SOFT BUT STILL CONCERNS

Distinguished chair, colleagues, ladies and gentlemen good afternoon,
Nowadays we usually consider "security" as a seamless part of our life, apparently something cost-free, no need to invest or care about it. This seems to be true till we face minor or big problems. Therefore, we start to be concerned about security, it is no more a cost-free "commodity", we need to invest some resources to reach "a certain level of "insecurity".

The evolution of potential threats forced to re-shape the "enemy" from Nation States to groups and individuals challenging with a wide range of "weapons" on different domains: digital, economic, healthiness and more,/ the wideness of the range of challenges forces to redefine the institutional definition of **state security** to a more effective concept of **homeland security** that enforces the idea of 360-degree security whatever is the threat. So, threat conceptualization has changed it includes massive migration, single or organised terroristic groups, and other non-state actors; simply consider the perceived environmental and humanity security under the shade of climate change.

In the name of 'security', western governments are now going to integrate their police forces, customs and immigration services into seamless national and international intelligence and law enforcement systems. Passport checks and immigration controls are being replaced by security fences and sprawling e-borders linked to dedicated border police forces; private security, high-tech surveillance and police intelligence is coalescing around the policing of mega-events (summits, protests, the Olympic games and more) and 'critical infrastructure protection' (airports, financial centres, power stations and more); 'policing' is becoming ever more 'proactive', based not on responding to crime and disorder, but identifying and neutralising security risks; a plethora of public and private bodies are being incorporated into the drive for more 'security'.

State actors face a very complicated scenario trying to match with the current and future developments of threats based on risk assessment, probability and projections. Many times, in this complex and risky scenario, the best or less harmful solution is to refer to the game theory and how to maximise the gain minimizing risks. This may led to choices motivated by contradicting goals.
Potential countermeasures deal with prevention of potential attacks and mitigation of possible impact because soft targets usually lack capacity to strike back against attackers. If we refer to terroristic groups or single activists they do not have "homeland" to strike back, the same in case of hackers and cyber-attacks. Key actors of such measures belong to governmental bodies, communities or private subjects.

In the US they call it "Securing the Homeland", in the EU, with its preference for interminably technocratic terminology, they call it "interoperability". Once again, the private sector is at the heart of this transformation: for 'military-industrial complex', read 'security-industrial complex'.

Or as former EU Commissioner Franco Frattini said:
"*Security is no longer a monopoly that belongs to public administrations, but a common good, for which responsibility and implementation should be shared by public and private bodies.*"

So, homeland security **unified** under a unique dome all the security measures including completely new ones like "triangulations" or 'pre-emptive measures' like "pre-emptive war" as it happened mainly in the US.

Soft Problems / Concerns - A "soft target" is a person, thing, or location that is easily accessible to the general public and relatively unprotected, making it vulnerable to military or terrorist attacks. Typically, the term is used to denote places with high concentration of people and low degree of security against assault, which creates an attractive target, especially for terrorists. Placing the soft targets in focus alongside the hard targets reflects an innovative attitude towards security management.

Cybercrimes are increasingly targeting Governmental or Law Enforcement agencies and Institutions, critical infrastructure, or targeting big companies. Financial markets may be influenced or tilted by cyber-attacks. Smart cities and grid models must carefully take into account cyber security issues; we don't appreciate the "rebellion" of our car or elevator, the unwanted locking of all the entrance doors of our company headquarters.

What about industrial machinery today fully computerised, or critical infrastructure management; in a cyber warfare scenario it might be enough to dispatch on the network a code name like "1024 millibar" to collapse the whole target infrastructure. This to do not mention aircrafts, ships, trains, metro and any other transportation means, PLC and more in general software programs are easily hacked. We are surrounded by "critical infrastructures" that may create mayor or minor impact on our daily life.

In addition, we find Hybrid Threats - Cyber technology and its pervasiveness created a completely new scenario, the new type of hostile actions can be grouped under the umbrella of "hybrid threats" a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.

"Hybrid threats" include: massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct,/ proxy actors can be vehicles for hybrid threats. An even increasing volume of information is flowing through the network including messages concerning potential future risks or cyber-weapons. Big data analytics, artificial intelligence and machine learning together with other technologies may help in these tasks.
Till what extent we are willing to give-up our privacy to increase security? The car we drive, the phone in our pocket, our wristwatch, the clothes we wear, are smart and connected; then the concept of "private" becomes far more ephemeral. Cameras, satellites, sensors and software virtually everywhere ensure that, no matter how much technology you eschew, someone can get some data off of you and profile. Which is the golden balance between privacy and security issues?

How to design a Security system
Here are some steps to be taken before a functional security system can be set up:

- What do I want to protect
- Against who/what
- How do attacks happen / Modus Operandi
- Threat and Risk Analysis
- Clarification of strategy and methods
- Specification and application of measures
- Team / asset management

Vulnerabilities, Threats, Risk - While creating a security system for a particular soft target (place or event), the first indispensable step is to clarify what is to be protected. Therefore, we start by defining the entities we value and do not wish to lose, and the harm that might be done. These usually includes the safety and lives of people, property, information, values or a good name.
In phase two, it is necessary to define potential sources of danger/threat against the protected entities. We identify particular enemy groups or categories of individuals with a conceivable motive to attack. In order to do so, we need to analyse previous attacks of similar nature and to consider potential sources of threat. It is necessary to keep in mind the specifics of the protected entity.
These two aspects are the cornerstone on which we should build a security system for a particular soft target. Guideline is based on a systematic analysis of the threats posed to each particular soft target.

Once the analysis is complete and the possible threats are defined, we can move on to select and implement adequate security measures. It is important to rank the threats by likelihood of occurrence and by seriousness of impact.
Rating list of major threats it helps to set up the security system more accurately and to allot resources more effectively.
Knowing the major threats makes it possible to select the adequate security measures to be adopted.

Time line - All incidents need to be handled in three phases. What can be done beforehand so as to reduce the likelihood of an incident, to minimize possible impact or to divert the attack altogether? What can be done during the attack? And finally, what can be done once the attack has occurred to mitigate its impact?

Unfortunately, when a soft target is attacked, professional teams are usually not present. However, educated staff (or members of the public present on the spot) can play an important role in the phase of immediate response.

Otherwise, if possible, it is always recommended to run or hide rather than fight (remember the American rule: run – hide – fight).

All security solutions designed for soft targets must be:

- fool-proof and efficient because people's lives are at stake
- creative because the resources which the soft targets can deploy are usually limited,
- flexible because they must meet the needs of various environments and they must be applicable to attacks by various enemy groups, tactics and weapons.

To conclude, to adequately face soft concerns LEAs must cooperate with private "soft-target" security and citizens, we need to foster the **Culture of Safety & Security as a first defence line, in doing so we will improve as well resilience even in case of human and natural disasters**.

http://www.youtube.com/watch?v=pmNoGaAsxpc