

Targeted topics

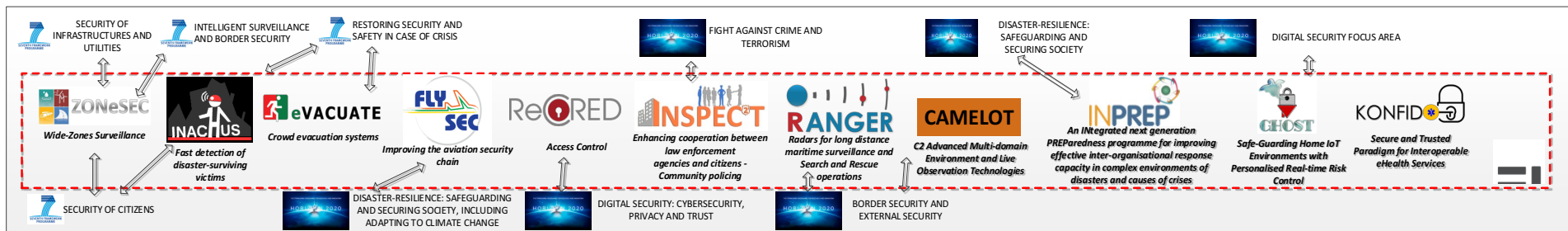
SU-INFRA01-2018-2019-2020	Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure
SU-DRS02-2018-2019-2020 subtopic 1	Technologies for first responders - subtopic 1: Victim detection technologies
SU-BES02-2018-2019-2020 subtopic 1	Technologies to enhance border and external security - subtopic 1: Providing integrated situational awareness and applying augmented reality to border security

EXUS Software Ltd
Dimitris Kanakidis
dkan@exus.co.uk
+30 2107450347

EXUS Software Ltd
Ioannis Komnios
i.komnios@exus.co.uk
+44 208 1237407

Competencies

- *Integration of large-scale, research and commercial systems*
- *Development of complex information and data management systems implementing data fusion algorithms*
- *Development of sophisticated Web-based and Mobile Apps for crowd safety*
- *Big data management and analytics for critical operations*
- *Cloud engines and analytics for Massively MultiUser Platforms(MMUPs)*
- *Strategic management, quality control and efficient coordination of large scale, multinational projects (21 running projects/13 coordinated)*



Project idea

	Prevention (P)	Detection (D)	Response (R)	Mitigation (M)
Local Level	CyberSecurity: Attacks to tele-monitoring devices, Communication for ambulatory services, quality of information provided through informal channels (e.g. internet and social media)			
	Physical: Tracking of ambulatory services			
	Tracking of medical personnel involved in home-care and ambulatory services			
	Patient and Personnel Education			
Regional Level	Securing logistics: Supply chains (pharmaceuticals, organ donation, food, other supplies)		Sharing information with the public in the vicinity of the installations, protection of rescue teams, security teams and monitoring teams	
	Physical: Protection of infrastructure		Communicating with the public, such as public service announcements	
	Patient and Personnel Education	Unusual behaviour: surveillance and detection of illness in patients/staff		Guiding authorized personnel and visitors to appropriate entrances/exits
	CyberSecurity: Attacks to local servers and electronic equipment within the hospital level, cross-region communication			
	CyberSecurity: Attacks to cloud based infrastructures, centralized systems, channels for cross country data exchange			
National Level	Securing logistics: Supply chains (pharmaceuticals, organ donation, food, other supplies)		Tracking: Supply chain (e.g use of medicine to disposal (environmental security))	
			Communicating with the public, such as public service announcements	
			Sharing information with the public in the vicinity of the installations, protection of rescue teams, security teams and monitoring teams	

Skills needed:

- Health Care and supply chain End-users (Healthcare system, Hospitals, suppliers)
- Cyber Security technology experts
- Home care Technology/Solution providers
- Social Scientists