 2017. The law provided for the digital offer of 575 administrative services by the federal, state and local governments by the end of 2022. Beside the digitalisation of the services, the portals of the public administrations were also to be networked (OZG webpage). The Act also implements Regulation (EU) 2018/1724 '*establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services'*. The Act's implementation proved to be more complex than expected and at the end of 2022 the target had not been achieved (d.velop news dated 14/12/22). The €3 billion allocated from the NRRP are distributed to regions and in particular to the 11,000 municipalities that are the ones concretely developing digital services according to OZG service standards (inter alia, highly user-friendly).

With regard to the second component of digital resilience, i.e., infrastructures, concrete examples of investments are from Portugal and Bulgaria.

- **Portugal**

The Regional Government of the Azores is supported by the NRRP in the modernisation and digitalisation of its public administration. Among the measures taken is the 'Azores_Ciber360º project' that provides the public administration with suitable digital infrastructure supporting the operation of a Computer Security Incident Response Team in an integrated manner. In August 2022, the regional government launched a public tender valued €1.66 million for the supply, installation and support of the Azores Cyber 360º platform (Government of the Azores website).

- **Bulgaria**

In August 2022, the Bulgarian government launched a public tender for the construction, development and optimisation of the TETRA digital system and radio relay network. The system is a professional mobile radio and supports voice and data communication by government agencies and structures responsible for crisis, accident and disaster management as well as national security issues (BTA news dated 19/08/22). The contract was awarded to the tune of some €55 million (SeeNews press release dated 7/10/22).

France and Italy provide examples of actual implementation of investments related to the third component of digital resilience, i.e., the human factor. The French example is a diagnostic investment while the Italian example relates to the granting of funds to LRAs for cybersecurity projects.

- **France**

In 2021, framed by its NRRP, the French government carried out a study to understand the cybersecurity situation of municipalities with less than 3,500 inhabitants. These 31,816 small municipalities represent 91% of all municipalities in the country. The study was grounded on the evidence that local authorities are increasingly targeted by cyber-attacks. The study's findings will be used to tailor the NRRP's component on the cybersecurity of local authorities to actual needs (Cybermalveillance.gouv.fr webpage accessed in March 2023)[10].

- **Italy**

In October 2022, the Italian government launched a call for projects aimed to strengthen the cyber resilience of the public administration at the subnational level. The call had an allocation of €45 million made available under the NRRP's Measure 1 (digitalisation of the public administration), Component 1 (digitalisation, innovation and security in the public administration), Investment 1.5 'Cybersecurity'. The call funded 51 projects within the given total budget. All Italian regional authorities (including the two autonomous Provinces) had at least one project approved, nine Regions had two projects approved. Additional 20 approved projects were proposed by 13 cities (ACN, 2023).

from the interviews *The expert from Innova Puglia provided details on the two regional projects approved under the Italian government's call related to 'cyber resilience'.*

The first project (valued at almost €1 million – ed.) relates to an assessment of the cyber posture, i.e., the state of security, of the Region, the health authorities, the regional agencies and in-house companies. The second project (also valued at almost €1 million – ed.) aims at strengthening the cybersecurity system of the Region in terms of staff training. It addresses a total of some 38,000 people from the Region, local health authorities, regional agencies and two in-house regional companies.

[10] The main findings of the study are: the majority (77%) of these local authorities have less than five computers; the same share (77%) outsource their IT management; 65% believe that cyberthreats are low, non-existent or not assessable; risky practices such as sharing passwords and using personal devices (i.e., telephone, emails, computers) in a professional setting are common.

Part 2. Case studies

This part includes eight case studies, developed to complement the state of play of LRAs' digital resilience as presented in Part 1. Highlights from the cases are used in Part 4 to draw conclusions and recommend actions.

2.1 Encompassing digital resilience into overall resilience. The progressive approach of the Municipality of The Hague, The Netherlands

The Municipality of The Hague started its digital resilience journey in 2007. Nowadays, the Municipality continues to prioritise investments in the field of information security while developing a more comprehensive resilience to a variety of external threats.

Background. The international environment to which The Hague is exposed almost certainly contributed to making the Municipality of The Hague aware early on of its vulnerability in the digital domain. The Municipality identifies two main steps it took to tackle digital resilience. The first step was to become aware of its attack surface. As it was lacking the internal knowledge to do so, the Municipality decided since the very beginning to rely on the services of an external provider. The second key step was the selection of this provider with whom to build a long-lasting cooperation.

Solutions and funds used for digital resilience. The Municipality's approach to digital resilience was gradual. After making an inventory of the municipal assets (e.g., websites, domains and servers) that could be attacked (i.e., of the 'attack surface' or 'digital footprint'), vulnerabilities and risks were defined and then progressively resolved. Because of the high number of assets and suppliers falling within the ecosystem of the Municipality, priorities in the resolving sequence had to be set. The Municipality prioritised vulnerabilities taking into account the potential impact on the availability and continuity of its own systems and services. In 2017, having completed this internal review process, the Municipality started organising annual hackathons called 'Hâck The Hague' where 'ethical hackers' were invited to hack the Municipality's system and ecosystem, including of its suppliers. In 2022, the event was attended by 200 hackers from 23 countries. Hackathons are considered to be an external review of the city's systems' security level and are used to detect vulnerabilities and improve resilience (Municipality of The Hague & Cybersprint, 2021).

Resolving risks also implies changing internal organisation and defining the measures to be taken by each employee to limit risk (Municipality of The Hague

& Cybersprint, 2021). To this end, the Municipality continued to invest in awareness-raising of its staff (e.g., by developing a privacy game) and arranged for there to be an information security officer in each of its five main departments. These officers report to a Chief Information Security Officer (CISO) who has an advisory role at the strategic level (Municipality of The Hague, 2018?).

In 2019, the Municipality made a step forward and, with its Resilience Strategy, included digital resilience into a broader resilience approach towards a variety of shocks, from cyber-attacks to extreme weather, civil unrest, pandemics, extremist acts and disruption of critical services. Since 2016, this comprehensive approach to resilience has been grounded in the Municipality's participation in the '100 Resilient Cities network'.

Generally speaking, in terms of funding, Dutch municipalities depend on national government support and this is indicated as the main funding source for information security in the Municipality. Also, in the past, information security did not have a centralised budget and capacity was developed within the various municipal departments. It is only in recent years that information security expertise has been centralised and budgeting from the various departments has been merged within the directorate of operations[11].

Highlights.

- In 2021, the Municipality of the Hague published an e-guide 'How to hack a city' where its experience is described. It is a 'must have' document for public administrators interested in initiating a path of digital resilience.
- The Municipality highlights how its digital resilience is necessary to avoid both economic and reputational impacts, i.e., undermining citizens' trust.
- Reorganisation of roles within the public authority (with the presence of information security officers in each department) is as important as the advisory contribution by the CISO at strategic level.
- The Municipality of the Hague cooperates a lot with private companies and knowledge institutes, such as universities and the Security Delta. The latter is the Dutch security cluster in which 275 organisations work together to exchange knowledge and cooperate nationally and internationally[12].
- Besides the support received for the preparation of the strategy, the Municipality's participation in the '100 Resilient Cities network' provides the following benefits: receiving funding for a Chief Resilience Officer; accessing a global network of providers of resilience services and knowledge; and smoothly cooperating with the network's cities on the basis

[11] Information provided by the Municipality's Chief Information Security Officer on 26/02/23.
[12] Ibid.

of a shared use of the City Resilience Framework (Municipality of The Hague, 2019).

2.2 A Security Operations Centre to enhance the digital resilience of the capital city of Berlin, Germany

The capital city of Berlin faces 15 million cyber-attacks per year. The increasing frequency of these attacks prompted the authorities of Berlin to establish a Security Operations Centre with dedicated resources and staff.

Background. ITDZ-Berlin is the municipal IT company of Berlin. It is a subordinate institution to the Senate of Berlin, the executive body governing the country's capital, Berlin, which is both a city and a federal state. Berlin is home to Germany's biggest municipal interconnected network with 1,100 kilometres of cables and tens of thousands of computers and phones. This network includes the State authorities of Berlin, the police, the fire brigade and the Courts (Balgaranov, 2022). There are '*15 million registered digital attack attempts per year on Berlin authorities. More than 530,000 spam emails are detected every month, flooding and paralysing systems, as well as 3,000 e-mails containing harmful computer viruses',* and *'a lot of these attacks aim at data theft or extortion*' while '*their frequency is increasing*' (Balgaranov, 2022).

Solutions and funds used for digital resilience. Berlin's digital path began in 1991. The reunification of Germany prompted the merge of Berlin's State Office for Electronic Data Processing with its Eastern counterpart, creating the Berlin State Office for Information Technology (LIT). In the 1990s, the focus of the Berlin administration was on decentralisation. This means that each department was responsible for its own IT operations (ITDZ-Berlin, 2021). However, the rapid advancements in digital technologies and the quality of requirements prompted the authorities to opt for a centralised option. This shift along with the 2016 Berlin's eGovernment Law, established ITDZ-Berlin as the municipal IT solutions provider (ITDZ-Berlin, 2021). The aim of the eGovernment Law was to provide user-friendly and secure eGovernment services to the citizens of Berlin and ensure that the authorities have efficient, secure and standardised IT equipment. ITDZ-Berlin currently employs over 1,000 staff.

In April 2022, due to the increasing number of cyberthreats targeting, in particular, citizens' personal data, the authorities of Berlin opened a security centre (the 'Security Operations Centre' - SOC) as part of ITDZ-Berlin. In the SOC, cyber-attacks are detected and defended around the clock (ITDZ-Berlin's webpage accessed in February 2022). The experts of the SOC collect and analyse 1,000 gigabytes of data daily from various systems such as firewalls, routers,

servers and network components. In the event of a cyber-attack, a standardised process applies, as agreed internationally and certified by the Federal authorities. The cost for the establishment of the SOC is reported to be €750,000 (Abgeordnetenhaus Berlin, 2022). Marc Böttcher, CEO of the ITDZ Berlin stated that '*the dangers of hacker attacks, malware and security gaps have been increasing for years. Our experience shows that IT security needs to be actively managed, continuously adjusted and professionally implemented. In the SOC we bundle expertise, the latest technology and organization. This makes it possible to standardize the topic of IT security for the authorities and institutions of the Berlin administration at a high level.'* (The Governing Mayor press release dated 13/04/22).

Furthermore, ITDZ-Berlin operates two data centres, one of which is for high-security data and is located in an underground bunker. Its information security management system '*and the entire technical and structural infrastructure of all office buildings*' are certified according to the ISO 27001 standards; it provides a private cloud for the Berlin administration; it established a Computer Emergency Response Team (CERT) that works proactively, checking the infrastructure of the administration's departments for vulnerabilities; and it regularly trains its in-house staff and raises awareness on the issues of security and data (ITDZ-Berlin webpage accessed in February 2023). Finally, for over 20 years ITDZ-Berlin has been an education provider of study programmes and apprenticeship positions, retaining among its staff some 70% of those qualified. ITDZ-Berlin has qualified 148 young people as IT specialists in the digitalisation of administration and, in 2020, had 73 people in training and studying (ITDZ-Berlin webpage accessed in February 2023).

Highlights.

- The Berlin administration undertook a centralisation process of its information security management. It built its digital resilience in-house and continually updates and enhances its various aspects in light of changing quality requirements and technological developments.
- The training function of ITDZ-Berlin contributes to attracting young people to the IT profession and, more importantly, provides a continuous source of IT specialists for Berlin's Security Operations Centre, thus overcoming the potential problem of a shortage of ICT specialists.
- Since 2015, ITDZ-Berlin is a member of EURITAS, the European Association of Public IT Service Providers. Under this umbrella, working groups focus on specific topics (e.g., the digitalisation of the public administration, standardisation of rules and of data) and exchange ideas and practices (ITDZ website accessed in February 2023).

2.3 A parallel journey: developing into a smart city while pursuing information security. The experience of the Municipality of Rijeka, Croatia.

The Municipality of Rijeka started digitalising its processes and services through the implementation of municipal projects. Today, it manages a communication hub and a data centre with a complex information system that, in 2018, was ISO 27001 certified.

Background. The way the Municipality of Rijeka is organised reflects well the equal importance given to ICT activities, including information security, and infrastructure development. The Municipality has a dedicated ICT department responsible for the planning, procurement and management of ICT resources; the operation of the internal (intranet) and external network; and data security and protection. The department also looks after the digitalisation of the public administration and of the utilities companies and other companies/institutions owned and/or funded by the Municipality. The ICT department has two divisions, one dedicated to the IT systems and the other one dedicated to IT and communication infrastructures. In terms of infrastructures, the Municipality manages a data centre and a communication hub, which allow *'maximum availability, flexibility and scalability in providing digital services to city employees, utility companies, institutions founded by the City of Rijeka and citizens*' (Rijeka's ICT Infrastructure Division webpage accessed in January 2023). Municipal projects on digitalisation started being implemented in 2008. These were later complemented by information security projects aimed at consolidating the ambition to become a smart city by 2030.

Solutions and funds used for digital resilience. Municipal projects often saw their scope being scaled up. For example, at the beginning of 2008, the eOffice project, originally aimed at implementing a software solution for the urban planning department, became a standard support provided to all municipal departments and to their functional processes. In 2013, the Municipality started introducing a centrally integrated system for financial and accounting management, which was gradually deployed to the institutions founded by the Municipality. The Municipality also developed the Information Service, a system providing a central entry point for users to access a variety of services related to, for example, taxes, schools, utilities and procurement (Rijeka's IT System Division webpage accessed in January 2023). It then used its local budget to develop the information security management system of its Data Centre, where all data related to the administration of the Municipality, to the functioning of utilities and of institutional processes are stored. Several of these data are sensitive and need to comply with the GDPR; in addition, they need to be accurate and accessible as they are at the core of the delivery of municipal services (e.g.,

charging of the public transport system, parking metering, monitoring of energy consumption, and, more generally, all those services based on IT solutions such as electronic signatures and smart city cards). In 2018, the Municipality had the information security management system at its Data Centre certified according to the ISO 27001standard. It was the second local authority within the country to get such a certification (after the city of Pula) (Rijeka's news dated 11/04/18).

Over the period 2018-2019, the Municipality of Rijeka benefitted from the support given to 40 selected European cities under the Digital Cities Challenge (DCC). The challenge was funded under the COSME programme (EC, 2019). Under the challenge, in July 2019, the Municipality released its digital transformation strategy 'Digital Ri-wave'. Among the main investments included in the strategy are the development of an intranet 2.0 in order to enhance eGovernment (€10,000 from the municipal budget); an open data portal 2.0 (€10,000 from the EU and municipal budget); an integrated document management system (€200,000 from the EU and municipal budget); a Centre of Competence for R&D projects related to smart cities' environment (over €17 million from the Operative Programme Competitiveness and Cohesion Croatia 2014-2020); and eProcurement (€40,000 from the municipal budget) (DCC, 2019). The Municipality of Rijeka is now one of 136 cities engaged in the Intelligent Cities Challenge (ICC). The Municipality's development plan 2021-2029 recognises that in order to become a smart city, its already well-developed ICT infrastructure needs to be upgraded to support Gigabit connectivity. The 'Connect Rijeka 2030' strategic goal will be achieved in cooperation with telecommunications operators (Rijeka's webpage accessed in January 2023).

Highlights.

- Up-scaling of the Municipality's initiatives (i.e., from one department to all departments, from the city to its founded utilities/companies) and regular investments from its local budget characterise the digital resilience path of the city.
- Participation in DCC and ICC strengthened the Municipality's planning and strategic vision towards a smart city concept.
- ICT infrastructure needs continuous upgrading, especially to support the delivery of smart services. Similarly, requirements for information security are continuously evolving. For example, the ISO 27001:2013 standard has recently been replaced by the ISO 27001:2022 standard. This update adds some new checks (e.g., those related to the use of cloud services) and new requirements in terms of threat intelligence and ICT readiness for business continuity, meaning that it also relates to assessment and treatment of information security risks.

2.4 Building a comprehensive digital resilience ecosystem. The Brittany Region's journey to become a European 'cyber valley', France

The Region of Brittany is a leader in the field of cybersecurity. The prioritisation of thematic investments by the regional administration, from both regional and European sources, enhanced by close cooperation with the national government, industry and academia, significantly contributed to the process of building digital resilience in the region.

Background. Brittany is one of the most advanced regions in France in terms of security of information systems and cybersecurity expertise (APEC, 2017). This development has been possible due to the historical presence within the region of leading technology companies, advanced government infrastructure (civil and military), a network of start-ups and highly innovative SMEs, and renowned schools and universities offering high-level training and research on cybersecurity. Since 2013, the 'Future Pact for Brittany', a joint commitment of the State and the Regional Council for the development of the region, has made cybersecurity a strategic priority for the region, positioning it as a pioneer in this emerging field (Brittany Regional Council, 2022). In 2014, the *Pôle d'Excellence Cyber*, or Cyber Centre of Excellence, was established in the form of a non-profit association by the Ministry of the Armed Forces alongside the Regional Council of Brittany. The centre provides cybersecurity training and support research in cybersecurity and technological development through the involvement of SMEs. Brittany's regional authorities have succeeded in designing and implementing a long-term strategy of digital resilience, which focuses not only on the regional government but also on its partners, according to a quadruple-helix collaboration with industry, civil society and academia (Brittany Regional Council, 2016). The absence of notable successful cyber-attacks evidences the digital resilience of the region and of the public-private ecosystem it has developed.

Solutions and funds used for digital resilience. The development of the cybersecurity sector was a priority in Brittany's Regional Strategy for Smart Specialisation (RIS3) 2014-2020, with an investment of more than €30 million coming from national, regional and ERDF funds (ECSO, 2019). For example, funds were allocated for the operations of the Cyber Centre of Excellence (e.g., €12 million over a six-year period for doctoral and post-doctoral grants and €6.3 million in research and training platforms). An allocation of €1 million was also earmarked to finance cybersecurity projects through the launch of calls (ECSO, 2019).

In early 2022, Brittany's Regional Council established a regional Cyber Security Incident Response Team (CSIRT). This initiative is partially funded under the

French National Recovery Plan from which the region received €1 million (Ouest France, 2022). The CSIRT is designed to assist public and private actors of intermediate size such as local authorities and SMEs in the event of cyber-attacks. The CSIRT is already functional, but the team will be undergoing additional training at the National Information Systems Security Agency until 2024. In 2022, the Region also decided, in parallel with a decision made at the national level to establish a 'cyber campus', to create a 'Territorial Cyber Campus' with the aim of coordinating initiatives at a territorial level, supporting synergies, training and capacities to control digital risks and innovation (Brittany Regional Council, 2022).

Brittany also plays a leading role in European projects related to cybersecurity. In 2018, it participated in the CYBER project (2018-2023), represented by *Bretagne Développement Innovation* (BDI) as lead partner, and the Regional Council. It had a budget of €342,760, of which €291,346 was funded through the ERDF under the Interreg Europe programme. CYBER had the objective of enhancing cybersecurity ecosystems in participating regions by boosting the competitiveness of cybersecurity SMEs through improved public policies (keep.eu project summary and BDI website accessed in February 2023). In the same year, the Region became the leader of the EC's pilot 'Cybersecurity Smart Regions' the aim of which was to develop interregional cooperation for smart specialisation on cybersecurity.

Highlights.

- The Brittany Region is an inspiring example of how an all-encompassing cybersecurity ecosystem significantly contributes to the digital resilience of the territory. In particular, supporting the innovation and excellence of the private sector proved beneficial in terms of digital services received and management of potential disruptions. Also, the investments made in education, research and development provide a solid base of expertise and scientific excellence.
- The Region is already transferring its experience in the cybersecurity domain to other regions. The CYBER project highlighted that common challenges faced by regions include '*the need for skills, the fragmentation of the cybersecurity market at the European level, and insufficient collaboration between the various players in the ecosystems, particularly between the public and private sectors*' (BDI webpage accessed in February 2023).
- The Region closely cooperates with the national government and complements national initiatives, such as occurred in the case of the 'Territorial Cyber Campus'.

2.5 Vilnius City's comprehensive set of measures for digital resilience, Lithuania

Selected among Europe's most innovative cities in 2021, the Municipality of Vilnius demonstrated its capacity to offer innovative services to citizens and businesses while introducing a comprehensive set of measures to ensure that its ICT systems and services are digitally resilient.

Background. Cyber-attacks on Lithuanian LRAs are common and referenced in most of the annual reports by the National Cyber Security Centre (NKSC website accessed in February 2023). In particular, the Municipality of Vilnius had already suffered from a so-called 'brute force' type of attack in 2015 (tv3 news dated 14/01/15). At that time, the attack disturbed the annual registration of children to the municipality's kindergarten. Although clear information was provided to the public by means of various news, press releases and social media, and a press conference was held by the Mayor himself (you tube video accessed in February 2023), trust in municipality's service provision suffered as citizens questioned the transparency of the overall process.

Since then, the municipality has significantly improved the resilience of its systems. Despite the fact that, in 2021, the National Cyber Security Centre reported municipal websites to be the most vulnerable against hybrid cyber-attacks (NKSC, 2021), Vilnius Municipality successfully countered most of them. For instance, in January 2021, multiple log-in attempts to the municipal platform occurred (LRT news dated 27/01/21), but attacking IPs were automatically blocked by the city's systems whereas several other municipalities did not manage to defend their systems against the same attack. The risk was also evaded during the intense DDoS (Distributed Denial of Services) attacks organised by the 'Killnet' cyber criminals' group in June 2022 (Kapsevičius, 2022).

Solutions and funds used for digital resilience. The main reason why the Lithuanian capital managed to significantly improve its resilience is, according to Mr. Pidkovas, Head of the City's Technology and Innovation Group, a mixture of cross-cutting measures, as well as an understanding of the risks and political support from higher levels of management and of decision-makers[13]. In 2021, Vilnius Municipality announced an ambitious ten-year Strategic Development Plan which provides the city's vision for 2021-2030. In the area of security and protection, the city set three strategic directions which are currently being implemented. They reflect a mixture of cross-cutting actions supporting different aspects of the city's digital resilience, namely: 1) creation of a Coordination

[13] Mr. Jonas Pidkovas was interviewed by the authors on 06/02/23.

Group for the city's digital infrastructure managers; 2) development and scale-up of the 'Vilnius Cyber Grid' concept whereby the city ensures an additional layer of security for internet access and for the city's digital infrastructures – the concept is currently being piloted in few public enterprises managed by the municipality with a view to later extending it to all the city's services and structures; 3) further development of the 'Hack me if you can' initiative, including through massive communication campaign and dedicated prizes (Vilnius Municipality, 2021). The latter is an initiative developed by the city and unique in the country, piloted in 2020 and now growing to engage more people. Its aim is to better secure the city's IT infrastructure by involving its residents and interested civil experts who are invited to test the city's platforms and applications by performing attacks on them, and then to inform the responsible municipal personnel about detected vulnerabilities. Importantly, the city also developed a Responsible Vulnerability Detection Policy, i.e., a set of rules of engagement for ethical hackers to identify and submit information on security vulnerabilities to the responsible authority, without a risk of being prosecuted or punished. This policy has also inspired national regulation on the topic (Government of Lithuania, 2021).

Finally, the municipality offers continuous upskilling for its ICT staff, is currently introducing cybersecurity and data protection training as part of the 'starting training' provided to new employees, and implements a continuous cyber data exchange with its public enterprises and a number of private companies operating in the city (information obtained through the interview with Mr. Pidkovas). Mr. Pidkovas further explained that all activities are currently funded using the municipal budget, but that the city plans to apply for EU funds, namely, the Digital Europe Programme.

Highlights.

- Vilnius City implements a comprehensive mix of cross-cutting actions to ensure its digital resilience. The effectiveness of this approach, fully funded by the city's local budget, is demonstrated by the city's high level of resilience during recent attempted cyber-attacks.
- Core elements of the approach are the existence of an overarching strategy supported by a high-level management; a coordinated approach within the municipality and among its public enterprises; collaboration and data exchange with the private sector; staff training; and innovative initiatives involving residents and local experts.
- Innovative approaches, such as the 'Hack me if you can' initiative, allow for the use of residents' expertise and ensure the engagement of city's experts. They are easily replicable elsewhere as long as a regulatory framework for vulnerabilities' disclosure is put in place.

2.6 Use of NRRP's funds to bridge the digital resilience gap of the Lazio Region, Italy

Over the night of 31 July 2021, the Lazio Region suffered from a ransomware cyber-attack to its data centre that compromised the provision of services and caused a data breach. In October 2022, the Region applied for funds from the National Recovery and Resilience Plan (NRRP) to implement a set of actions aimed at pursuing its digital resilience.

Background. The cyber-attack suffered by the Lazio Region in the summer of 2021 had enormous repercussions in the media. The media response echoed beyond national borders and this was probably what the Region meant when it called this a terrorist attack and the most serious criminal (digital) offensive ever to have occurred in the country. Media coverage was also due to the fact that the cyber-attack affected a key infrastructure (i.e., the computational data centre of Lazio) and the regional online booking system for COVID-19 vaccination. At the time, the system was overwhelmed by thousands of requests. Among the consequences suffered were the temporary unavailability of health data and the halt of the COVID-19 vaccination booking system. The Region also lost some of its internal documents of which no offline back-up existed. The Region made announcements concerning the attack on its social media feeds (e.g., Twitter, Facebook) the day after the attack and published a formal note on its website on 7 August 2021. LazioCrea S.p.a., the company owned by the Region and managing the data centre, published an online note on the attack on 16 August 2021. The ransomware's intrusion occurred through the laptop of an employee of LazioCrea S.p.a. who was smart working (web article by Navacci, M. dated 08/08/21 and published on the Network Digital 360) and was apparently facilitated by the absence of authentication requirements for privileged access. LazioCrea S.p.a. reported that no ransom was paid, but that the cost of recovery extended to millions of euro (blog by Fadda, D. dated 25/10/22 and published on '(in)Sicurezza Digitale'). LazioCrea S.p.a. asked for the support of the Leonardo Group, a private service provider, to recover from the attack and to interact with the national body in charge of incidents monitoring and intervention.

Solutions and funds used for digital resilience. At the national level, the Lazio Region's incident fed the policy debate on the need to invest in the resilience of the public sector and in the upskilling of civil servants. The timing was appropriate as a national law on 'urgent provisions related to cybersecurity' had entered into force a few months earlier, in June 2021 (Law Decree n.82/2021). This was a follow-up to the country's commitments made in the NRRP. The law established the National Agency for Cybersecurity (ACN) that became responsible for the implementation of the national cyber strategy. The strategy is very much focussed on the strengthening of resilience capacities, including those

of the public administration (ACN website). In August 2022, the government launched a call for proposals funded under the NRRP for interventions aimed at enhancing the 'cyber resilience' of regions, autonomous provinces and main towns.

In May 2022, the Lazio Region released its regional Digital Agenda 2022-2026 and, in October 2022, applied for about €2 million under the above call with the following three project proposals: 1) raising security awareness of the Region's public servants with an approach tailored to the different roles, functions and organisational management within the authority; 2) improving the solutions used for the monitoring and defence against cyberthreats, including AI-based ones; 3) enhancing the security of the Region's ICT infrastructure and information systems coherently with the national provisions for cybersecurity and data protection (Lazio Region press release dated 20/10/22). The Region saw two of these projects funded with a budget of over €1.2 million. The awareness-raising project, although assessed as eligible, was not funded because of insufficient financial coverage at a national level.

Highlights.

- The cyber incident made the Region and its agency aware of their vulnerability. If learning from incidents is important, waiting for an incident to happen before embarking on a digital resilience path is not strategic.
- There is evidence of the strategic role of the NRRP in initiating or speeding up digital resilience processes, which were evidently lagging behind at both the national and sub-national level. Inclusion of a tailored budget for digital resilience in the NRRP is instrumental to the launch of relevant initiatives by LRAs.
- Cyber incidents have occurred in several public administrations across Italy, but the way the case of the Lazio Region was communicated may have been disproportionate. The communication of cyber incidents to the general public may be instrumental to the achievement of different goals.

2.7 Building a digital resilience culture after participation in an EU-funded project. The case of the Municipality of Amadora, Portugal.

Further to its participation in a Horizon 2020 project that emphasised the importance of the human component in pursuing cybersecurity, the Municipality of Amadora boosted its digital resilience activities.

Background. The Municipality of Amadora was one of five local public authorities involved in the H2020 project 'COmpetitive Methods to protect local Public Administration from Cyber security Threats' (COMPACT). The project, implemented over the period 2017-2019 and funded under the Societal challenge 'Secure societies - Protecting freedom and security of Europe and its citizens', aimed at strengthening the digital resilience of participating public administrations through awareness-raising, training, provision of tools for quick and effective risk assessments as well as monitoring, information-sharing and knowledge-sharing services. The Municipality of Amadora received a net EU contribution of €140,875.00 under the project.

Solutions and funds used for digital resilience. Within the framework of the COMPACT project, the Municipality of Amadora developed two best practices ready for adoption by other local authorities. The first relates to the category 'Physical and Environmental Safety Policy'. The Municipality first defined the physical area to be protected (e.g., the City Hall office, data processing centres, cabling cabinets and work areas) on the basis of the presence of critical information. Then, it classified this area into red and yellow zones and set specific rules for accessing the two security levels, including by third parties, through 'physical access control mechanisms' (COMPACT, 2019). The other best practice relates to making municipal services compliant with the provision of Regulation (EU) 2016/679 on data protection (GDPR). To this end, it was necessary to understand in which contexts personal data were used by civil servants when rendering services and to validate the storing and processing processes. In February 2019, the Municipality adopted the monitoring technology Business Process Intrusion Detection to automatically identify personal data and validate GDPR compliance. This solution offers protection against cybersecurity incidents (e.g., intrusions or forgery of equipment behaviour) and operational security incidents (e.g., equipment and network failure, human error or natural disasters) (COMPACT, 2019). More comprehensively, GDPR compliance required the preparation of an action plan including carrying out training sessions for municipal employees, the reorganisation of the management structure (with the nomination of a data protection officer) and the definition of counter-measures for handling data breaches. Activity reports of the Municipality from 2020 and 2021 evidence the many initiatives undertaken by the Municipality to enhance its

digital resilience after the completion of the project. Among these initiatives are an internal consultation to assess the knowledge and level of awareness of its employees in terms of cybersecurity; the implementation of a series of information security solutions to safeguard employees' remote working modalities (particularly important in early 2020, during the first wave of the COVID-19 pandemic); the running of a behavioural monitoring solution able to teach public servants in a user-friendly way how to avoid mistakes; and the procurement of a Disaster Recovery solution to improve the resilience of the technological infrastructure and critical systems in case of incidents (Municipality of Amadora, 2021 and 2022). In 2021, the Municipality continued to enhance the skills of its employees on the implementation of its Information Management and Security System and GDPR compliance, according to national Law No 58/2019. External service providers were hired for the training with a cost of some €8,000 (SecurityMagazine press release dated 27/07/21). In October 2021, a Security Awareness Training was also carried out in a flexible manner so as to facilitate the participation of employees. Awareness-raising campaigns on information security and cybersecurity were carried out on the municipal intranet and via e-mail. All these activities were regularly monitored and evaluated. In addition, the Municipality defined the roles and objectives of information security management and continued to certify its ICT services according to the ISO 27001 standard (Amadora was one of the first two Portuguese municipalities to be certified by this standard). All of the above was endorsed and supported by top-management (Madeira Simões, 2021).

Highlights.

- The municipality was encouraged in its embarking on a path to digital resilience by its participation in the EU project. This is evidenced by the regular provision of training, the awareness-raising initiatives for civil servants, the continuous enhancement of information security solutions, the renewal of the ISO 27001 certification and the endorsement of all these initiatives by the top-management of the municipality.
- The general objectives of information security management in the municipality are said to be reputational and economic. Namely, the double aim is to improve the image of the municipality while simultaneously reducing damage that may be caused by incidents.
- The case of Amadora underlines the key role of the human factor in making a local authority digitally resilient, which nevertheless must be associated with the use of appropriate tools, instruments, technologies and organisational changes.

2.8 Danish public sector multi-level collaboration for digitalisation and cybersecurity

The Danish government's path towards digital resilience dates back to December 2014 when the first National Cyber and Information Security Strategy was issued. But it is since 2001 that a multi-level collaboration across central, regional and local governments has been pursuing a digital public sector (DIGST website).

Background. Denmark was heavily targeted by cyber-attacks in past years. For example, in 2015 and 2016, two severe breaches hit the Danish Defence Ministry revealing employees' emails. This serious threat to security was communicated by the Danish ministry, which focussed on the limited extent of the damage, as hackers gained access to non-classified documents, and on the actions taken internally to improve the security of emails with non-classified content (Euractiv news dated 24/04/17). This specific breach was the trigger for the Danish government to decide to invest in cybersecurity. Another major breach occurred in 2020, when the self-service software of the Danish tax portal leaked the Danish personal identification numbers (the so-called CPR) of 1.26 million Danes, i.e., one fifth of the Danish population (CyberLands website). In the same year, public computers across the country were attacked and once again CPR numbers were stolen. The public authorities communicated clearly about immediate actions to be taken by citizens, e.g., changing passwords of any account used via a public computer (CPH Post, 2020). These data breaches, although with no major security aftermaths, prompted the government yet again to develop a new strategy and invest in cybersecurity.

Solutions and funds used for digital resilience. At the national level, the implementation of cyber and information security has been driven by the continuous update of multi-year national strategies. In parallel to these strategies, the central government, regions and municipalities cooperate to further increase information security efforts, protect privacy and ensure a high level of security of digital infrastructure at all levels through jointly prepared digital strategies. For example, the National Cyber and Information Security Strategy 2015-2016 laid the groundwork for the implementation of security standards (e.g., the ISO27001) across all levels of governments (DCCS, 2015). This became a focal point (i.e., 'The public sector protects data') in the joint Digital Strategy 2016-2020 (The Government - Local Government Denmark - Danish Regions, 2016). At the municipal level, investments in information security were made between 2016 and 2019 for the development of a baseline platform '*where municipalities indicated the status of information and personal data security on more than 400 parameters. The focus areas were ISO 27001-2, personal data security and cyber security*' (i-Trust webpage). This baseline platform made it possible for all municipalities in the country to measure their status with regards to IT security

and the impact of their efforts over the years. At the regional level, the Danish Regions developed a Joint Regional Information Security Policy under which they committed to comply with existing legislation in terms of protection of information and created the basis to adopt ISO 27001 standard in their IT systems (Danish Regions, 2017).

The current National Strategy for Cyber and Information Security covers the period 2022-2024. The strategy places an emphasis on securing ICT operations in the public sector as well as safety of critical infrastructures. For its implementation, the government allocated around €36 million across 34 initiatives (DIGST webpage accessed in February 2023). This supplements the resources allocated via the 2018-2023 Defence Agreement[14] through which Denmark's cyber defences were considerably reinforced at a cost of more than DKK 1.4 billion (approx. €180 billion) over six years (DIGST, 2018). As part of the Strategy, the Division for Cyber and Information Security in the Danish Agency for Digital Government is in charge of implementing information security initiatives in collaboration with local governments and regions, which are thus continuously working to strengthen their cyber and information security (DIGST webpage). One of the outcomes of the strategy is the development of the sikkerdigital.dk, a website where regional and local authorities have access to resources such as guidance on information security and management; training materials on cybersecurity for administration and managerial staff, procurement lawyers and IT system administrators; and practical recommendations on GDPR and data protection in public authorities.

Highlights.

- The Danish cooperation model across different levels of government allowed '*for the Danish public sector to make joint investments in areas which are particularly complex and in which there are interdependencies across different authorities, sectors, and levels of government'* (DIGST webpage).
- Political commitments and guidelines to foster cybersecurity that focus on a specific level of government, such as the Danish Regions Joint Regional Information Security Policy, enable all authorities belonging to that level to follow the same necessary steps in their path to digital resilience.
- Sikkerdigital.dk is a one-stop-shop platform with resources related to cybersecurity and skills. It is an example of a concrete investment made at the central level to create a knowledge base for the benefit of public authorities, but also of citizens and businesses.

[14] A national white paper on armed forces agreed by political parties.

Part 3. Cost of digital non-resilience

This part develops a **definition of digital non-resilience from the perspective of local and regional authorities** and explains **why its cost cannot be quantified.** It then describes the types of damage caused by digital incidents, the impact deriving from the damage and the factors that, with lack of monetary quantifications, should be taken into account by LRAs when deciding whether to invest in digital resilience. Building on the findings of the online consultation, the experts' interviews and desk research, the last section develops scenarios on the evolution of the digital resilience of European LRAs by 2025 and 2030 and identifies relevant wild cards that might potentially threaten the smooth achievement of digital resilience by LRAs in the next years.

3.1 The cost of digital non-resilience for LRAs: a definition

According to the definition of digital resilience of public authorities as given in the introduction of this study, the components that LRAs can improve through investments are **digital infrastructures** (i.e., communication networks and information systems including hardware and software) and **skills** (i.e., digital and cybersecurity skills). These components, when considered together, represent the **digital layer of a public authority** guaranteeing the authority's functioning and the provision of services (both digital and 'traditional').

The exposure of a local or regional authority to threats expresses its vulnerability. This vulnerability generates costs if threats materialise into incidents compromising the authority's functioning and the provision of public services. Examples of incidents include a cyber-attack by a criminal organisation that locks tax payment data stored in a municipality's server; or a flood damaging the ICT infrastructure of a regional authority providing online access to eHealth records. Such incidents that compromise the digital infrastructure of an LRA are referred to as digital incidents.

> The **cost of digital non-resilience** for a public authority is defined as the actual or estimated monetary cost that an authority affected by a digital incident sustains in an effort to restore its functioning and provision of services to a level at least equal to the one existing before the digital incident.

There are two major challenges related to the assessment of the cost of digital non-resilience for a public authority. First, **there are no standard methods to assess the cost of digital non-resilience for LRAs**. This evidence from desk

research is confirmed by the outcomes of the interviews carried out within the pool of experts.

> **from the interviews** *Experts' opinion on the way to quantify the damage, assess the impact, or evaluate the costs of a digital incident affecting European LRAs.*
>
> Half of the interviewed experts were unable to suggest methods to assess damage, impact or cost of digital incidents affecting LRAs. One think tanks/academia expert proposed a computation of damage based on multi-dimensional indicators measuring, for example, how much time services are offline and which services are disrupted. Another expert from the same sector suggested combining risk assessment with cyberthreat intelligence. He also reported the existence of cybersecurity self-assessment tools for the private sector/SMEs. One example of this is the tool made available online by the Cybersecurity Observatory, an initiative funded by CNR, the European Commission, Registry.it, the Tuscany Region and other entities. Among other outputs, the tool provides an estimate of annual losses for any type of threat and an overall assessment of the cyber risk.

Second, **the quantification of the cost of digital non-resilience for one authority cannot be used to quantify the cost for another authority**. There are a number of elements specific to each authority and related to both its digital layer and its daily operations that need to be considered. For example, the number of personal computers connected to the internet or the number (and type) of public services provided to citizens and businesses, for which data are digitally stored. On top of these elements, there is the digitalisation level of the authority. The more LRAs are digitalised, the higher is the potential damage caused by digital incidents.

3.2 Damage caused by digital incidents

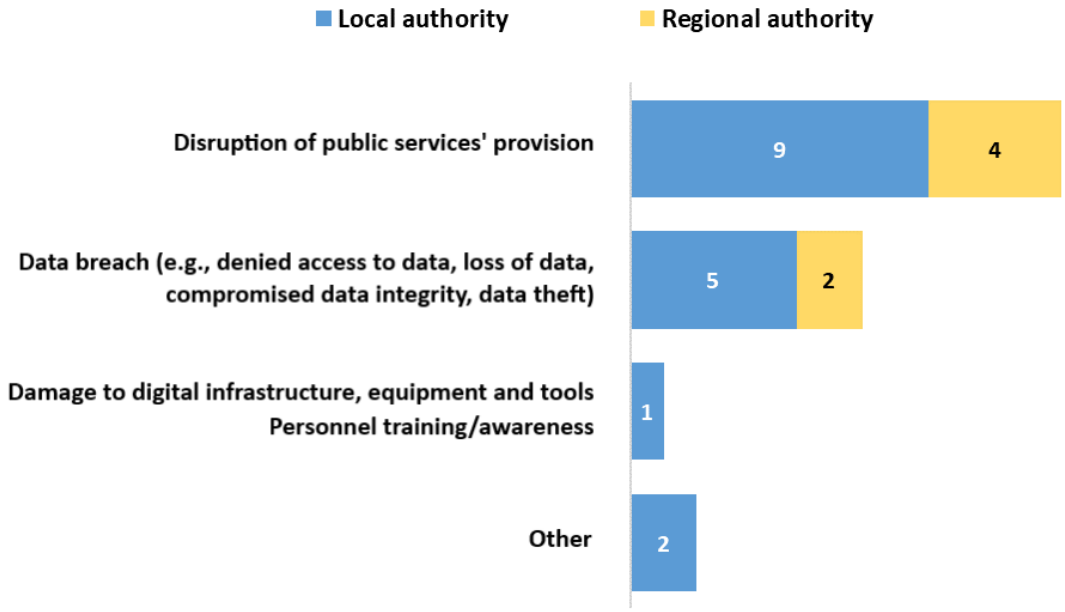
Part of the cost of digital non-resilience of LRAs caused by digital incidents depends on the type of damage (e.g., affected personal computers, loss of data) and the pervasiveness of the damage (e.g., number of personal computers to be replaced, gigabytes of leaked personal data)[15]. The online consultation carried out in this study investigated the type of damage suffered by LRAs in case of cyber-attacks. The interviews with experts were used to ask opinions on which type of damage caused by cyber-attacks may have a higher cost for LRAs.

In the consultation, among the 17 authorities declaring to have suffered at least one cyber-attack with significant disruptive effects from 2000 onwards, ***disruption of public services provision*** is the most selected **type of damage**

[15] As described in Table 1, different types of damage to the digital infrastructures of LRAs generate different types of impacts.

suffered both at the local and regional level (76% of the attacked LRAs)[16]. *Data breaches* follows, selected by 41% of the attacked LRAs. In only one case, the attack caused *damage to digital infrastructure* (Figure 15).

Figure 15. Damage suffered by the attacked authorities



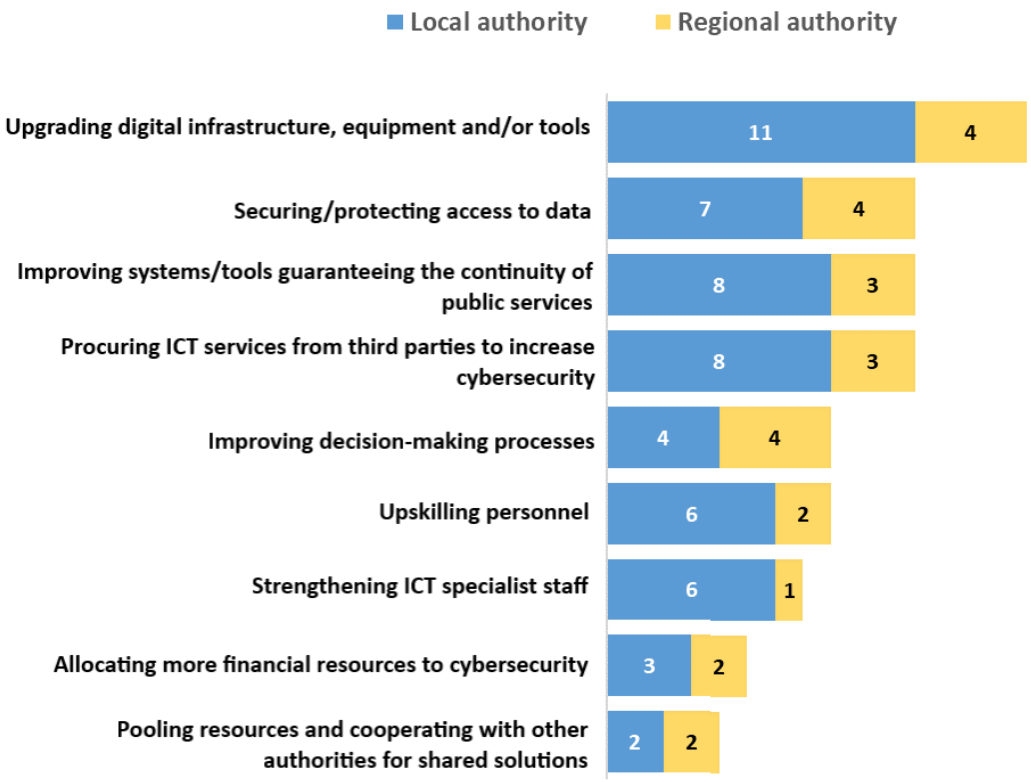
Source: online consultation.

On **actions taken by the authorities after suffering cyber-attacks**, the most selected option is the ***upgrading of digital infrastructure, equipment and/or tools*** (15 selections, 88%) (Figure 16)[17]. This is followed (with 11 selections each, 65%) by *securing/protecting the access to data*, *improving systems/tools guaranteeing the continuity of public services* and *procuring ICT services from third parties to increase cybersecurity*. The least selected action by local authorities is the *pooling of resources and cooperating with other authorities for shared solutions*; for regional authorities, it is the *strengthening of ICT specialist staff*.

Answers from the attacked authorities highlight that a systemic improvement of prevention (focusing on digital infrastructure) and preparedness (focusing on digital skills of public servants) comes after a cyber-attack and that rarely one single action was selected (i.e., 15% of local authorities and none of the regional authorities). Among local authorities, the most common choice was the selection of three or five actions (23% of the respondents, each). Some of them (8%) selected nine actions.

[16] Multiple selections were possible for this question.
[17] Multiple selections were possible for this question.

Figure 16. Type of actions taken after the cyber-attack



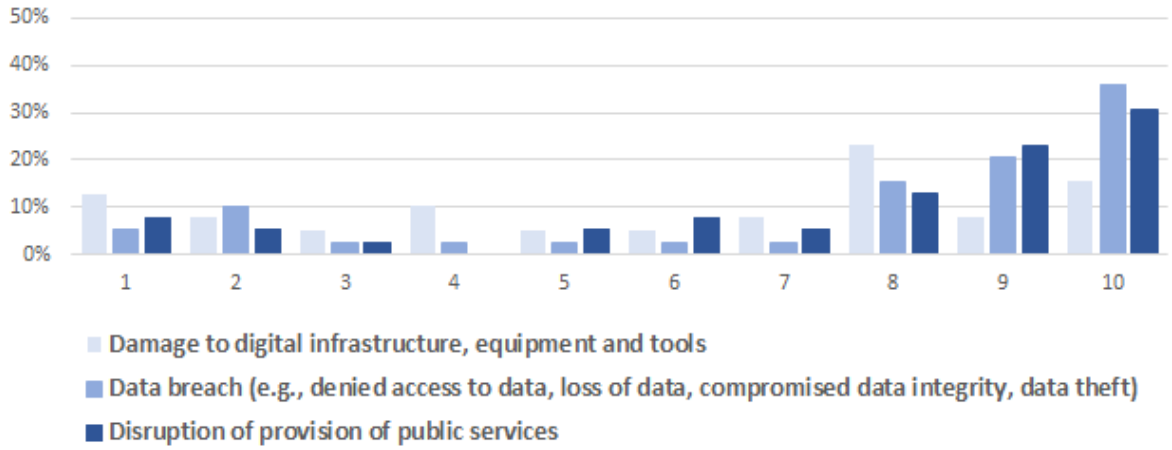
Source: online consultation.

In the consultation, 47 LRAs reported not to have suffered from cyber-attacks from 2000 onwards. These authorities were asked about their perception of the relevance of damage that may be caused in case of a cyber-attack. Perceptions were provided against three main types of damage (damage to digital infrastructure, data breach and disruption of public service provision) and scored on a scale from 1 to 10, where 1 = no damage and 10 = very significant damage. *Data breaches* are perceived to cause at least high damage (i.e., rated 8 or more) by 72% of the respondents and for one third of them *data breaches* generate *'Very significant damage'* (i.e., rated 10). The second most perceived damage is *Disruption of the provision of public services.* It is supposed to cause at least high damage (i.e., rated 8 or more) by 68% of the respondents and for 28% of them *disruption of the provision of public services* generates *'Very significant damage'* (i.e., rated 10).

When analysing the perception of the relevance of the damage by types of authorities some differences emerge (Figure 17 and Figure 18). Data breaches are considered to cause the most significant damage by local authorities. At least high damage (i.e., rated 8 or more) are perceived by 72% of the local authorities. Local

authorities have a perception of low damage caused by *digital infrastructure, equipment and tools*. This is confirmed by the comparison between the weighted means for the three types of damage: 6.0 for *digital infrastructure, equipment and tools*; 7.5 for *disruption of the provision of public services*; and 7.6 for *data breaches*.

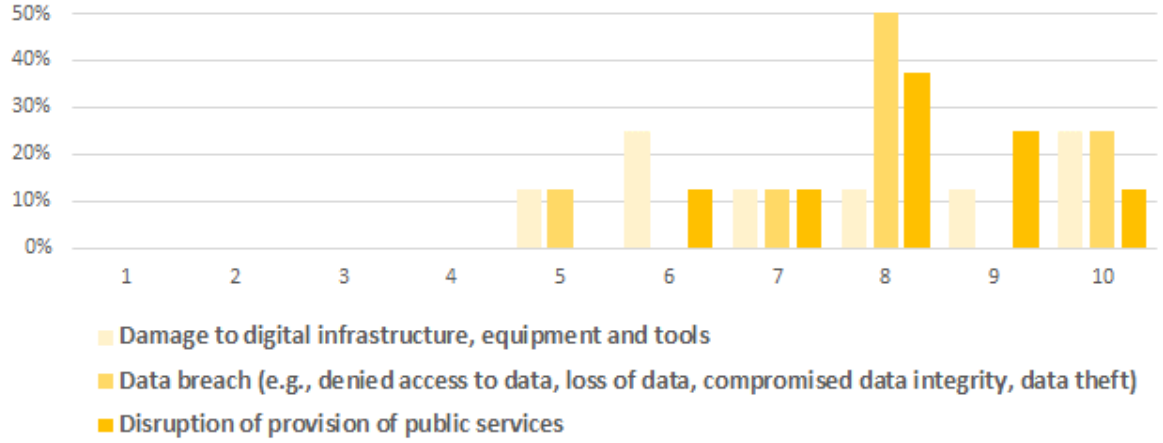
Figure 17. Perception about the damage that may be caused by a cyber-attack (local authorities not having suffered cyber-attacks from 2000 onwards)



Source: online consultation.

In the case of regional authorities, data breaches and disruption of services' provision are equally considered to cause at least high damage (i.e., rated 8 or more) by 75 % of the respondents. However, in general, **regional authorities perceived higher damage caused by cyber-attacks and less differences between the types of damage than local authorities**. This evidence is given by the fact that no scores below five are given by regional authorities. The weighted means are 7.6. for *digital infrastructure, equipment and tools*, 8.0 for *data breaches* and 8.1 for *disruption of the provision of public services*.

Figure 18. Perception about the damage that may be caused by a cyber-attack: (regional authorities not having suffered cyber-attacks from 2000 onwards)



Source: online consultation.

❞ **from the interviews**👀 *Experts' opinion on which type of damage caused by cyber-attacks may have a higher cost for LRAs.*

Referring to the same types of damage, **data breaches** were considered by six interviewed experts as the type of damage with the highest costs for LRAs. One of the industry experts commented on the social impact of data breaches because public services, in particular for citizens, are compromised as a consequence. Two experts considered the **disruption of public service provision** as the damage with the highest costs**.** Two other experts stated that public service disruption ranks second after data breaches when referring to costs**.** Experts from the public sector highlighted that the relevance of the impact of public service disruption depends on the type and number of services that LRAs provide, the data they store, and the intensity and duration of the disruption. In addition, it was highlighted that the damage, and related costs, depend on the services affected by the digital incident. For example, in the case of health systems, the interruption of the service may have a possible impact in terms of human lives and reputation of the LRAs. Another public sector expert advised that it is unwise to underestimate the high cost of damage to digital infrastructure, equipment and tools.

3.3 Impacts deriving from the damage caused by digital incidents

In addition to the type and pervasiveness of the damage, the cost of digital non-resilience for LRAs is affected by the **threat causing the digital incident**. Different impacts can be expected for natural disasters or cyber-attacks. Information about estimates of costs related to digital incidents' damage caused by **natural disasters** is not frequent. Usually, natural disasters have widespread effects on entities and territories with a consistent impact on the physical layer and a large number of actors (e.g., no access to buildings by citizens, unavailability of power for businesses) that make it complex to 'isolate' the part of costs directly related to the digital layer of the affected public authorities. For

example, in the case of a flood, the cost of digital non-resilience of an affected public authority is often hidden or included in the overall cost of the event.

The fact that **cyber-attacks** are malicious actions often targeted at, or at least affecting only, individual victims, makes it possible to identify the damage suffered by the authority and the related direct costs of the digital incident. Nevertheless, information about the damage of cyber-attacks is often not made public for a number of reasons and, when disclosed, costs are still hard to quantify[18] given the different types of impact that should be considered.

When referring to cyber-attacks, ENISA (2022) classifies their impact into five types: reputational, digital, economic, physical and social. In Table 1, these types are described from the perspective of LRAs and stress the difference between cyber-attacks and natural disasters.

Table 1. Types of impact of digital incidents for LRAs within this study

Type of impact	Description
Economic Impact (EI)	This is the direct monetary loss incurred by the public authority further to the incident and is not linked to its recovery phase. According to this definition, the EI concerns primarily cyber-attacks. Examples are a paid ransom for unlocking stolen data or an administrative fine for not properly informing the competent authorities of a data breach. Lost revenue for the affected authority, further to the disruption of public services that are provided on a payment basis, may also generate EI. The EI is the easiest one to quantify in terms of cost of digital non-resilience.
Digital Impact (DI)	This primarily refers to the public authority's digital infrastructure that can be temporarily or permanently compromised. The DI is a consequence of cyber-attacks as well as of natural disasters. In terms of the financial cost of digital non-resilience, repair costs (e.g., through the involvement of IT specialised subcontractors), costs for new infrastructures to replace the compromised ones (e.g., new personal computers) and human resource costs required to restore the functioning of the authority and the affected public services are all consequences of DI. A second, but not secondary, DI relates to the unavailability of data. Part of the cost of digital non-resilience is then linked to the time, effort and expense needed to restore these data for the provision of services. In the case of unavailability of data, the digital impact may be coupled with additional monetary losses (i.e., EI).
Social Impact (SI)	This refers to the effects that an incident has in terms of the interrupted provision of public services to citizens and businesses. The SI is a consequence of cyber-attacks as well as of natural disasters. Its extent varies according to the length of the interruption, which, in turn, depends

[18] For ENISA (2022, p.14), in case of a cyber-attack, *'determining and assessing the effect following an incident entails a level of assumption in which a certain degree of subjectivity cannot be avoided.'*

Type of impact	Description
	on the DI. The SI then contributes to the RI (see below). The SI is one of the most challenging to quantify in terms of cost of digital non-resilience.
Reputational Impact (RI)	This implies a negative or adverse perception by the general public of the authority that suffered damage due to an incident affecting its functioning and provision of services. The RI is also a consequence of natural disasters, although, in the case of cyber-attacks, trust in the public authority can be significantly affected if information on the attack and its damage (especially in the case of data breaches) are not properly communicated to the general public. The extent of the DI (e.g., the number of interrupted services, the number of affected users, the type and quantity of lost data) is the primary factor affecting the authority's reputation (that is blamed for being unprepared). In terms of the cost of digital non-resilience, the reputation of the public authority is affected also by the time needed for recovery. As for the SI, monetary quantification of the RI is challenging.
Physical Impact (PI)	This refers to any kind of injury or harm to human beings caused by the digital incident. This type of damage is usually a direct consequence of natural disasters. In the case of cyber-attacks, PI may occur, for example, when the digital incidents jeopardise the provision of crucial healthcare services. Quantification of costs due to PI contributes to the assessment of the cost of digital non-resilience of LRAs.

Source: authors' elaboration on the categorisation of ENISA (2022).

In the case of cyber-attacks, the cost of digital non-resilience of a public authority results from the quantification of all five types of impact caused by digital incidents[19]. When a natural disaster is the cause, EI and RI contribute marginally.

❞ **from the interviews**👀 *Experts' opinion on other high-cost consequences of cyber-attacks.*

Notably, five experts referred to **the loss of public trust or reputation among citizens** as 'the' high-cost consequence of digital incidents caused by cyber-attacks to LRAs. In addition, one industry expert commented that LRAs should properly consider the way the public is informed about the damage occurred. It is not important to offer information on what actually happened, what was the cause of breach or what damage it caused, but it is critical to properly communicate what was breached and the authority's capability to react and protect in the future. Wrong messages may generate a negative reputational impact. Among the other possible high-cost consequences for LRAs, one industry expert and one think tank/academia expert highlighted **the potential negative effects of cyber-attacks on the democratic process**. This is the case when digital tools (e.g., platforms) are made available to citizens to participate in the decision-making process, for example, through

[19] Future research can explore another type of impact that is not considered in Table 1: the environmental impact of digital incidents affecting LRAs.

electronic voting. One of the experts referred to cases of hacking attempts occurring in different countries during political elections.

3.4 Factors affecting LRAs' decision to invest in digital resilience

Whatever the threat is (Box 2), by considering the occurrence of a digital incident, LRAs face a dilemma based on a choice between two strategies:

A. **not investing and, in the event of digital incidents, bearing the cost of digital non-resilience**, or
B. **investing continuously to achieve a certain level of digital resilience** that may guarantee the functioning of the authority and the continuity of the provision of public services, or a prompt recovery in case of digital incidents.

The choice for Strategy A means that costs are faced only if the incident occurs (e.g., in the response and in the recovery phase). Strategy B requires LRAs to regularly bear expenses for prevention (e.g., purchase of updated firewalls) and preparedness (e.g., regular awareness-raising of public servants). These expenses contribute to building the digital resilience of the public authority. However, additional costs for response and recovery, although substantially lower than those incurred under strategy A, may also take place.

Figure 19. Factors affecting LRAs' decisions to invest, or not, in digital resilience

	Factors favouring Strategy A: bearing the cost of digital non-resilience	Factors favouring Strategy B: investing in digital resilience
Occurrence & likelihood of digital incidents	• Uncertainty of the occurrence of digital incidents with a significant disruptive effect.	• Increasing likelihood of digital incidents with a significant disruptive effect due to the increasing number of: - natural disasters driven by climate change; - cyber-crime organisations targeting public administrations.
Costs & expenses	• Lack of awareness about the cost that a digital incident with a significant disruptive effect may cause. • Uncertainty of the level of digital resilience to be achieved to avoid bearing the costs in case of digital incidents with a significant disruptive effect. • Uncertainty of the expenses needed to maintain digital resilience in the future. • Mitigation of the cost through cybersecurity insurance.	• Lack of financial capacity to bear huge recovery costs that a digital incident with a significant disruptive effect may cause. • Opportunity to face reasonable expenses over time (also using public funds and other financial instruments).
Human resources & skills	• Need for an organisational change in allocating responsibilities for digital resilience. • Need for structural support from ICT specialists. • Need for continuous digital awareness raising / training of public servants.	• Opportunity to have the authority's management able to react to digital incidents with a significant disruptive effect. • Reducing the damages and impacts of digital incidents with a significant disruptive effect by awareness-raising/training public servants.
Constitutional role of the authority	• Impossibility of market failure of a public authority (even if hit by a digital incident with a significant disruptive effect).	• Societal responsibility of the public authority as a provider of public services.
Politics & policies	• Short-term vision of the political representatives.	• Provisions at the national and European level for increasing cybersecurity requirements also for LRAs (e.g., the entry into force of the NIS2 Directive). • Provisions at the national and European level guarantee the continuity of some LRAs services (e.g., the entry into force of the CER Directive).

Source: the authors.

While considering the **factors affecting the decision** of European LRAs towards the choice of one (A) or another (B) strategy, we grouped them into five categories: **occurrence & likelihood of digital incidents**, **costs & expenses**, **human resources & skills**, **constitutional role of the authority**, and **politics & policies.** Factors are detailed in Figure 19, by group. Evidence for each group is then provided in the following section 3.5.

Box 2. An 'old' dilemma

The trade-off between investing in prevention and preparedness to increase resilience and bearing costs for reaction and recovery after the occurrence of a disruptive event, has been debated in the domain of natural disasters for decades. The Sendai Framework for Disaster

Risk Reduction 2015-2030 emphasises the **need for disaster risk management rather than disaster management**. One of its four priorities is '*Investing in disaster risk reduction for resilience*' (Priority 3). The underlying assumption is that '*Reducing disaster risk is a cost-effective investment in preventing future losses'* (UNDRR, 2015, p.9).

3.5 Evidence on factors affecting LRAs' decisions to invest in digital resilience

Although LRAs are supposed to stick to a 'precautionary principle' in their decision-making process[20] and, hence, opt for not facing the risk of bearing the cost of digital non-resilience, this does not necessarily materialise into an investment strategy for digital resilience. Among other reasons, there might be a lack of funding (see Part 1) or the presence of other obstacles. In some cases, it may be due to unawareness of the costs implied by digital non-resilience. This section aims at providing public authorities with evidence (i.e., examples of digital incidents occurred to LRAs) aimed at supporting the decision-making process.

3.5.1 Occurrence and likelihood of digital incidents

One of the main arguments in favour of not investing in digital resilience relates to the perception that the likelihood of experiencing a digital incident with a significant disruptive effect is extremely low. In reality, natural disasters are increasing in number and intensity (UNDRR, 2015) and, in recent years, public authorities, including LRAs, have become a 'privileged' target of cyber-attacks. According to the last editions of the ENISA threats landscape (2021a, 2022), public administration/government is the most affected sector by cyberthreats.

The most frequent cyberthreats during the period 2021-2022 are grouped into eight types (ENISA, 2022): ransomware, malware, social engineering, threats against data, threats against availability (i.e., denial of service), threats against availability (i.e., internet threats), disinformation or misinformation, supply chain attacks. These threats differ according to the specific motivations of attackers. **Monetisation** is the main reason for cybercrime groups; **geopolitics/espionage** aimed at gaining information (e.g., sensitive data, classified data) or **geopolitics/disruption** aimed at creating disservices are undertaken by state-sponsored groups; and **ideology** is behind the actions carried out by hacktivists. The objectives of cybercrime groups, state-sponsored groups and hacktivists are pursued quite uniformly through any type of existing cyberthreats, although **ransomware** is adopted for the sole motivation of monetisation.

[20] The precautionary principle is applied in the environmental domain (EC-DG ENV, 2017) and aims at ensuring a higher level of environmental protection through preventative decision-making in the case of risk.

It is therefore not surprising that, given the motivations behind the attacks, public authorities are a privileged target. LRAs in particular are victims of ransomware for monetisation. In 2019, according to Kaspersky experts, ransomware attacks shifted towards a new target: municipalities. In that year, the number of municipalities attacked by ransomware (174) increased by approximately 60% compared to 2018 (Securelist article dated 11/12/19). In addition, cases of LRAs attacked more than one time are not uncommon. Referring to section 1.1, **more than one quarter of the authorities participating in the consultation suffered from at least one cyber-attack with significant disruptive effects** in the last three years (i.e., from 2000 onwards). Out of these 17 LRAs, 13 are local authorities and, among them, two declare that they have been attacked more than 10 times.

3.5.2 Costs and expenses

The decision of a public authority to invest in digital resilience is negatively influenced by the lack of information about the cost caused by a digital incident with a significant disruptive effect. In addition, uncertainty concerning the level of digital resilience to be achieved as well as the expenses needed to maintain resilience over time may prevent public authorities from committing to investments that may result to be insufficient. If not investing in digital resilience, any local and regional authority in Europe (whatever the size) should be prepared to bear the recovery costs of digital incidents. It is common that LRAs having suffered an incident, after bearing the cost of their digital non-resilience, invest to avoid suffering the same impacts again (Box 3).

Box 3. Large impacts for small municipalities

The Municipality of Fara Novarese (Italy, 2,000 inhabitants) is part, together with two other small municipalities, of the *Unione Novarese* 2000, a grouping of municipalities sharing the provision of some public services to their communities. In June 2017, they were all targeted by a cyber-attack. The NotPetya malware affected the server of the *Unione* and, through the joint ICT network, the digital infrastructure of the three municipalities. Having informed the competent Italian authorities, the Municipality of Fara Novarese requested the support of an external private ICT company to assess the damage and restore operations. Access to most of the citizens' data in the Municipality's servers and computers remained denied, even after having involved another ICT company specialised in data recovery. The overall cost for external ICT support and for hardware replacement of the three municipalities was around €25,000. However, the highest impact related to data restoring. In the Municipality of Fara Novarese, for example, the database was fully operational again in November 2017. This required an extraordinary effort by the municipal staff who had to re-digitalise all the information archived on paper. At present, the municipality relies on the structural support of an external ICT company for its cybersecurity and stores citizens' data on two different cloud services, the Italian Single National Registry and the CloudPA of the Italian Agency

for Digitalisation (AGID). In 2022, to improve its digitalisation, the municipality applied for, and was granted, more than €150,000 from the NRRP.
Source: interview with a public servant from the Municipality of Fara Novarese (16/02/23).

Immediate evidence of costs borne by LRAs is provided in the case of attacks that are perpetrated through ransomware. A ransomware prevents users (e.g., public servants employed in the authority) from accessing their devices or locks files until a ransom is paid. The affected city or regional authority has to decide to either pay the ransom or lose the data needed to guarantee public services and, in addition, face the costs of restoring data and related services (EMSISOFT article dated 20/08/19). The ransom amount can be used as a rough proxy of the economic impact (EI) of the cost of digital non-resilience when the incident is a cyber-attack. According to Kaspersky experts, focusing on data of ransomware attacks targeting US municipalities (more than 170) from 2017 to 2019, the average ransom request was around $1 million. However, the ransom requests varied greatly between small and large authorities, with a 20 times multiplier factor (Securelist article dated 11/12/19). If the public authority opts not to pay, the recovery cost can also vary greatly (Gallagher webpage). It ranges from the cost of a few working days for the IT staff/consultants (e.g., to recover data from a back-up) to the cost of restoring digital infrastructures and of making data available again. The public authority's willingness to pay can be interpreted as a **sign of its condition of digital non-resilience**. In addition, the payment of the ransom can sometimes be more convenient than the costs incurred for the recovery. However, LRAs usually do not reveal if they have paid a ransom or not, so as not to signal their preference to pay and, in this way, attract more cyber criminals.

Nowadays, ransomware remains the preferred method of attack against government entities in the USA (KnowBe4, 2022). In the period 2018-2022, ransomware attacks against U.S. government organisations potentially impacted more than 230 million people and downtime costs were estimated at around $70 billion. The majority of these 330 ransomware attacks aimed at compromising the daily functioning of the authorities (e.g., stopping processes, interrupting services and causing disruption) and not at stealing data. In around 20% of the attacks, ransom amounts were revealed and ranged from $1,000 to $5.3 million. The total requested amount for these attacks was nearly $36.5 million. According to publicly disclosed information, cyber-criminals received payments from around one-third of the public authorities that declared to have received a ransom claim and the total amount paid was around $5 million (Comparitech article dated 9/11/22).

Still, the payment of the ransom in the case of cyber-attacks remains a widely debated topic. Payment offers no certainty concerning, for example, the unlocking of data and is therefore de-facto a reason to favour this type of crime. It is notable that while in the private sector the affected organisation is free to decide whether to pay or not, in the case of public authorities the issue is more sensitive (SecurityIntelligence article dated 10/10/19). For example, in 2021, the State of North Carolina approved a law that prevented government authorities from paying ransoms with the aim of discouraging this cybercrime (The National Review article dated 5/04/22).

In this context, the role of cybersecurity insurance is controversial. A regularly paid insurance premium is in some cases an option for those public authorities that cannot afford the structural investments to become digitally resilient. Cybersecurity insurance takes on part of the LRAs' risk. Insurance coverage helps to mitigate the economic and digital impact (EI and DI) of a ransomware attack, but LRAs remain exposed to social and reputational impacts (SI and RI) (Box 4).

Box 4. The active role of insurance companies in case of ransom

In May 2019, the Ryuk ransomware blocked the computer systems of the City of Riviera Beach (Florida, USA, 35,000 inhabitants) for three weeks. By clicking on a malicious link in an email, a city employee enabled the ransomware to spread through the city's IT network causing the shut-down of all computers. Among the impacts, disruptions were suffered in the systems controlling the water utility, in the city's communication system (e.g., emails and phone calls) and in the system recording 911 (emergency) calls. In addition, the official website of the city went down. The request for payment to unlock computers amounted to 65 Bitcoin (around $600,000). The city council voted unanimously to authorise its insurer to negotiate and pay the ransom. The attack raised the awareness of the members of the city council about the potential damage of cyber-attacks. The city was forced to replace a large part of its IT infrastructure, but it also started defining future digital investments. One week after the attack, the council authorised the purchase of 310 new desktops, 90 laptop computers and other hardware, for a cost of $941,000. More than one third of this amount was covered by the insurance company.
Sources: Threatpost news dated 20/06/19; The Palm Beach post news (no date).

However, the public disclosure of the information that an authority is covered by cybersecurity insurance can inform cybercrime actors **that this authority is more likely to pay the ransom than non-insured ones.** The interpretation of cybersecurity insurance as an 'incentive for cyber extortion attacks' should be carefully considered together with all the positive effects that insurance coverage can provide such as training of staff and support in incident response (Marsh webpage). In addition, in the case of ransomware attacks to LRAs, insurance companies have often taken an active role (either in the front-end or in the back-end) in negotiating the ransom with cybercrime actors and/or in interacting with ICT companies to recover the affected digital infrastructure (Box 5).

Box 5. The intermediary role of ICT companies in cases of ransom requests

On 21 June 2021, the **City of Liege** (Belgium, 190,000 inhabitants) suffered a Ryuk ransomware cyber-attack. The ransomware autonomously propagated itself in the municipality ICT network connecting 1,800 computers and in doing so it encrypted their hard disks. This affected the services related to civil status data such as appointment-making for birth, marriage and death registration. Immediately after the event, the city did not publicly disclose any information about potential data leakage and the amount of the ransom request. Key services were restored in less than two months and the overall cost to restore the ICT network and related services was assessed at about €1 million. Half of this amount was covered by the Ethias cyber-attack insurance to which the city subscribed. Unofficial sources report the payment of a ransom, in bitcoins, made by the ICT consultancy in charge of restoring the city's ICT network in order to obtain the encryption keys. The ransom was reportedly part of the overall assessed cost.
Sources: RTC news dated 22/06/21; l'avenir news dated 22/06/21; Le Soir news dated 30/11/21.

When ransomware attacks are perpetrated on LRAs, data breaches are a type of damage that immediately generates digital impact (DI) and economic impact (EI), but social impact (SI) and reputational impact (RI) may also follow subsequently (Box 6).

Box 6. The impact of non-adequate communication to the general public

On 21 July 2021, the Municipality of Thessaloniki, Greece (310,000 inhabitants in the municipality and 1 million in the metropolitan area), was attacked by the 'Grief' Ransomware Group that stole and locked some files stored in the city's servers. According to the recommendations of the national authorities, the Municipality interrupted all its services and online applications to allow a thorough proper investigation and to avoid additional spread of the virus. A ransom of €20 million was sought, but the Municipality refused to pay and effectively undertook three actions: it filed a lawsuit that allowed the e-crime prosecutor of Northern Greece to open an investigation; it initiated a close cooperation with the national Government, the Cyber Security Authority and the Personal Data Protection Authority to promptly face the consequences of the attack; and it activated a business continuity plan to gradually restore its services through the involvement of an ICT company (the company created a brand-new digital 'environment' with files not locked and with information from back-ups). Immediately after the attack, the representatives of the Municipality, including the deputy mayor in charge of eGovernment, guaranteed that stored data were secured (including through paper copies of documents) and that no leak of citizens' personal data had taken place. Unfortunately, three weeks after the attack, citizens' personal information and sensitive data such as names, tax identification numbers, addresses and debts to the municipality were posted on the dark web. This resulted in a demand for a public apology and the resignation of the deputy mayor in charge of eGovernment.
Sources: ekathimerini.com news dated 23/07/21; TechNadu news dated 27/07/21; Capital.gr news dated 23/07/21; GRTimes news dated 24/07/21; GRTimes news dated 25/07/21.

Finally, if proper notification and communication of data breaches are not made to the competent national authorities, administrative fines can represent an additional burden for LRAs, in line with the provisions of the GDPR (Regulation (EU) 2016/679).

3.5.3 Human resources and skills

The higher the digital and cybersecurity skills endowment of a public authority, the lower the cost of digital non-resilience. Prevention can be increased by investing in hiring ICTs specialists as well as in making public servants aware and digitally upskilled. For example, training of personnel on ransomware attacks using phishing or social engineering can reduce the likelihood of success of attacks. Investments in the structural support of ICT specialists (in-house or contracted) contribute both to preparedness (e.g., through the adoption of updated cybersecurity measures and tools) (Box 7) and response (e.g., by promptly reacting to/counteracting the attack) (Box 8).

Box 7. Public digital services require ICT expertise

Both in 2021 and 2022, the Municipality of Florence (Italy, 380,000 inhabitants) was at the top of the ICity Rank, an index measuring the digital transformation of the 108 main Italian towns. In recent years, the Municipality experienced a steep rise in the use of its public network and services, from 1.9 million accesses in 2019 to over 3.5 million in 2021. Online payments increased by 378% between 2020 and 2021. In order to keep pace with its digital transformation, the Municipality planned the hiring of 43 ICT experts over the period 2022-2024 and allocated €8.6 million from the REACT-EU funds for investments in network and big data infrastructures.
Sources: Municipality of Florence press releases dated 23/11/21 and 15/07/22.

Box 8. A prompt reaction driven by cybersecurity skills.

On 8 December 2022, the **Normandy Region** (France) was victim of a cyber-attack. The day after, the national authorities, the national agency for the security of information systems and the police services were contacted in order to file a complaint. With the support of an ICT company specialised in cyber-attacks, the regional department in charge of the authority's digital infrastructure started to characterise and analyse both the attack and its damage. To prevent the spread of contamination, all computers were disconnected. This included web access to the administrative services provided by the Region's offices located in the Municipality of Caen and in the Municipality of Rouen. The assessment of the damage implicated an analysis of the compromised ICT network as well as of its 600 servers and 1,500 computers. As an immediate recovery strategy, on the day after the attack, the Region's website was restored using a new address. This was also aimed at properly informing citizens of the incident and keeping them updated. Within 48 hours, more than 1,000 new computers were distributed to the authority's staff and in less than three days

new email addresses were created while the switchboards in the offices of the Region were restored within one week. Other services remained unavailable for a longer period.
Source: Normandie Region webpage accessed in February 2023.

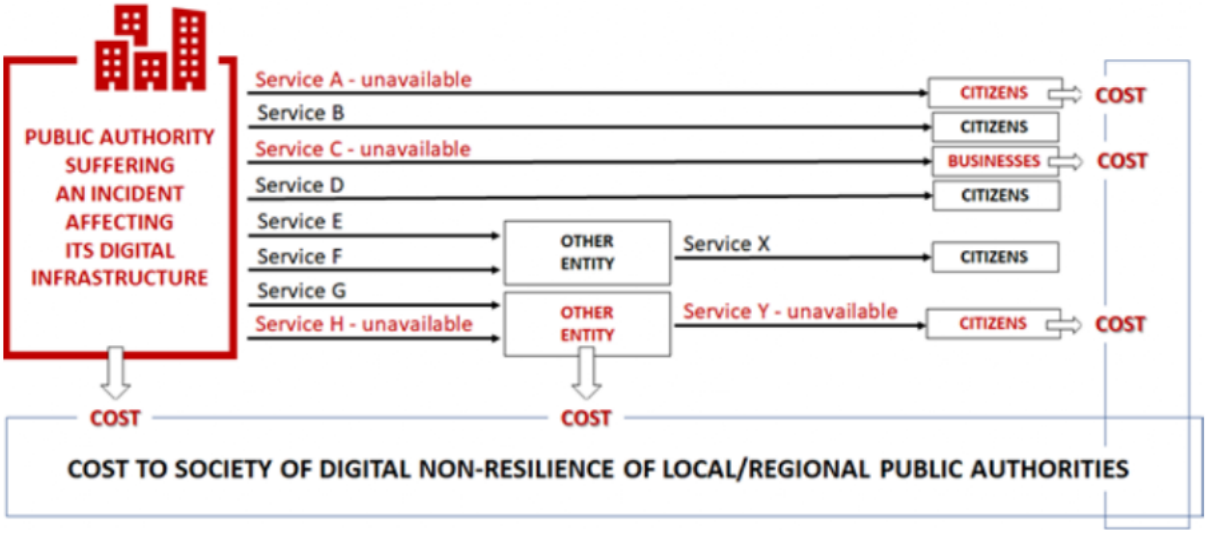
On the contrary, in case of digital incidents, lack of in-house or contracted expertise requires subcontracting, or requesting emergency support to restore digital infrastructure and recover public services, either to their pre-incident state or following a 'new normality'.

3.5.4 The constitutional role of the authority

The main actors impacted by the digital non-resilience of a local or regional authority are the authority itself, citizens and businesses. Even in critical situations, LRAs, as public administrations, should guarantee the services that address societal needs. European LRAs provide a large variety of services and some LRAs are also responsible, directly or indirectly, for services of general and/or of economic interests (SGIs and SGEIs, respectively)[21]. For this reason, citizens and businesses suffer from the interruption of the services directly provided by the authority, but also from the reduced functionality of other linked organisations/providers. Hence, digital incidents may disrupt eGovernment services, traditional services that nevertheless rely on the use of digital infrastructures (e.g., using citizens' data digitally stored) and other entities' services that depend on the regular service provision of the affected public authority. Due to these cascading effects, an LRA's digital non-resilience may generate a cost for the affected public authority, for the entities depending on its services and for citizens and businesses that suffer from both direct and indirect service disruption. This is the **societal cost of digital non-resilience of public authorities** (Figure 20)**.**

[21] Examples of SGIs include transport, postal services, water and gas supply, energy production and distribution, and waste disposal. Instead, SGEIs largely relate to critical infrastructures such as roads, energy grids, airports and ports as well as telecommunication infrastructure.

Figure 20. Dependencies contributing to the societal cost of digital non-resilience of public authorities



Source: figure created by the authors.

The societal cost of digital non-resilience of one public authority affects the community it serves, but a wider cost should not be excluded as connections exist between authorities within the same administrative level and between different administrative levels (not only in the same country). This situation may occur even if only one of the connected public authorities is digitally non-resilient (i.e., the weakest link aspect).

3.5.5 Politics and policies

One barrier to the digital resilience of LRAs in Europe is the fact that **investments in digital resilience are not yet considered to be a priority by a large number of local and regional policy-makers**. In fact, **the cost of digital non-resilience is the consequence of political decisions** because the dilemma between the two choices, to invest or not to invest in digital resilience, is not at the technical level.

Policies at a national and EU level support a more digitally resilient public administration at subnational level by means of two instruments: more suitable funding (Part 1) and increasing legal provisions that also touch upon LRAs (e.g., the GDPR, the Directive on the Resilience of Critical Entities, the NIS2 Directive and the Cyber Resilience Act). Financial incentives coupled with legal requirements may generate structural change supporting LRAs' digital resilience. In particular, with reference to the definition of digital resilience provided in the introduction of this study, legal requirements will improve those aspects on which LRAs have limited influence, namely the legislative framework and the external infrastructure necessary for the delivery of LRAs' services. In particular, Europe will reinforce its cybersecurity environment through the NIS2 Directive (Directive (EU) 2022/2555) and its systemic resilience through the CER Directive

(Directive (EU) 2022/2557). Both directives were published in December 2022 and are to be transposed by Member States by October 2024.

from the interviews *Experts' opinion on the impact of the NIS2 Directive on public authorities and LRAs in particular.*

The majority of the experts (80%) commented that the NIS2 Directive will affect the digital resilience of European LRAs. According to the Directive, national and regional authorities are obliged to put in place at least minimum measures to reduce cyber risks. Reporting obligations will also apply. One think tanks/academia expert commented that both national and regional authorities will need to make adaptations to comply with the EU-wide harmonisation that the Directive aims to achieve. An industry expert stressed the fact that legislation also imposing baseline standards on public authorities is positive per se, but that baseline standards as well as legislation need to be reviewed and updated in a timely manner; in addition, resilience is not achieved by default when a public authority is formally compliant. Another think tanks/academia expert commented that the Directive is relevant in making LRAs aware of the existing interconnections in a territory and of the need for more coordination among actors at local and regional level.

from the interviews *Experts' opinion on the impact of the CER Directive on public authorities and LRAs in particular.*

Only four experts (40%) commented that the CER Directive will affect the digital resilience of European LRAs. According to one of the experts, the digital resilience of European LRAs will improve thanks to the risk assessment requested from Member States to identify critical entities and assist those entities in meeting their resilience requirements. One think tanks/academia expert drew attention to the fact that, due to interdependencies between public authorities, systemic failures may also occur in cases of cyber-attacks targeting small public authorities that are digitally non-secure.

3.6 LRAs' digital resilience and the cost of digital non-resilience by 2030

The spread of crime in the digital world and the high frequency of extreme events will challenge European LRAs in the years to come. In addition, at a local and regional level, the effectiveness of the reinforced framing conditions combatting cyberthreats and supporting the resilience of essential services is still unclear.

The EC's resilience dashboards for the social and economic, green, digital, and geopolitical dimensions includes an assessment of the digital resilience of Member States based on indicators at the national level and defines an evaluation framework for understanding evolution over time (EC, 2021c). Indicators for digital resilience are grouped into four areas: digital for personal space, digital for industry, digitalisation of public space and cybersecurity. When considering indicators included in the **digitalisation of public space**, the public authority

perspective is taken into account mainly in terms of demand for public services (e.g., lack of online public services for businesses, people not having access to digital public services) and offer of public services that are provided by a limited number of LRAs (e.g., eHealth, judicial system e-tools). For **cybersecurity**, indicators provide an assessment from the perspective of citizens and businesses (e.g., cybersecurity incidents experienced by people, ICT security incidents in enterprises), but the public sector perspective is overlooked.

Although the above framework is not suitable to assess LRAs' digital resilience, it is significant because it relates to some of the 14 Megatrends affecting Europe outlined in the Megatrends Hub of the JRC. In particular, the digitalisation of public space is connected to '**Increasing the influence of new governing systems'** (Megatrend 12) and '**Accelerating technological change and hyperconnectivity'** (Megatrend 1), and cybersecurity is linked to '**Changing the security paradigm'** (Megatrend 4). As already considered in our '*Territorial foresight study in addressing the digital divide and promoting digital cohesion* (CoR, 2022), when moving to the subnational level, Megatrend 12 related to potential new geopolitical dynamics in the world loses relevance. Instead, Megatrend 1 implies an overall acceleration of digitalisation in general and of public administration in particular, and Megatrend 4 concerns the increase in new security threats, especially in the digital world. As the digitalisation of public administration implies higher exposure to digital incidents than in the past (especially if 'not controlled' through digital resilience), the concurrent reinforcement of these two megatrends in Europe may lead to high cost of digital non-resilience at subnational level in the near future.

Within this study, an investigation of the potential evolution of digital resilience of LRAs is carried out by means of **two foresight exercises**, developed out of the input from the ten interviewed experts (see Box 1). During the interview, each expert was involved in two challenging sets of questions in order **to understand the evolution of European LRAs' digital resilience by 2030**. The first set relates to the most likely situation in terms of digital resilience of European LRAs by considering the increasing challenge of cyber-attacks (i.e., connected to Megatrend 4) and given the change of the framing conditions 'guided' by the EU (e.g., related to the forthcoming transposition of the NIS2 and CER directives by the end of 2024). The second set relates to the unexpected. Experts were asked to assess the likelihood of digital-related wild cards and their potential impact on the digital resilience of LRAs. Answers from the experts were used to build two foresight exercises.

3.6.1 Foresight exercise 1: which are the possible scenarios for LRAs' digital resilience?

The experts were asked to select the most likely situation of LRAs' digital resilience in 2025 and in 2030. Six given situations[22] were proposed or, alternatively, the experts could propose another situation, if deemed more likely than the given ones, and add any relevant comment. The experts' opinions on the given situations led to the identification of **five scenarios** combining the expected state of LRAs' digital resilience in 2025 with its evolution in 2030:

Scenario 0	The state of the art is persisting
Scenario 1	'The smallest' are lagging behind in digital resilience
Scenario 2	A part of Europe is becoming digitally resilient through a top-down approach.
Scenario 3	Territorial cooperation is contributing to the creation of ecosystems for digital resilience
Scenario 4	Europe is acting to achieve digital resilience at all administrative levels

Scenario 0. The state of the art is persisting.

In this scenario, the digital resilience of LRAs **in 2025** will be more or less the same as today. An increasing digitalisation of the public administration across Europe will continue to be regularly threatened by cyber-attacks (and importantly exposed to damage caused by natural disasters). **In 2030,** as outcomes of investments made, two main situations may occur: 1) the situation will remain more or less unchanged because of the uneven distribution of funds among LRAs, or because funds are not sufficient to achieve a certain level of digital resilience; 2) the situation will improve but not evenly across LRAs or the EU. The disparity will be particularly evident between regional and local authorities. With the exclusion of some front-runners (pushed by technical or political leaders informed about the consequences of cyberthreats), awareness-raising in small municipalities about the relevance of digital resilience and the related cost of digital non-resilience will continue to be limited. There may be disparity at a

[22] The six given situations are: 1. The majority of LRAs in the EU27 are digitally resilient; 2. Digital resilience is achieved by the majority of LRAs in only a limited number of Member States; 3.The majority of the regional public authorities and the largest urban authorities in the EU27 are digitally resilient, but most of the smallest local public authorities (e.g., towns, villages) lag behind; 4. In almost all the Member States, national authorities provide ad-hoc solutions that make LRAs digitally resilient; 5. In a limited number of Member States, national authorities provide ad-hoc solutions that make LRAs digitally resilient; 6. European authorities provide ad-hoc solutions that make LRAs digitally resilient across the EU.

geographical level if in some Members States, national authorities actively intervene to provide ad-hoc solutions to make their LRAs digitally resilient. In addition, this scenario implies that the issue of LRAs' digital resilience is not explicitly addressed in EU policy debates related to cybersecurity and resilience. In 2030, most of the European LRAs will be exposed to the cost of digital non-resilience due to lack of adequate guidance in terms of awareness-raising and/or support through ad-hoc funds.

Scenario 1. 'The smallest' are lagging behind in digital resilience.

Here, the majority of the regional public authorities and the largest urban authorities in the EU27 will be digitally resilient **in 2025**, but most of the smallest local public authorities (e.g., towns, villages) lag behind. The progress of European LRAs in terms of digital resilience will depend on their size. The difficulties faced by local and especially rural municipalities to keep pace with digitalisation are also linked to their lack of adequate infrastructure for connectivity (e.g., 5G). **In 2030,** the smallest local public authorities will continue to lag behind, but thanks to current investments in broadband and the availability of funding for digital transformation, improvement in smaller administrations is also expected. However, an effort to 'digitally educate' local authorities will remain a pre-condition for achieving a certain level of digital resilience. Cooperation between the various administrative levels will also be needed to reduce the gap experienced by local authorities. This scenario does not exclude the possibility of a two-speed progression across EU countries leading to the achievement of digital resilience by the majority of LRAs in only a limited number of Member States. This will contribute to an increase in the digital divide among public administrations within Europe. In 2030, the cost of digital non-resilience will remain primarily a concern for (small) local authorities with some possible differences persisting between Member States.

Scenario 2. A part of Europe is becoming digitally resilient through a top-down approach.

This scenario indicates that in a limited number of Member States, national authorities provide ad-hoc solutions that make LRAs digitally resilient **in 2025**. However, as there is a different 'digital culture' across EU countries, structural change will take time and, **in 2030**, the situation is likely to be the same as in 2025, with policies (e.g., incentives/legal provisions) that facilitate the achievement of digital resilience by LRAs in some Members States while in other EU countries LRAs' digital resilience lags behind. In 2030, the cost of digital non-resilience primarily will concern the LRAs of some Member States only.

Scenario 3. Territorial cooperation is contributing to the creation of ecosystems for digital resilience.

This scenario says that the majority of LRAs in the EU27 will be digitally resilient **in both 2025 and 2030**. Regional authorities will progress faster towards the achievement of digital transformation and digital resilience. They will be in the position to integrate national initiatives with actions supporting the digital transformation process of local authorities across territories. Regional authorities will act as aggregators/facilitators supporting local authorities in optimising specific administrative processes and improving the overall efficiency of the public administration. This will lead to ecosystems for digital resilience at the territorial level. Systemic digital resilience will also be pursued through, for example, the support of regional authorities in fostering the use of emerging technologies and the pooling of resources by local authorities. In 2030, the cost of digital non-resilience will concern only a minority of LRAs in Europe, i.e., those that do not belong to digitally resilient territorial ecosystems.

Scenario 4. Europe is acting to achieve digital resilience at all administrative levels.

In this scenario, ad-hoc solutions provided by European authorities will make LRAs digitally resilient across the EU **in 2025**. **Until 2030**, national authorities may take an intermediary role to facilitate the transfer of these solutions to the regional and local level. This will lead to a Europe-wide ecosystem for digital resilience. In 2030, the cost of digital non-resilience will primarily concern those (few) European LRAs either not adopting these solutions or experiencing a delay in implementing them. Europe will aspire to become a digitally resilient ecosystem.

According to the experts, **Scenario 1 (*'The smallest' are lagging behind*) is the most likely to occur** in the next few years taking into account the ongoing digitalisation process of public administrations accompanied by EU provisions that promote the cybersecurity and resilience of critical entities. Although the smallest local authorities are gradually closing the gap in terms of digital resilience, the societal cost of being digitally non-resilient in the upcoming years could be dramatic for all citizens and businesses served by such authorities. This opens up opportunities for the adoption of ad-hoc policies at EU and national level to foster not only digital transformation but also the achievement of a certain level of digital resilience in the smallest local authorities.

3.6.2 Foresight exercise 2: what can disrupt LRAs' progress towards the achievement of digital resilience by 2030?

Unexpected or unlikely large-scale events can radically affect megatrends and, in turn, impact the realisation of possible future scenarios. Wild cards (i.e., events with a low probability of occurrence and a high impact) are consequences of past weak signals, which were ignored or not adequately taken into account. For this foresight exercise, the experts were asked to assess the likelihood of four digital-related wild cards **by 2030** and their negative impact on the achievement of European LRAs' digital resilience[23] (Figure 21).

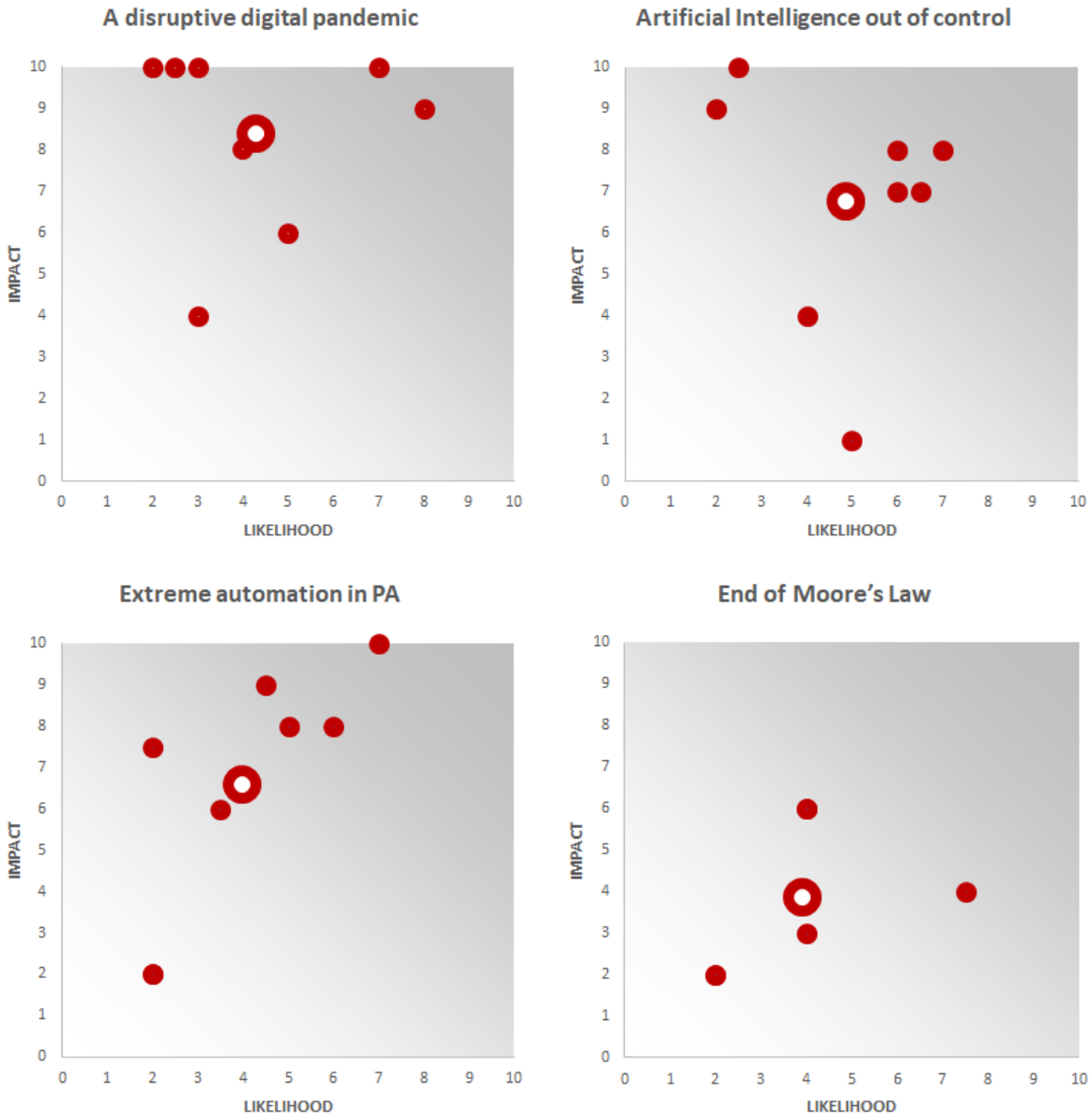
Only eight experts took part in this exercise. The proposed wild cards were selected from among those that were indicated to be most relevant for digital cohesion in a previous forecast exercise (CoR, 2022): i) *a disruptive digital pandemic – a super virus collapses the internet*; ii) *Artificial Intelligence out of control – public and private services almost unavailable for weeks*; iii) *extreme automation in public administration – a crisis of confidence in justice and rule of law*; and iv) *the end of Moore's Law – physical constraints prevent additional developments of digital technologies*.

According to the experts' answers, on average, the highest impact would be generated by ***a disruptive digital pandemic*** (score of 8.4). Four experts rated as '10' its impact on LRAs' digital resilience. One expert defined the occurrence of a digital pandemic as 'catastrophic' for public authorities. *A disruptive digital pandemic* is also perceived as quite likely to occur (score of 4.3). Those experts rating its occurrence with a very low likelihood (score of 2.0) believe that the internet will be less prone to disruptions in the future than it is now.

Artificial intelligence out of control is perceived as the wild card with the highest likelihood of occurring although its average score is rather low (4.9). One industry expert highlighted that this is something that might well occur, not because AI becomes fully out of control itself, but rather because the logic of automated algorithms may generate continuous repetitive behaviours that might overwhelm IT systems and prevent their regular functioning. However, another expert from the public sector stressed that, at the EU level, the AI Act is trying to set rules to avoid these digital incidents and strengthen confidence in the opportunities offered by AI.

[23] The requested assessment of likelihood of each wild card was from 1 = very low likelihood, to 10 = very high likelihood; the assessment of their impact was from 1 = very low impact, to 10 = very high impact.

Figure 21. Experts' assessment of likelihood and impact of each wild card



Notes: the average value is represented by the big empty dot in each figure; the charts on 'Extreme automation in PA' and 'End of Moore's law' show fewer dots because some of them overlap.
Source: figure elaborated by the authors.

On average, the likelihood of occurring and the impact on LRAs' digital resilience of the wild card ***Extreme automation in PA*** are similar to the ones of *Artificial intelligence out of control.* The expert (from industry) scoring 10 to the impact of this wild card highlighted that huge consequences will be suffered by public authorities, but the more significant consequences will be at the expense of society as a whole. Another industry expert highlighted that in rural areas and in small municipalities, where human interaction in the provision of public services is still key, the impact of *extreme automation in PA* would exacerbate the lack of

confidence in justice and in the rule of law, hindering the digital resilience process of the public authorities.

The ***End of Moore's Law*** is the wild card with the lowest likelihood and impact on the achievement of LRAs' digital resilience (on average, the score is 3.9 for both). One industry expert stressed that, even if it does happen, the result will be a slowdown in technologies development without significant impact.

In summary, when focusing on the achievement of LRAs' digital resilience by 2030, this foresight exercise indicates that *a disruptive digital pandemic* should be considered a wild card with an impact that goes well beyond the consequences of the disruption of LRAs' digital services. If such a wild card occurs, digital resilience will be a world-wide concern. LRAs will only be one of the stakeholders suffering the cost of this event. The *end of Moore's Law* will have a limited impact. An indirect consequence could be the rise in price of some technologies preventing LRAs from investing adequately in digital resilience.

Instead, weak signals behind the wild cards related to *Artificial Intelligence out of control* and *Extreme automation in public administration* **merit the attention of policy-makers**, especially at the EU level, to facilitate the achievement of digital resilience by LRAs by 2030. In fact, the societal cost of LRAs' digital non-resilience would be largely amplified by the occurrence of these two wild cards.

Part 4. From digital threats to digital resilience: conclusions and recommendations

Results from the online consultation with European LRAs, insights from the experts' interviews and findings from desk research, including the case studies in Part 2, confirm that digital resilience across European LRAs varies widely. Some public authorities are actively pursuing and consolidating their digital resilience for years; some others evidently lag behind, or have difficulties in embarking on a path to digital resilience because of lack of funds and/or capacities; and yet others have low or no awareness of the need to become digitally resilient. Against this heterogeneous landscape across Europe, **recommendations follow the steps of a theoretical path towards 'a reasonable level' of European LRAs' digital resilience**. These steps should be undertaken through interventions by a number of actors.

Step 1. Political awareness to go for digital resilience

The awareness of political leaders reflects the will of municipal or regional councils to become digitally resilient. **Political will is a pre-condition for digital resilience to be achieved** by a public authority.

Recommendation # 1.1

Member States and the EC, with the support of ENISA, should consider running **awareness-raising campaigns addressed at the political representatives of cities and regions**. These campaigns might, for example, show the different types of impact of digital non-resilience on public administrations, i.e., the economic, digital, social, reputational and physical impacts. The European Cybersecurity Month to be held in October 2023 could include activities and events specifically targeted at LRAs.

In the consultation, it became apparent that local authorities consider the lack of awareness at the top-level management to be the second most important obstacle to increasing their digital resilience, while for regional authorities it is less of a concern. These findings are in line with the experts' opinions that regional authorities prioritise digital resilience more than local authorities.

Notably, the online consultation also highlights that those LRAs having suffered an incident with a significant disruptive effect start, afterwards, to structurally invest in digital resilience. This evidence is also confirmed by the examples of LRAs, victims of cyber-attacks, included in Part 3.

Recommendation # 1.2

The European Committee of the Regions should consider **facilitating the exchange of experiences between municipalities**, possibly in partnership with leaders of big and small cities who actively pursue digital resilience because of their political vision, or because their administration already suffered from cyber-attacks. The digital resilience of local and regional authorities could be proposed as one of the themes of the 2024 European Week of Regions and Cities. The timing of this would be ideal as October 2024 is when the NIS2 Directive and the CER Directive are to be transposed into national laws.

The most likely scenario in one of the foresight exercises predicts that the smallest authorities will lag behind in 2030 with respect to digital resilience, at least in some EU countries. Policies addressed at a local level are needed now, in order that small administrations do not get left behind. The digital resilience of public administrations within countries and between EU countries also contributes to digital cohesion.

Recommendation # 1.3

The European Committee of the Regions should put **digital resilience of local and regional authorities high on its political agenda**. Taking into account the increasing frequency of cyber-attacks focussing on local and regional authorities and the upcoming legislative requirements on cybersecurity and resilience to which some LRAs must comply, the timing for this is ideal. The cost of digital non-resilience of local authorities is a key topic that may be raised in the participative exercise coordinated by the EC for the preparation of the annual EU strategic foresight report. This deserves particular attention when megatrends and scenarios by 2030 are defined.

The political decision-making process must be grounded on a robust knowledge base. The understanding of the monetary costs involved in digital non-resilience is a necessary pre-condition for LRAs to pursue digital resilience. As made evident by the findings from the experts' interviews, there are no standard methods for LRAs to quantify damage, assess the impacts and evaluate the cost of digital non-resilience, especially those caused by cyber-attacks.

Recommendation # 1.4

ENISA, in collaboration with the EC and Member States, should define and suggest **ad-hoc methods for LRAs to assess their cyber risks, their vulnerabilities and potential impacts of digital incidents** as well as to estimate the cost that may be the consequence of cyber-attacks. The ambition should be to **create reference guidelines** for European LRAs in line with the risk assessment practices carried out by insurance companies to define insurance premiums, or with the conformity checks made by standardisation bodies to release certifications.

A common EU position could be considered with regards to ransom payments, drawing on the experience of the USA, where the spreading of hackers specialised in crime against local authorities for monetary purposes led more than one federal state to impose the non-payment of ransoms by public authorities. Awareness of political leaders on the potential societal cost of digital non-resilience may also lead, in the mid-term, to a change in the legislative framework on cybersecurity and cyber resilience (i.e., the first component in the digital resilience definition).

Recommendation # 1.5

EU institutions and Member States should consider **debating the possibility of reducing the propagation of cybercrime motivated by monetisation, including through the obligation on public authorities of non-payment of ransoms sought**.

Step 2. Definition of the governance model for digital resilience

Once awareness on the relevance of digital resilience is raised at the political level, subsequent decisions depend on the actual digital layer of the public authority, i.e., its digital infrastructures and digital and cybersecurity skills. This will require that an **inventory of the attack surface or 'digital footprint'** be made. Information on **vulnerabilities to digital incidents and the identification of the corresponding risks** serve, both at the political and operational/technical levels, to define the most suitable and feasible approach to digital resilience and the investments needed to achieve a 'reasonable' level of digital resilience.

The evidence collected within this study shows that the type of cybersecurity management in a public authority strictly depends on its size. Public authorities with over 10,000 employees tend to rely on a dedicated department/office in charge of cybersecurity. This department/office may take full responsibility for cybersecurity or may be supported by external ICT services. Conversely, the

smaller a public authority is, the fewer staff they are likely to have in charge of cybersecurity. The consultation shows that among LRAs with less than 100 employees, the most common form of cybersecurity management is an individual who is in charge of cybersecurity but also has other functions. Departments or task forces dedicated to cybersecurity are more likely to have a dedicated budget.

From the findings of the case studies, we identified at least **five different governance models for digital resilience** derived from the cybersecurity management approaches adopted by LRAs. The first of these models is kick-started by the first component of digital resilience, i.e., compliance with the legislative framework. The other models are more mature and address all the components of digital resilience (i.e., legislative framework, digital infrastructures and skills).

The minimum level model. In this model, a certain level of digital resilience is pursued because funding opportunities for cybersecurity suddenly arise, or because there is an urgent need to comply with specific law provisions. This model is unstructured and driven by one-shot incentives. The case of the Lazio Region, for example, shows how the funding made available through the NRRP became an incentive to prepare a regional digital strategy and to design cybersecurity projects to access RRF's resources. This model allows LRAs to reach **a minimum level of digital resilience that gets closer to the legal requirements** set by EU or national governments. Thus, it may represent an **entry point** onto a path to digital resilience for those public authorities that are lagging behind. It may remain unstructured over time (with the risk for the authority of falling back under a minimum level of digital resilience), or transform into a more structured model. On the leverage effect of legislation, evidence shows that, already in 2016, several LRAs started pursuing compliance with GDPR provisions and that this incentive later led to the certification of their information management systems according to ISO 27001 standards. The Danish case is exemplary in this sense, but the case of the Municipality of Amadora also provides good insights on the leverage effect of the GDPR. De-facto, provisions such as those that are expected to be imposed by the Cyber Resilience Act will also bring European LRAs closer to a 'reasonable' level of digital resilience through the procurement of digitally resilient goods and services.

Recommendation # 2.1

Member States, with the support of their national entities in charge of cybersecurity, should consider **developing a compliance monitoring system** to understand the level of uptake of the legislative provisions on cybersecurity and cyber resilience across regional and local administrations. The aim should

be supportive as opposed to disciplinary, so as to encourage administrations lagging behind and thereby reduce the number of 'the weakest links'.

The progressive model. In this model, digital resilience is pursued gradually, mainly **through own resources**. This model may be initiated by a single specific action, or project, and then developed further as initiatives multiply. Although they each have distinguishing features, three of the cases in Part 2 reflect this model and relate to small- and medium-sized cities (from 100,000 to 500,000 inhabitants): Amadora, Rijeka and Vilnius. Common characteristics across the three cases include the **focus given to the human factor (awareness-raising and training of public servants) and the political endorsement** of cybersecurity initiatives.

Recommendation # 2.2

The European Committee of the Regions, in agreement with the EC, should consider **creating an award for small- and medium-sized local authorities that have independently but successfully pursued their digital resilience.** It would be a **'preferential mark'** if and when these authorities apply for EU funds. This would allow these cities to increase their competitiveness in open calls and to access funds that may help to consolidate their path to digital resilience.

The centralised model. In this model, cybersecurity task forces are built within the public authority. The case of the capital city of Berlin is exemplary for this model. This model involves making **significant investments** as well as ensuring **high levels of centralisation of budget decisions and standardisation of ICT solutions** across the public administration. A peculiar feature of this model is the **in-house availability of ICT expertise**, the lack of which the consultation indicates as an important obstacle to increasing LRAs' digital resilience (the second most important obstacle for local authorities). In this context, Berlin developed a sustainable system by including an educational branch within its cybersecurity task force (the ITDZ-Berlin). This branch educates and trains specialists who may subsequently be employed in the task force.

Recommendation # 2.3

Regions and large cities should **adopt innovative approaches to meet the increasing demand for ICT specialists within the public sector**. As competition for qualified ICT expertise grows, initiatives to attract and retain skilled ICT staff are needed. In addition, digital skilling and up-skilling of staff in large cities and regions could be undertaken in cooperation with training or

education institutions, or through in-house learning arrangements aimed at building-up ad-hoc ICT professionals for the public administration.

The externally supported model. In this model, digital resilience is pursued by the public authority through structural collaboration with external service providers. The case of the Hague is exemplary for this model, that has two peculiar features: the **identification of the service provider(s)** and **the reorganisation of roles and functions within the public authority**. The complexity of the organisational structure is one of the two main obstacles to increasing digital resilience indicated by regional authorities in the consultation. If re-organisation is not feasible, the externally supported model becomes a **delegated model** where cybersecurity is totally outsourced. The delegated model entails a transfer of responsibilities to third parties and the only implications for the public authority are monetary ones (in the case studies, we chose not to include LRAs with this type of arrangement). The delegated model is a result of structural conditions that do not justify in-house structural investments. This model is likely to be adopted by small municipalities.

Recommendation # 2.4

Member States and regional authorities should facilitate municipalities in the **identification of qualified ICT service providers**. A directory/catalogue of accredited cybersecurity service providers for the public sector, by type of operation area, might facilitate local authorities in identifying and mobilising support if needs arise, including in the event of cyber-attacks.

The ecosystem model. Digital resilience in this model is pursued concurrently with other stakeholders in a whole-of-the-system approach. The case of Brittany is exemplary for this model. Brittany has implemented a territorial approach to cybersecurity that is framed by its smart specialisation strategy. Within the strategy, **national and regional actors** take responsibility for the **joint funding and implementation** of a wide range of activities touching upon research, innovation, training and technology development in the cybersecurity domain. This model relies on **multi-level cooperation among public administrations** and also, importantly, involves the **private sector**. In the consultation, multi-level cooperation was the most selected option by LRAs in specifying what is needed to enhance their digital resilience.

Suggestions related to this model are reported under step 4 ‘Creation of links with the surrounding environment’.

Step 3. Choice of investment strategy and identification of funding sources for digital resilience

After the identification of the governance model, the next steps relate to the **identification of the areas in which to invest** and of the **funds to be used for such investments**. The definition of digital resilience provided in the introduction of this study points to two relevant investment areas for LRAs: digital infrastructures and digital/cybersecurity skills. In general, investments for digital resilience target prevention, preparedness and reaction. When investments relate to LRAs' digital infrastructures, digital resilience is enforced through prevention. Innovative digital tools such as 'digital sandboxes' offer a safe environment between cybercrime actors and LRAs' staff. In these safe environments, suspicious files are carefully examined before accessing the main network and information system.

Recommendation # 3.1

Among their investments in prevention, LRAs should consider the **use of innovative digital tools such as the 'digital sandboxes'**. These tools reduce the vulnerability of their infrastructures to cyberthreats by creating a buffer zone around the digital layer of the authority.

Preparedness and response capacity (i.e., reaction) are enforced through investments in digital/cybersecurity skills, the second key investment areas for LRAs. Improvements within LRAs may, for example, relate to staff awareness-raising, test and detection of the reaction capacities of ICT specialists, or proofing of a decisional readiness mechanism.

Recommendation # 3.2

National entities in charge of cybersecurity in EU Member States and ENISA should organise **multi-stakeholder cybersecurity exercises** where LRAs' procedures to resist, react and recover as a result of a digital incident are tested at a local or regional level, or across different administrative levels where a cooperative approach is envisaged. In addition to these exercises, one of the forthcoming editions of Cyber Europe may focus on the active involvement of LRAs testing digital incidents that affect the interruption of public service provision.

As already extensively discussed in Part 1, **the lack of availability of funds for investing in digital resilience is a significant obstacle for LRAs**. Access to national and European funds seems particularly difficult for local authorities. Indeed, as highlighted during the interviews, LRAs' accessibility to specific funds

varies depending on factors such as the size of the public authority, the investments that need to be taken and the competencies requested to make projects operational. To facilitate the channelling of resources to lower administrative levels, digital solutions and technologies as well as services that could be of use at subnational level to pursue digital resilience, could be purchased centrally. This centralised purchase of goods and services to the benefit of lower administrative levels could follow a call for projects.

Recommendation # 3.3

Member States supported by their national entities in charge of cybersecurity should **act centrally to launch calls for projects related to the development and uptake of innovative cybersecurity solutions at the level of local public administrations**.

As shown by case studies and by the results of the online consultation, a multi-source approach is the most common funding approach used by LRAs to pursue digital resilience. Not all LRAs have dedicated offices searching for funding opportunities and, eventually, applying for funds.

Recommendation # 3.4

Member States, supported by their national entities in charge of cybersecurity and by the European Digital Innovation Hubs located in the country, should support LRAs in the **identification of funding opportunities available for enhancing digital resilience**. A constantly updated mapping of these opportunities may guide LRAs to find an effective mixture of resources to progress towards digital resilience.

As shown in one of the foresight exercises, large-scale impact and unlikely events (nowadays only signalled by weak signals) such as *Artificial Intelligence out of control* and *Extreme automation in public administration* may significantly affect LRAs' progress towards the achievement of a certain level of digital resilience in the future years. LRAs should be prepared for today's threats and for future challenges.

Recommendation # 3.5

The EU should consider **addressing future challenges of digital resilience through the launch of specific calls under suitable funding programmes** such as the Digital Europe Programme and Horizon Europe (e.g., innovation actions or coordination and support actions in work programmes 2025-2027).

Calls should focus on current and future needs of LRAs with respect to digital resilience and should require LRAs' active involvement, not only as test beds, but also as implementers in identifying and adopting innovative solutions and practices for digital resilience.

Step 4. Creation of links with the surrounding environment

Multi-level cooperation is the type of support that is most in demand in the online consultation. Three-quarters of the participating local and regional authorities consider it the best way to enhance their digital resilience. In some EU countries, multi-level cooperation for cybersecurity is culturally embedded in policy-making (e.g., the case of Denmark). However, the Brittany case shows how cybersecurity may become an all-encompassing ecosystem by including it in its regional smart specialisation strategy.

Recommendation # 4.1

The cybersecurity market, with its expected growth, is an enabler of economic and social development. The EC, regional authorities, the Joint Research Centre and European Digital Innovation Hubs (EDIHs) could consider supporting a follow up of the 'Cybersecurity Smart Regions' partnership by facilitating **the development of cybersecurity ecosystems** in all those European regions sufficiently endowed with cybersecurity industry, innovative start-ups, research and academia. This would generate positive externalities for municipalities belonging to the ecosystem.

The mandate of European Digital Innovation Hubs also envisages the provision of support to public administrations as well as the facilitation of knowledge transfer of the most advanced digital technologies and solutions.

Recommendation # 4.2

European Digital Innovation Hubs (EDIHs) should facilitate **the pooling of resources across municipalities of their regions to enhance cybersecurity aspects** such as awareness-raising, secure use of innovative digital instruments and technologies (i.e., artificial intelligence, blockchains) and cross-exchange of knowledge on solutions increasing digital resilience.

The existing links between the green and the digital transitions highlight how they reinforce each other. In particular, we highlighted the contribution of advanced digital technologies to the protection of critical infrastructures and critical entities. Digital technologies may also offer situational intelligence in warning and

response systems and support recovery from disasters. As stressed by both the CER and the NIS2 Directives, the digital dimension is associated with the **functioning and continuity of systems which are vital for society**. As such, **the digital dimension and its resilience contribute to territorial safety** and should be an integral part of emergency management.

As is the case in other domains, where synergies create economies of scale and scope, or multiply the benefits, a silo approach to digital resilience is less effective than a more holistic approach.

Recommendation # 4.3

Regional authorities should coordinate the inclusion of **digital resilience as a dimension of territorial resilience**. Cyber-attacks with significant disruptive effects for LRAs' digital infrastructures as well as for critical infrastructures and entities should be considered to be as important as natural and anthropic disasters. Digital incidents could be included in emergency planning, disaster management and post-disaster recovery at the territorial level.

The inclusion of digital resilience as a dimension of territorial resilience across Europe mirrors the inclusion of digital cohesion as a component of territorial cohesion as elaborated in a previous study (CoR, 2022).

Annex I Bibliography

Abgeordnetenhaus Berlin (2022), *Schriftliche Anfrage des Abgeordneten Christopher Förster (CDU) zum Thema: Security Observations Center*, 19.Wahlperiode.

Agenzia per la cybersicurezza nazionale - ACN (2023), *Allegato A - Graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziabili & Allegato B - Graduatoria definitiva delle proposte progettuali ammesse e parzialmente finanziabili*.

Anderson J. (2022), *Europe Needs High-Tech Talent*, Foundation for European Progressive Studies.

Association pour l'emploi des cadres (2017), *Cybersecurity in Brittany: focus on expertise - Summary*, Les Études de L´Emploi Cadre, No. 25/2017, June 2017.

Balgaranov D. (2022), *Berlin opens a cyber-security centre to protect against increasing attacks*, published on The Mayor.eu.

Brittany Regional Council (2016), Deliberation, *La Bretagne, Cyber valley européenne*, 13 octobre 2016, n°16_DGS_04.

Brittany Regional Council (2022), Deliberation, *Coopérer pour fédérer l'écosystème breton de la cybersécurité*, 24, 25 et 26 février 2022, n°22_DGS_02.

Committee of the Regions (2022), *Territorial foresight study in addressing the digital divide and promoting digital cohesion*, 4 July 2022.

COMPACT (2019), *D6.8 Best Practices and guidelines for immediate adoption by local PA – Deliverable of the H2020 project COMPACT*.

Copenhagen Post, 2020, *Cyber-attack on public computers results in significant data breach*, article by Luke Roberts dated 8 September 2020.

Courtney C. (2020), *Countering hybrid threats: the vital need for digital resilience*, Friends of Europe.

Danish Agency for Digital Government - DIGST (2018), *The Danish National Strategy for Cyber and Information Security 2018-21*.

Danish Center for Cyber Security - DCCS (2015), *The Danish Cyber and Information Security Strategy*.

Danish Regions, *Joint Regional Information Security Policy*, 2017.

Digital Cities Challenge (2019), *Digital Transformation Strategy of for the city Rijeka - Digital RiWave*, July 2019.

DigitalEurope (2023), *The digital front line. 15 actions to boost Europe's Digital Resilience*.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

Eisenhardt K. (1989), Building theories from case study research, The Academy of Management Review, pp 532 - 550.

ENISA (2021), *Addressing the EU Cybersecurity Skills shortage and gap through higher education*, November 2021.

ENISA (2021a), *ENISA Threat Landscape 2021* (April 2020 to mid-July 2021), October 2021.

ENISA (2022), *ENISA Threat Landscape 2022* (July 2021 to July 2022), October 2022.

European Commission (2019), *The Digital Cities Challenge - Designing Digital Transformation Strategies for EU Cities in the 21st Century*, Final Report carried out by Technopolis Group and Carsa, 19 July 2019.

European Commission (2021), *A cybersecure digital transformation in a complex threat environment* - Brochure, 28 January 2021.

European Commission (2021a), *Annex to the Commission Implementing Decision on the financing of the Connecting Europe Facility – Digital sector and the adoption of the multiannual work programme for 2021-2025*, C(2021) 9463 final, Brussels, 16.12.2021.

European Commission (2021b), *Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021-2022*, C(2021) 7914, Brussels, 10.11.2021.

European Commission (2021c), *Resilience dashboards for the social and economic, green, digital, and geopolitical dimensions*, 29 November 2021.

European Commission (2022a), Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final, Brussels, 15.9.2022.

European Commission (2022b), Report from the Commission to the European Parliament and the Council, *Review report on the implementation of the Recovery and Resilience Facility*, COM(2022) 383 final, Brussels, 29.7.2022.

European Commission (2022c), *Digital Economy and Society Index (DESI) – Denmark*, accessed in January 2023 from: *https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance*.

European Commission (2022d), *Digital Economy and Society Index (DESI) – The Netherlands*, accessed in January 2023 from: *https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance*.

European Commission (2022e), Communication from the Commission to the European Parliament and the Council on *2022 Strategic Foresight Report*, COM(2022) 289 final, Brussels, 29.6.2022.

European Commission, Directorate-General for Environment (2017), *The precautionary principle: decision-making under uncertainty*.

European Commission-Directorate-General for Informatics (DIGIT) (2022), *Digital path to recovery and resilience in the European Union*, study carried out by Wavestone.

European Cyber Security Organisation (2019), *ECSO Position Paper on the role of the regions in strengthening the European Union's cyber security*.

European Parliamentary Research Service (2022), *The NIS2 Directive: A high common level of cybersecurity in the EU*, Briefing 08-02-2023.

European Policy Centre (2021), *National Recovery and Resilience Plans: Empowering the green and digital transitions?*, discussion paper, April 2021.

George, M., O'Regan, K. and Holst, A. (2022), *Digital solutions can reduce global emissions by up to 20%. Here's how,* web article dated 23.05.22 accessed in February 2023, part of the 'World Economic Forum Annual Meeting'.

Government of Lithuania (2021), *Lietuvos Respublikos Krašto Apsaugos Ministro įsakymas 'Dėl nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašo patvirtinimo'*, (No, v-484), 9 July 2021, Vilnius, Lithuania.

Government of the Czech Republic (2021), *Action Plan for the National Cybersecurity Strategy for the years 2021 to 2025*.

ITDZ-Berlin (2021), *Mehr als 50 Jahre IT für Berlin*.

Kaspersky (2019), *Story of the year 2019: Cities under ransomware siege*, Kaspersky Secuirty Bulletin, 11 December 2019.

Kapsevičius, G. (2022), *Who are those "Killnet" who attacked Lithuania: enthusiasts, interns or scouts?*, 15min.lt.

KnowBe4 (2022), *The Economic Impact of Cyber Attacks on Municipalities*, *whitepaper*.

Koks, E.E., Van Ginkel K.C.H., Margreet J.E. Van Marle M.J.E and Lemnitzer, A. (2022), *Brief Communication: Critical Infrastructure impacts of the 2021 mid-July western European*

flood event, Natural Hazards and Earth System Sciences, 22(12), 3831-3838. CC BY 4.0 license.

Madeira Simões, R. (2021), *Preocupações com cibersegurança na CM Amadora*, ITSECURITY web article dated 22/12/21 by the Head of Systems and ICT Division of the Municipality of Amadora.

Microsoft (2022), *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*, Digital Security Unit, April 27, 2022.

Muench, S., Stoermer, E., Jensen, K., Asikainen, T., Salvi, M. and Scapolo, F. (2022), *Towards a green and digital future*, EUR 31075 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-52452-6, doi:10.2760/54, JRC129319.

Municipality of Amadora (2021), *Relatório de gestão 2020*, CMA 12.05.2021,GER,I,RE, 51286.

Municipality of Amadora (2022), *Relatório de gestão 2021*, CMA 10.04.2022,GER,I,RE, 50036.

Municipality of The Hague (2018?), *Toward cyber resilient cities*, Pioneered by the Rockefeller Foundation, 100 Resilience Cities.

Municipality of The Hague (2019), *The Hague Resilience Strategy 2019*, Pioneered by the Rockefeller Foundation, 100 Resilience Cities.

Municipality of The Hague & Cybersprint (2021), *How to Hack a City – e-Guide*, V1.0, November 2021.

National Cyber Security Centre – NKSC (2021), *National Cyber Security State Report*, Report Nr. GL-337, Vilnius, Lithuania.

OECD (2022), *Digitalisation for the transition to a resource efficient and circular economy*, OECD Environment Working Papers, No. 192, OECD Publishing, Paris.

Ottis R. (2008), *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

Ouest France (2022), *Bretagne. La Région reçoit 1 million d'euros pour créer un centre de réponse aux cyberattaques*, article dated 14 July 2022.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility.

Regulation (EU) 2021/1056 of the European Parliament and of the Council of 24 June 2021 establishing the Just Transition Fund.

Regulation (EU) 2021/1057 of the European Parliament and of the Council of 24 June 2021 establishing the European Social Fund Plus (ESF+).

Regulation (EU) 2021/1058 of the European Parliament and of the Council of 24 June 2021 on the European Regional Development Fund and on the Cohesion Fund.

Regulation (EU) 2021/1059 of the European Parliament and of the Council of 24 June 2021 on specific provisions for the European territorial cooperation goal (Interreg) supported by the European Regional Development Fund and external financing instruments.

Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014.

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

The Government - Local Government Denmark - Danish Regions (2016), *A stronger and more secure digital Denmark - The Digital strategy 2016-2020*, May 2016.

The Shift Project (2019), Climate crisis: the unsustainable use of online video – The practical case for digital sobriety, report led by Maxime Efoui-Hess for the think tank The Shift Project.

United Nations Office for Disaster Risk Reduction (2015), *Sendai Framework for Disaster Risk Reduction 2015 – 2030.*

UK Council for Internet Safety (2019), *Digital Resilience Framework: A framework and tools for organisations, communities and groups to help people build resilience in their digital life*.

Vilnius Municipality (2021), *Strategic Development Plan 2021-2030*, Vilnius, Lithuania.

Yin R. (2003), Case study research: design and methods, SAGE, pp. 85 - 106.

EN

ISBN 978-92-895-2664-7
doi: 10.2863/5099

QG-05-23-158-EN-N

Publications Office
of the European Union

European Committee
of the Regions

Created in 1994, the European Committee of the Regions is the EU's political assembly of 329 regional and local representatives such as regional presidents or city-mayors from all 27 Member States, representing over 446 million Europeans.

Rue Belliard/Belliardstraat 101 | 1040 Bruxelles/Brussel | BELGIQUE/BELGIË | Tel. +32 22822211
www.cor.europa.eu | @EU_CoR | /european.committee.of.the.regions
/european-committee-of-the-regions | @EU_regions_cities