IDENTIFIED CALL	HORIZON 2020
TOPIC	Security for smart and safe cities, including for public spaces
Type of Action	IA Innovation action
Hyperlink CALL	Link
Open call	14t March 2019
Deadline CALL 1st stage	22nd August 2019
Challenge	In the cities, public spaces such as malls, open crowded gathering areas and events, and non-restricted areas of transport infrastructures, constitute “soft targets”, that is potential, numerous targets spread across the urban area and subject to “low cost” attacks strongly impacting the citizens. The generation, processing and sharing of large quantities of data in smart cities make urban systems and services potentially more responsive, and able to act upon real-time data. On the one hand, smart cities provide for improving the security of open and crowded areas against threats (incl. terrorist threats) and risks, by leveraging wide networks of detection and prevention capabilities that can be combined with human response to crisis to enhance first responders' actions. On the other hand, the distinct smart technological and communication environments (urban, transport infrastructures, companies, industry) within a smart city require a common cybersecurity management approach.
Scope	The security and good operation of a smart and safe city relies on interconnected, complex and interdependent networks and systems: public transportation networks, energy, communication, transactional infrastructure, civil security and law enforcement agencies, road traffic, public interest networks and services. Such networks provide with an efficient infrastructure for detection resources and "big data" collection. The screening of such data are being used by security practitioners to enhance their capabilities and performances. For instance, crowd protection and the security of public and government buildings can be improved through the identification of threats or of crime perpetrators, and the early detection of dangerous devices or products; first responders may get quicker on site by calculating in real time the shorter possible route to the scene of disaster.Proposals under this topic should develop and integrate experimentally, in situ, the components of an open platform for sharing and managing information between public service operators and security practitioners of a large, smart city.
Impact	• Creation of dedicated, harmonised, advance cybersecurity solutions for smart cities adopting common approaches with all involved stakeholders (e.g. administrators of smart city/port/transport) balancing their – sometimes conflicting – goals (e.g. urban development, efficiency, growth, competitiveness, resilience). • In situ demonstrations of efficient and cost-effective solutions to the largest audience, beyond the project participants. • An easier level of integration by developing a holistic cyber-security framework for smart cities that benefits all smart infrastructures hosted within it (e.g. smart buildings, smart ports, smart railways, smart logistics). • IoT ecosystems (rather than distributed IoT infrastructures) built adopting common approaches in their cybersecurity management, achieving economies of scale (e.g. avoiding duplication of efforts in the analysis of IoT data, selection of cybersecurity controls). • Novel concepts of operations taking account of mutiple, heterogeneous data sources and the social media. • Novel tools and systemic approaches to protect citizens against threats to soft targets
Budget call (and for project)	8 EUR million for Innovation Actions would allow the areas to be addressed appropriately.