Position Paper – Contribution to Public Consultation
European Commission White Paper :
How to Master Europe's Digital Infrastructure Needs?

Brussels, 27 June 2024

The Confederation of European Security Services (CoESS) highly welcomes the European Commission's White Paper on "How to master Europe's Digital Infrastructure Needs". We strongly believe that, together with recent EU Council Conclusions on the future of the EU's digital policy and of cybersecurity, the Paper sets the basis for future initiatives to enhance resilience, innovation and competitiveness in the European economy. Private security services in Europe increasingly depend on digital infrastructure, particularly in the Monitoring and Alarm Receiving business, due to advancements in technology and customer expectations for real-time response capabilities. Digital infrastructure enables seamless integration of surveillance systems, alarms, and real-time data analytics, enhancing the efficiency and effectiveness of monitoring and alarm response operations. The transition to 5G technology and the adoption of cloud infrastructure are thereby pivotal for the advancement of security services such as in Monitoring and Alarm Receiving Centres (MARC). As set out in this contribution to the consultation, this shift requires transparency in infrastructure investments (e.g. in the case of the 5G transition), EU regulation that promotes innovation and legal certainty, as well as robust security measures that adapt to evolving threats in a technologically connected environment.

2/3 discontinuation and 5G transition

1. Opportunities and Challenges

The 2G and 3G networks will be phased out as planned in favor of 4G and 5G. While monitoring and alarm services in Europe still largely rely on 2G/3G networks, the transition to 5G networks offers many important opportunities for significantly faster and more reliable connectivity, enabling the integration of advanced technologies such as drones and Artificial Intelligence (AI), thereby enhancing the efficiency and capabilities of security services.

An important challenge is however that the closing of 2G/3G networks proceeds currently quicker than the building up of 4G/5G networks – affecting many products and services that today use the 2G or 3G networks, especially affecting utilities and commodities services, such as monitored alarm services, eCall services in cars, up to the entire IoT ecosystem. Society is heavily impacted because shutting down networks with no proper preparation could render devices obsolete and essential services inaccessible:

- A pre-mature shutdown of 2G/3G networks impacts certain segments of the population who still use them, such as the elderly or individuals in rural areas with limited access to newer technologies due to the lack of coverage on those areas or to the need to carry out an exhaustive migration of the services. In practice, that means for example that, in some areas in the countryside, it will be hard to find solutions that can communicate a security or fire alarm to a MARC.
- But shutdown will not only affect the above, but also other emergency-related services, such as eCall service which is currently settled on 2G protocols. It is worth noting that there still is no final 4G based eCall standard, in part because of complexities inherent in the VoLTE standard, meaning that it is not possible even today to migrate away from 2G/3G services.
- In addition, we stress that while 4G and 5G have greater data transmission capacity, it is not needed for simple warning or signaling systems. 2G may even be a more useful technology in rural areas, thanks to its range.

It is natural for consumers and industry to take for granted the availability of services to maintain connections. Likewise, it is reasonable to expect the ability to reach out for assistance when needed. Within the EU, access to emergency services is fundamental. This entitlement is in legislation, and those responsible for offering electronic communications networks and services are obliged to ensure continuous access for their users. A progressive and well defined phasing out of 2G/3G in liaison with affected stakeholders and industries, including private security services, is therefore of utmost the importance to avoid serious societal and economical implications and to ensure a seamless implementation and business continuation.

2. Recommendations for action at EU-level

CoESS considers that the European Commission should ensure proper coordination at EU-level and promote public consultations by the regulator in each EU Member State to evaluate each country's circumstances and potential impacts of a 2G/3G shutdown without granting the proper time to carry out the migration to new technologies.

It is worth highlighting that in no country, except in Finland, a public impact analysis has been carried out by the supervision authorities. In Finland, such analysis concluded in the modification by law of telco licenses to grant 2G availability until 2029. In our views, 2G/3G availability should be granted in, at least, one network in each country until 2029/2030 (as Finland has done) to ensure a smooth transition. Such a postponement would enable a more resource-efficient transition and mitigate challenges. Without prolonging the 2G/3G network's lifespan to a reasonable deadline, businesses, consumers, and society will encounter significant disruptions in essential services and functionalities.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**

Cloud Services

1. Opportunities and Challenges

Innovation in Monitoring and Alarm Receiving Centres (MARC) depends on cloud services for several key functions – namely sensitive data storage (e.g. surveillance footage and alarm data), real-time data processing and analytics allowing rapid response to security incidents, and the integration of security solutions. They are therefore of central importance to future connectivity needs of security companies, but can also present challenges in terms of physical and cyber security.

Protecting personal data and complying with privacy regulations remain priorities for the security industry and companies must strengthen their security measures to prevent data. The risk of lost information must however be traceable so the part that lost the information can also take the responsibility of the situation. VSS system, alarms and client information that is a part of the MARC, will also be in the cloud and if there is somewhere in the architecture a loss of information it must be traceable.

2. Recommendations for action at EU-level

CoESS will closely monitor regulation of cloud infrastructure, including through the vast EU legal framework on cybersecurity and data protection. We however note that open cloud platforms are global in nature and generally conform to global standards. It should therefore be guaranteed that EU-specific regulations and Standards are aligned with global security standardisation, as this could otherwise limit the ability for European corporations to use the major providers' services and compete on a global market.

Promotion of innovation

1. Opportunities and Challenges

The integration of technology such as drones and AI into security services is expected to play an important role in the ever-evolving transformation of the security industry. They can offer useful intelligence in real time that can provide security officers with an additional "sense", enhance occupational health and safety, improve security measures through enhanced decision-making, and shorten response time in case of an incident. Security services become more sophisticated and reach a new level of "intelligence".

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**

CoESS Members however report that both at national and EU level, they fear a risk of overregulating technology and see different interpretations of EU law hampering important innovation. For example, the use of drones is so strongly regulated and in many countries inefficiently enforced that their deployment in security services is highly hampered and businesses fear investments (see multiple statements of CoESS on the matter at www.coess.eu).

2. **Recommendations for action at EU-level**

CoESS hopes for an implementation of the EU AI Act and EU Drone Strategy 2.0 which promotes innovation and technology-neutrality, e.g. as part of the AI regulatory sandboxes. For the future, another matter where overregulation should be avoided is end-to-end security, for which reliable global standards exist.

Resilience of Critical Digital Infrastructure

1. **Opportunities and Challenges**

CoESS highly welcomes recent steps to enhance physical and cyber resilience of critical digital infrastructure in Europe at all levels – including the comprehensive legislative framework of the EU Cybersecurity Act, NIS 2 and CER Directives, and the EU Cyber Resilience Act. What counts now is their effective and adequate transposition/application at national level.

2. **Recommendations for action at EU-level**

While we welcome the European Commission's frameworks to oversee the transposition of aforementioned EU law, we further recommend the next Commission to keep the topic of physical and cyber security high on its agenda, considering the following aspects:

- **Infrastructure modernisation:** the EU should facilitate the modernisation of existing infrastructures to make them more robust against cyber threats. This process should however take place in full transparency and engagement with relevant stakeholders, as explained in the context of the 5G transition process.
- **Promotion of Standards in the implementation of EU law, including the NIS2 and CER Directives, and the EU Cyber Resilience Act:** This should include both Standards developed at global level, at ENISA (e.g. on cloud services) and by the EU Standardisation Bodies (e.g. EN 50518 including security norms for Monitoring and Alarm Receiving Centers, and EN 17483

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

including quality norms for security companies protecting Critical Infrastructure). In standardisation and audits, an adequate focus must be put on infrastructure architecture, resilience and service continuity in case of an incident.

- **Ambitious transposition of the NIS2 and CER Directives:** as highlighted in our White Paper on cyber-physical security of Critical Infrastructure (available at www.coess.eu), it is crucial to address cyber and physical security of Critical Infrastructure interdependently. A cyberattack can have physical consequences or be used to prepare a physical attack, while human error or sabotage can enable a large scale cyber-attack. We call on the European Commission to help EU Member States transpose the NIS 2 and CER Directives in an ambitious way, promoting holistic resilience and security along both the cyber and physical security value chains. We believe that particularly the resilience of the energy sector, telecommunications, cable infrastructure and essential services such as data centers are of primary importance to digital infrastructure in the security industry.

About CoESS

CoESS acts as the voice of the private security industry, covering 22 countries in Europe and representing 2 million security officers as well as over 45,000 companies. The private security services provide a wide range of services, both for private and public clients, ranging from Critical Infrastructure facilities to public spaces, supply chains and government facilities. CoESS is recognised by the European Commission as the only European employers' organisation representative of the private security services. Representing a labour-intensive sector, CoESS is actively involved in European Sectoral Social Dialogue and multiple EU Expert Groups – including SAGAS, SAGMAS, LANDSEC, RAILSEC and the EU Operators Forum for the Protection of Public Spaces.

EU Transparency Register Number: 61991787780-18

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**