PATHWAYS TO INNOVATION IN DISASTER RISK MANAGEMENT

Paolo Venturoni – CEO European Organisation For Security
4th June 2018
The European Organisation for Security (EOS) is the voice of the European security industry and research community. Operating in 15 different countries, EOS Members provide security research, solutions, and services across many security domains, including: Soft Target & Critical Infrastructure Protection, Transport Security, Border Security and Cybersecurity.
EOS Members
Content

• Man-Made Hazards
• Comprehensive Approach
• Capabilities Deployment
• Integrated System approach
• Technology/Process Considerations
• Paths to innovation
• End-to-end approach
• This presentation will focus on the risk management of man-made technological hazards

• Technological hazards, according to the UN Office for Disaster Risk Reduction are those that originate from technological or industrial conditions, dangerous procedures, infrastructure failures or specific human activities, such as nuclear, chemical or transport accidents

• While a greater weight is given in this presentation to the security dimension of these hazards, the considerations are, from a technological stand-point, largely applicable also to safety considerations

• The security perspective introduces an intelligent malicious element in the risk management equation
A Comprehensive Approach

• Managing man-made hazards is as much a matter of deployment of technological solutions as it is of processes implementation

• Therefore, a comprehensive approach is necessary to effectively prevent, manage and recover from man-made accidents

• Such a comprehensive approach must rely on a framework which includes Risk Analysis, Prevention and Protection solutions, Assessment and Process Validation

• The preliminary risk analysis phase is particularly important as it allows to define priorities, according to cost-benefit considerations, for capability development and deployment
A Comprehensive Approach

- Preparedness
- Response
- Mitigation
- Recovery

Risk Analysis

Assessment & Process Validation

Prevention & Protection

Resilience
Capabilities development and deployment must be approached from a system perspective integrating evaluation of the threat, budget considerations, technological requirements and environmental conditions.

In the different phases of an accident it is key to be able to process vast amount of data in order to produce reliable and actionable information.

Seamless integration of different technologies requires a focus on standards and interoperability.

From a security perspective it is important to ensure also a reasonable degree of European autonomy when deploying technological solutions.
Capabilities deployment

System Integration approach

- Data and information gathering
- Mobile/5G
- Autonomous & remotely piloted systems
- Geo-referencing
- Screening and Detection systems
- AI
Integrated System approach
Integrated System approach

01 CASE MANAGEMENT
- AUTOMATED CASE CREATION
- MANUAL CASE CREATION
- 3rd PARTY INGESTION

Cases ingested from various sources, along with additional data from other sources

02 PROFILER
- RISK PATHWAY ASSIGNMENT

AI and ML algorithms suggest a risk level for each case. The system learns from itself using verdicts from processed cases

03 DECISION CENTRE
- SPLIT INTO 5 RISK CATEGORIES, CUSTOMISABLE TO SPECIFIC PORT PROCESSES
- CONFIRM/ OVERRIDE RISK PATHWAYS

Customs officers either confirm or override the suggested risk levels from the profiler engine, these risk levels correlate to various action pathways depending on what inspection processes your port has available

04 OPERATIONS OPTIMISER
- NON-PHYSICAL ANALYSIS & INSPECTION TOOLS

All data feeds into a single view for supervisors to understand and control current operations, and an optimiser to make the best use of available resources. Case verdicts feed back to the ML algorithm

05 COMMON OPERATIONAL VIEW
Technology/Process Considerations

• Technology solutions produce also false alarms: need to develop protocols
  - Alarm resolution/search takes time, space and staff
  - Can’t evacuate without very good reason
• Technology must work in different and complex environments
• Performance monitoring and verification of compliance should be regularly conducted
• Training of staff is key, and also large scale exercises at the EU level
• End-users and Industry need to work in partnership to optimize requirements
• Definition of requirements and procurement of capabilities are key to foster innovation in the DRM domain.
• Research & Development activities must be finalized at closing technological gaps in order to ensure deployment of state-of-the-art capabilities.
• Research and innovation are functional to respond to market (end-users) needs.
• Definition of requirements and standards, funding of capacities and R&I financing to be realized through Public Private cooperation and dialogue.
End-to-end approach

Market deployment

- Security solutions, operations, & maintenance
- Security staff training
- Manufacturing & Capability Deployment
- End-users procurement

Research & Innovation

- Risks & threats assessments capability requirements
- Concepts of operations & technology roadmaps
- Security solutions, development, R&D projects, integration, test & validation

EU & NATIONAL SECURITY POLICIES
WORLDWIDE COMPETITIVENESS
PRIVACY & LEGAL CHALLENGES
GUIDELINES & REGULATIONS
END-USER FUNDING
MARKET DEFRAGMENTATION
STANDARDS IMPLEMENTATION

END-USER FEEDBACK AND EVALUATION

PAN EUROPEAN CERTIFICATION PROCESS

EU & NATIONAL SECURITY POLICIES
GOVERNANCE (PUBLIC-PRIVATE PARTNERSHIP)
PRIVACY & LEGAL CHALLENGES
GUIDELINES & REGULATIONS
COMMON STANDARDS
ENVIRONMENT INTEROPERABILITY
R&I FUNDING

PRE COMMERCIAL PROCUREMENT Gateways to move to the next development phase
THANK YOU
We can provide contacts for individual manufacturers or can engage as a group

W: www.eos-eu.com
E: maria.properzi@eos-eu.com
T: +32 27937594