



## INTEGRATED CYBER SHIELD (ICS)<sup>TM</sup>

Integrated Cyber Shield<sup>TM</sup> is the SELEX Sistemi Integrati architectural solution conceived with the main purpose to obtain intrinsically secure systems through a built-in cyber resilient architecture, suitable for real-time protection, analysis and reaction to cyber attacks.

### THE CONTEXT

*Cyber attacks to infrastructures are social/economical threats, not merely menaces against IT networks*

Essential systems providing water, electricity, healthcare, finance, food and transportation are now increasingly network dependent, distributed and interconnected. The detrimental consequences of this growing dependence become apparent during time of political conflicts, social instability, and other traumatic events.

Internet has made information exchange easier and more efficient, but it has also created a new space where criminals and terrorists can operate almost undetected. Then, once confined to physical world, modern human conflict has spread to cyberspace that can be regarded as a massive socio technical System of Systems, humans being a significant component of it. Cyber attacks cover a

wide range of actions: attacks can affect data, processes and programs, as well as the network environment. Such attacks might involve intrusions into unprotected networks for the purpose of compromising data tables, degrading communications, interrupting commerce, or impairing critical infrastructures (such as transportation or medical and emergency services) in such a way that trust is undermined at the expense of a smoothly running economy and society. Thus, a cyber attack compromises the security expectations of an individual, of an organization, or of a nation. Achieving global cyber security is a matter of strategic economic interest for all nations.

*SELEX Sistemi Integrati starts from the awareness that Cyber Warfare can only be faced through an architectural approach that aims to guarantee the global system protection, by combining technologies, processes and organization models.* This approach enables analysis, modeling and simulation, as well as the validation in term of security for all systems.

The application of a system-based culture on this matter implies to assist major institutions in adopting technologies and processes that put cyber security at the centerpiece of their infrastructures.

Therefore, the dimension of cybersecurity problems and the definition of suitable countermeasures require a

sort of “holistic” approach, not only intended to monitor and mitigate the effect of cyber attacks, but mainly to prevent their effect by designing more robust systems with respect to any threat from cyberspace, design their resilience and, if necessary, provide them with proper reaction capabilities.

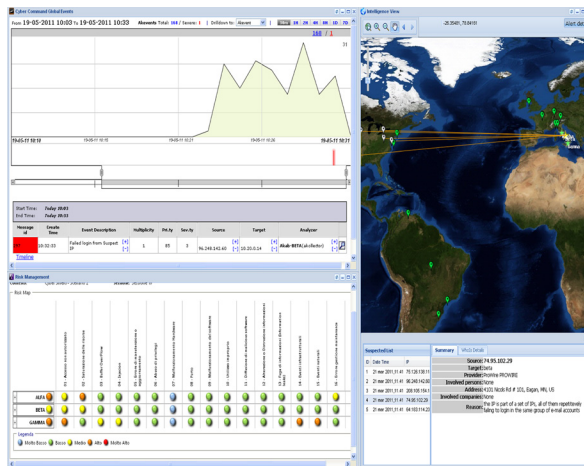
## THE SOLUTION

**Only a system-wide approach can ensure prevention and detection of coordinated cyber attacks, which could be otherwise misinterpreted as singular threats**

Integrated Cyber Shield represents the answer to the new issues of Cyber Security and Cyber Warfare, in order to prevent, identify and localize criminal, terroristic and military attacks. While most of existing systems are only based on traffic analysis to defend from intrusions, adopting the criteria of hash signature to identify malware and potential virus, SELEX Sistemi Integrati adopted a new approach that considers both the technical aspects and the behavioural component behind any kind of cyber attack. Based on the analysis of already detected attacks, traditional systems and tools are unable to contrast complex menaces, often unknown and unpredictable. In this case the analysis of particular behaviours detected on applications and data connections can show the evidence of a new cyber attack. This approach is the basis for the development of reliable and secure systems, strengthening the resilience of complex, distributed and heterogeneous infrastructures. *This approach implies that the cyber space dimension is embedded into systems since their design phase and plays a role in the architectural approach.* The Integrated Cyber Shield solution also looks at the protection of legacy systems, to strengthen their resilience to cyber attacks by injecting cyber protection solutions into existing system architectures.

In fact, since cyber attacks are emerging threats, many systems of systems and critical infrastructures were realized without suitable protection or are currently shielded with successive added-on limited solutions.

Then, Cyber Shield provides a global architectural solution and an operational solution.



## THE OPERATIONAL POINT OF VIEW

**No valid defence can be applied when the enemy is already at the gate or inside your walls (Sun Tzu, “The Art of War”).**

From the operational side, Cyber Shield provides a platform that manages all data collected in the cyber-space through a network of different sensors, correlates them and analyses the resulting information to detect and localize any kind of cyber attack, predefined or unprecedented, and establishes the countermeasures to contrast attacks and smoothly restore operations. This Cyber Command System provides every CERT (Computer Emergency Response Team) with a qualified Cyber Operational Picture, showing the situational awareness and the capability to protect, detect, contrast and recovery in case of cyber attacks against domains under protection. Through the analysis and correlation of real time information, it is possible to identify and isolate cyber threats, to protect the networks in case of attacks and react for impairing their offence capability.

## KEY POINTS

Integrated Cyber Shield is the SELEX Sistemi Integrati advanced solution to protect systems of systems and critical infrastructures against any kind of cyber attacks and react against them.

This solution is based on two pillars:

- a system architecture approach for realizing highly resilient infrastructures
- a command & control system that analyses, protects and contrasts cyber intrusions, providing a comprehensive Cyber Operational Picture.

Based upon:

- expertise of SELEX Sistemi Integrati in: the realization of large complex systems for homeland security and defense, a wide portfolio of net-centric C2 systems, long standing experience in system engineering, participation in international NATO initiatives on Cyber Security: these factors represent the foundation of the SELEX Sistemi Integrati Cyber Shield solution.
- global approach: strategic architectural methodologies and modeling for a multilayered risk assessment looking at technical, social and economical aspects.
- proactive solution: a “living” architecture capable to adapt itself properly to the situation in order to provide the best means of defense and reaction
- amplified system resilience: capability to realize built-in cyber protected system architectures, as well as to reinforce existing infrastructures with ad-hoc interventions on legacy system architectures to minimize damage and recovery time
- dynamic protection: able to detect, localise and contrast both well-known and unprecedented attacks, also evaluating attack dimension in space and time.