WHITE PAPER

# SECURITY AND RESILIENCE OF INFORMATION AND COMMUNICATION TECHNOLOGY NETWORKS FOR THE PROTECTION OF CRITICAL INFRASTRUCTURES

**November /2009**

Version 1.0
EOS ICT Security Working Group

EUROPEAN ORGANISATION FOR SECURITY

## Table of Contents

# Executive Summary

Over the last two decades, the world's landscape changed considerably, relying increasingly on ICT systems for the **availability and exchange of information in all sectors to fuel economic growth and improved competitiveness**. Whether we speak of ICT systems as applications, telecommunications or integrated system solutions, they have become key components of many Critical Infrastructures, and, as such, their disruption, malfunction or compromise can seriously impact our societal and individual well being.

However, based on the analysis of past incidents, security is not always implemented as a pervasive feature in these critical systems. Even though what is at stake is a feature recognised by all actors as being key, security field specialists often propose concurring approaches and security is rarely designed into the systems, even though from a technical point of view, approaches such as the Secure-by-Design enable the design of secure systems. Furthermore, security is still perceived as a constraint rather than as an opportunity, and operators overlook the return on investment of secure operations versus the high costs incurred through intentional or accidental security breaches.

The factors leading to such a situation are multifaceted. On the one hand, ICT security is not always part of the core competencies of Critical Infrastructure Operators. Moreover, not all ICT solution providers give security the right level of importance, delegating the core of security to specific sub-systems and not considering the whole picture of security.

Despite the progress that has already been made, there remains a lack of security awareness, or more precisely a lack of understanding of the security process. More often than not, this lack of awareness and understanding affects the early procurement process of a critical system and potentially impedes its implementation at the later stages.

Moreover, even though the Communication from the European Commission on Critical Information Infrastructure Protection[1] constitutes a major step forward in the protection of Europe from large scale attacks and disruptions, the initiatives currently existing under the FP7 Security Theme, EPCIP, ICT PSP and the ICT Programme will not lead to satisfactory results without ensuring their coherence, a goal that could be achieved through the establishment of a federated European Cyber Security Programme.

Therefore, drawing on its huge pool of experts and based on its state-of-the-art analysis, the European Organisation for Security (**EOS**), composed of major European security suppliers and representing over 20% of the 100 Billion Euro worldwide security market, **strongly recommends the European Commission** (EC) **to:**

1. **Establish a public-private dialogue on ICT security**, not only with the telecom operators, but also with the energy, transport and finance sector, system providers and security professionals in order **to inform stakeholders on the issues at stake, raise the awareness** of possible solutions **and exchange best practices.** This engagement should start with establishing a baseline of the existing processes and organisations already developed and operating within the cyber security arena in order to exploit best practices and ensure any EU proposals seamlessly fit in;
2. **Define a common framework** at EU and preferably international level to secure Europe's information systems **on the basis of a Secure-by-Design-Based-System Approach;**
3. **Ensure an equal level of investment in security** by providing financial guidance and support to operators, thus avoiding market distortions, and **by establishing a federated EU Cyber Security Programme** to support Threats & Risks assessment methodologies, feasibility studies, pilot actions & deployment within Critical Information Infrastructure Operators.

[1] COM(2009)149 final, « Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience".

# Introduction

Over the last two decades, the world's landscape changed considerably and became reliant on the availability and exchange of information in all sectors to fuel economic growth and improved competitiveness.

The common enablers of this revolution are the underlying networks allowing information exchange and the vast storage capacity available where terabytes of digital data are now standard even for home computers. While initially such networks were often limited to a single enterprise, the entire world has since grown to rely on the pervasive use of large information networks, including the Internet and, more recently, the virtualisation of resources through the adoption of concepts such as cloud computing[2].

**The dependency of the economy on such ICT systems is both a main driver for innovation and a major weakness of operations**:

- A main driver because the increased outreach has led to exponential growth and the exchange of sensitive data and information is today vital to the protection of political, societal or economic interests of all countries.
- A major weakness because the pervasiveness and connectivity of infrastructures have made it virtually impossible to unambiguously identify the main operators. Therefore, when failures occur, the chain of responsibility is unclear and structured emergency and recovery plans are difficult to define, while in parallel economic or even life-threatening impacts can reach dimensions that are often huge with respect to the initial cause of failure.

In addition to failures, the dependency of the economy on information networks has also given rise to the emergence of criminal activities that intentionally target them. We increasingly see attacks targeting public and private critical infrastructures as well as identity thefts affecting the privacy of citizens and the operations of businesses. Security has moved from a contained environment to one whose limits have moved beyond single corporations and indeed into the entire space, leading to the introduction of the "cyber security" terminology.

The US government has made important investments on intelligence and cyber security. In Europe, the approach and funding is more fragmented (often also national level).

The EU Market linked to ICT / cyber security is wide and unstructured having as main stakeholders the Consumers (Citizens), Professionals (Operators: public or private), Administrations and Solution / Technology / Services Suppliers.

In this complex context, security for national infrastructures has become a top priority in the vast majority of EU Member States. Unfortunately, as will be seen in the following, the protection of these essential assets is insufficient, and more remains to be done. **Our approach is to support this priority through a Secure-by-Design framework** (further developed in annexes I and II), **within a comprehensive European policy, applied across all ICT systems on which Critical Infrastructures operate.**

[2] Cloud computing is the provision of dynamically scalable and often virtualised resources as a service over the Internet on a utility basis. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing services often provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers. Cloud computing is capability that provides an abstraction between the computing resource and its underlying technical architecture (e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

# The environment of Cyber Security

## *ICT systems within Critical Infrastructures*

As introduced, the role played by ICT systems in Critical Infrastructures has become fundamental. It is therefore important to clarify the systems that we are targeting, in terms of what a system actually means as well as the scope of our approach in increasing their security levels and applying a Secure-by-Design approach.

**A Critical Infrastructure (CI) represents any environment, small and large, active in isolation or in connection, regional, national or trans-national, whose operations are critical to the everyday lives of citizens, administrations or industries, and whose failures can lead to large and / or catastrophic impacts.** The ICT systems we are addressing support such environments. In some cases, the ICT systems themselves constitute a CI.

From a theoretical point of view a system is a set of interacting or interdependent entities, real or abstract, forming an integrated whole. In the ICT world, these so-called entities can be incarnated by a vast variety of components ranging from small to huge. On the small side, a hardware component used in the control system of cars, airplanes and other transport means requires a high security level to avoid any outside tampering with its programming and operation. On the larger side, the information systems increasingly linked together to manage the electricity distribution and power balancing across European countries have to, collectively, reach a security level that protects them from accidental failures and criminal activities.

To ensure that the target ICT systems are well understood, let's consider the following examples.

### SCADA[3] environments

It is now well understood that the SCADA systems currently in operations, running many segments of our Critical Infrastructures in the field of electricity, water, oil & gas and transportation, suffer from many security weaknesses. Only very recently in April 2009, the US government has admitted that the nation's power grid is vulnerable to cyber attack. This situation is sometimes aggravated as these often relatively old systems have been designed to satisfy drastic safety requirements but with little care devoted to security. In addition, they often rely on huge networks spanning across wide geographical areas with equipment located in very remote locations. Security upgrades, often involving hardware, are made difficult, and consistent implementation of security is a true challenge.

Unfortunately, the history is still running and "improvements" are applied to these environments often without a prior comprehensive security assessment when introducing either new IP[4] based equipment, open Operating Systems or links with the standard IT of the corporate world.

On the other hand, the situation is improving through a new emerging security culture, but the levels of maturity vary with the sectors which have been exposed earlier to these threats being more advanced. It is therefore necessary to support all sectors in reaching the necessary security level.

[3] Supervisory Control And Data Acquisition

[4] Internet Protocol

In these often large legacy systems, the goals are to:

- **improve the federated security through increased interoperability and collaborative management of the infrastructures;**
- **identify the local vulnerabilities of the environment and recommend targeted improvements to decrease the open-doors into the overall system.**

### Telecommunication networks

With the emergence of an increasingly interconnected world, the telecommunication networks have reached out and spanned across the globe. In the meantime, entire countries have and are moving their administration to computerised environments, with the goal of increasing the efficiency of their operations both within their own governments and in offering services to their citizens and industries.

Recent events have shown that while this approach represents positive advances in terms of accessibility to information, at the same time the vulnerability of these regions and countries has largely increased when attacks, such as repeated denial-of-services and organised botnets[5], come into play. In this case, the vulnerability lies in the fact that the redundancy of the underlying networks is insufficient and therefore attacks can be achieved relatively easily by targeting a small number of identified nodes. In some cases, redundancy could have been implemented, but was simply not thought about in the initial design. In other cases, the existing telecommunication networks do not even allow such a redundancy to be implemented without going to expensive back-up solutions involving satellites, for instance.

In these environments, the goals are to:

- **decrease the risks of criminal activities by identifying the key entry points that have to be protected;**
- **identify as soon as possible (few minutes) cyber attacks, especially to critical nodes, and the identity of those who perpetrate the attacks in order to mitigate and respond;**
- **identify the necessary redundancies in the underlying environments and optimising the cost of implementing the minimal level that is required;**
- **identify the potential collaborations that can span across the borders to effectively create redundancy through international operating plans that can be put quickly into force whenever necessary.**

### Consequences

What these two examples demonstrate is that **ICT systems do not constitute a single family to which a single solution can be applied**: on the contrary, it is their diversity that constitutes both a huge potential and a major difficulty. Even the hardware components that are included in every element of our environment, from cars to infrastructure management systems, from household appliances to strategic control systems, have to be considered. Indeed, because of their integration into these systems, they can, either in isolation or together, constitute major vulnerabilities.

Our strategy therefore applies to ICT systems whose failures can prove dramatic for the infrastructures they support.

[5] Collection of compromised computers (called Zombie computers) running malicious software under a common command-and-control infrastructure. Botnets in effect create temporary computer networks used to, for instance, create attacks targeting servers by requesting nearly simultaneous access, thereby moving beyond the maximum answer capacity of the servers and bringing down the services provided by these servers.

## *The Cost of Cyber Security*

The next step is to analyse the security breaches that have to be avoided. Due to the connectivity evolution, security has evolved into **cyber security, which can be expressed as the threats to personal, corporate and national security, safety and resilience caused by breaches in the globally-interconnected digital information and communications infrastructure known as "cyber space".**

For instance, the UK Government recently released its Cyber Security Strategy in June 2009, with its vision:

*"Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience." – UK Cyber Security Strategy 2009*

*"Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our position in cyber space" – Rt Hon Gordon Brown MP, UK Prime Minister*

To address these challenges, the UK Government announced the establishment of an Office of Cyber Security (OCS) to provide strategic leadership, and a Cyber Security Operations Centre (CSOC) to actively monitor the health of cyber space and co-ordinate incident response and provide better advice and information to business and the public.

The US is also developing a Cyber Security Plan and has issued a review of its Cyber space Security Policy in May 2009:

*"A growing array of state and non-state actors are compromising, stealing, changing, or destroying information and could cause critical disruptions to U.S. systems… It is the fundamental responsibility of our government to address strategic vulnerabilities in cyber space and ensure that the United States and the world realize the full potential of the information technology revolution." - White House Cyber space Policy Review 2009*

*"Cyber threat is one of the most serious economic and national security challenges we face as a nation" - President Obama, May 29 2009*

**Cyber security is not only about reducing the risk of these threats, but also about exploiting opportunities to secure personal, corporate and national advantage in the use of cyber space.**

While cyber security is a complex issue, the best approach to defining its importance is to position it in a global economic context.

Indeed, when national infrastructures are implemented and operated, their primary goal is not security but a driver of economic and social services such as delivering energy, operating transport infrastructures, supporting services for the citizens ranging from governmental to health and education etc.

With respect to this function, security is perceived as a necessary feature, but not as a key contributor to the economics of the infrastructure, whereas on the contrary the financial impact of a non-functional infrastructure or even worse, the impact of malicious operations following the theft of information, the injection of wrongful processes etc, can expand far beyond the original cost of implementing security.

In other words:

- the evolution of connectivity has led infrastructures to rely on pervasive networks
- the accessibility of the Internet with 1.5 billion connected individuals has opened many more doors to intentional and unintentional errors
- security has moved from a feature to protect operations within known frontiers to a function to be managed in the whole cyber space.

In this context, security is not a technological issue but is a complete and complex mindset involving all organisations and individuals. Technology supports its implementation but does not guide its proper operation.

The real challenge facing operators is therefore to reach the best compromise in terms of cost / functionality at the level of security *implementations* and *processes*, taking advantage of the cyber space that provides them on the one hand with accrued access to information, faster intervention capabilities and on the other with a giant leap in vulnerability.

But what is the real cost of cyber security? Is it the cost of implementing the features, or of not implementing them?

### *The Threats to Cyber Security*

Consider the following examples. As early as 2005, 1.2 million credit card accounts of the Bank of America were hacked – with a direct impact on 900,000 Pentagon employees[6]. In July 2009, hackers accessed company confidential information of Twitter that was stored on cloud based Google Apps– putting in jeopardy the 7 million $ plan by Los Angeles to also shift to cloud computing based applications.[7] In 2009, the UK Financial Services Authorities fined bank HSBC a total amount of 3 M£ for failing to put in place adequate security measures to protect data.[8]

Beyond these security breaches that are confined to the online world, cyber security also impacts the physical world – and the awareness of the cost and reputation impact is increasing. For instance, water utilities and other plants have become direct targets for such incidents, with both insiders and outsiders identified as the originators of the malfunctioning. The recent article "Is your plant secure" [9] on the Water & Wastes Digest portal highlighted the following examples.

In 2008, a Polish teenager turned the tram system in the city of Lodz into his "own personal train set" by taking control of the tracks. Four trains were derailed and several had to make emergency stops. In Australia, a disgruntled employee of a municipal wastewater station used his knowledge of its control system to discharge large amounts of wastewater into the nearby environment. Consequences of these cyber attacks are that plants lose extremely valuable assets such as computer networks and actual equipment, environmental damage is caused, area security is threatened and monetary damage is most certainly done.

As these examples highlight, cyber security breaches can impact many different areas, and their financial consequences can reach far beyond the initial cost of increasing the security of the infrastructures.

As shown in Figure 1, the impact of cyber security breaches can be classified into the following key areas:

[6] http://www.time.com/time/nation/article/0,8599,1032140,00.html
[7] http://www.cio.com/article/498237/Twitter_Breach_Revives_Security_Issues_with_Cloud_Computing
[8] http://www.fsa.gov.uk/pages/Library/Communication/PR/2009/099.shtml
[9] http://www.wwdmag.com/Is-Your-Plant-Secure-article9171

- **National security**. This can be compromised through the unauthorised disclosure of national intelligence and secrets or by the intrusive manipulation of systems that control critical national infrastructure.
    - Whole nations can be the target of cyber attacks, such as Estonia in 2007, which faced effective distributed denial of service attacks using a range of techniques from an overwhelming amount of low level internet traffic through the command of botnets[10]. The target of the attack ranged from parliament, banks and media enterprises within Estonia for a sustained period and caused disruption to various services albeit for confined time periods and limited impact.
- **Economic security**. Intrusions into systems that support critical business operations such as the financial systems that underpin stock markets can cause significant financial losses to business and individuals and have the potential to cause damage to the economy. Risks to personal financial security (such as identity theft and credit card fraud) are also important.
- **Public safety and Citizens' protection**. The manipulation of systems that control critical national infrastructure, such as water and energy utilities could lead to life-threatening situations posing a serious threat to the safety of the public. Threats to personal data and misuse of Identity can affect Citizens' privacy and cause serious damages to societal and economic life.
- **Environmental protection**. As well as the threat to public safety, breaches in the security of critical national infrastructure can also lead to physical damage being done to the environment.
- **Quality of Life**. All of the above have a significant effect on the quality of life of the citizens.

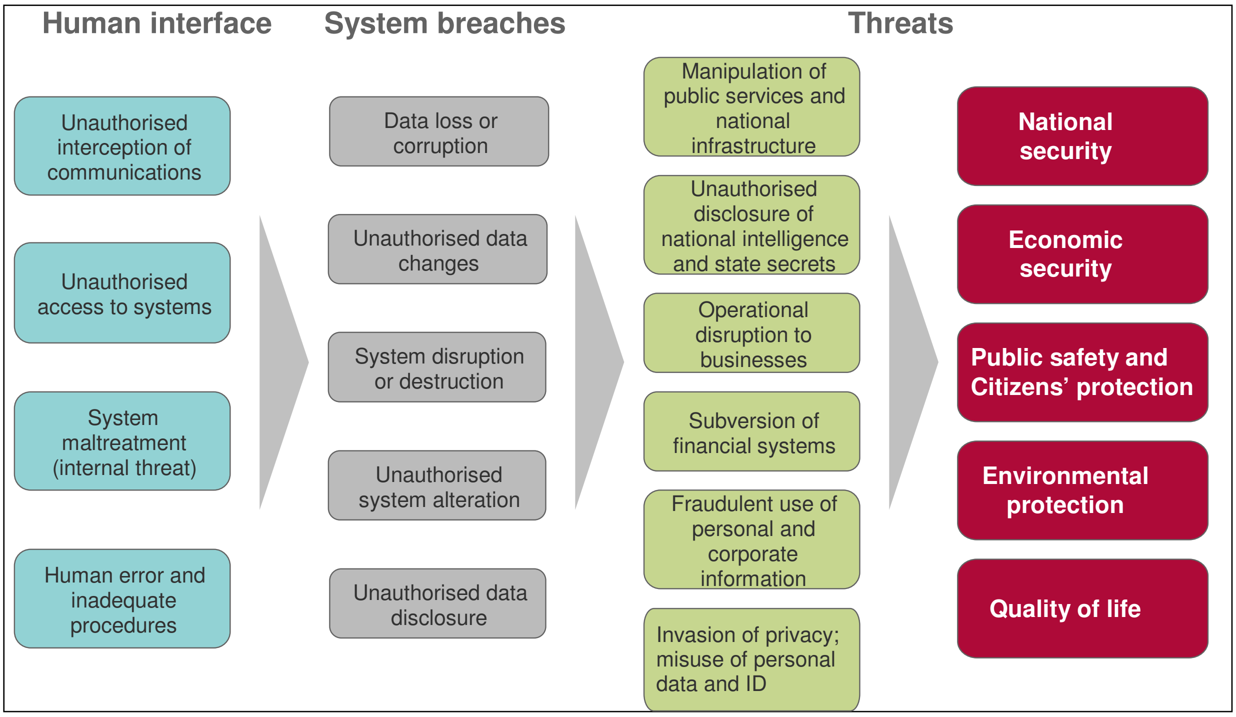

Human interface
System breaches
Threats
Unauthorised interception of communications
Unauthorised access to systems
System maltreatment (internal threat)
Human error and inadequate procedures
Data loss or corruption
Unauthorised data changes
System disruption or destruction
Unauthorised system alteration
Unauthorised data disclosure
Manipulation of public services and national infrastructure
Unauthorised disclosure of national intelligence and state secrets
Operational disruption to businesses
Subversion of financial systems
Fraudulent use of personal and corporate information
Invasion of privacy; misuse of personal data and ID
National security
Economic security
Public safety and Citizens' protection
Environmental protection
Quality of life

**Figure 1 - the impact of security breaches** © Detica 2009

[10] Botnets are networks of computers enrolled either willingly or unwillingly through viruses and used to, for instance, create attacks targeting servers by requesting nearly simultaneous access, thereby moving beyond the maximum answer capacity of the servers and bringing the services provided by the servers down.

These potential threats can be the result of breaches to system and data security, specifically:

- Data loss, corruption and manipulation.
- System disruption, manipulation and destruction.
- Unauthorised data disclosure.

Primarily system breaches are caused by unauthorised access to systems or the interception of communications, but also significant damage can be caused by human error or lack of judgement due to inadequate policy, processes and procedures.

It is imperative to understand the human factor at play in the potential proliferation of these threats:

- **External:** where the breach is from an external unauthorised actor. These actors can be terrorists or have a political motivation, criminals seeking personal gain from fraud and extortion, but also thrill-seekers and people who seek notoriety within the hacking community.
- **Internal:** where the breach comes from an internal authorised user. For example, a breach can be perpetrated by a disgruntled employee. The extent to which damage can be done by an internal source indicates inadequate security policy, processes and procedures and underlines the need for ICT security to be considered and integrated with the entire security management system of an organisation.

The picture that emerges is complex: not only can security breaches originate from both internal and external sources, but security itself encompass a series of domains whose list is in constant evolution.

For instance, the Annual Security Survey[11] organised for the financial world prioritises every year the topics included within the security domain. It also rates the security operations of financial institutions across the world in terms of governance, investment, risk, use of security technologies, quality of operations and privacy. Even within the list of security technologies, the list of domains is changing with access and identity management often high on the list, closely followed by privacy[12], resilience, data protection and other such topics.

Overall, all these elements strongly support the fact that security requires a comprehensive approach, and while innovation is fuelling the technology to provide more and more advanced solutions, innovation is also helping criminal organisations to become increasingly devious in their attacks.

As a consequence, the expansion of security needs is exponential, and the operators are learning it the hard way – by taking the necessary actions and, sometimes, being fined large amounts, when security breaches occur.

**The goal of EOS is to shift this reactive, costly and potentially dangerous approach to one in which cyber security becomes:**

- **a more proactive and efficient mechanism that can enable business processes,**
- **an opportunity at the implementation and operational levels,**
- **a positive discriminator in the business scenarios.**

The goal of the EOS ICT WG is to support this shift.

[11] « Protecting what matters - the Sixth Annual Global Security Survey » by Deloitte Touche Tohmatsu

[12] “Privacy requires security, not abstinence » – MIT Technology Review – 2009 – July-August issue

# Current Gaps and Needs

Based on our state-of-the-art analysis and the informed understanding of our ICT experts, ICT security can be attributed to the following gaps and unaddressed needs.

## *Operational issues*

### ***Lack of sufficient awareness and expertise on the importance of ICT security on part of most CI operators***

To begin with, critical infrastructure (CI) **operators do not necessarily have all the expertise or even sufficient awareness of security issues** regarding the systems they procure or develop. Often, the **business functionality remains the primary driver, while security is considered a possible constraint at best, or even managed as an afterthought**. This state of affairs results in **late implementation, patched-up solutions** and leaves little room to address the needs at the required level. Moreover, at this late stage of implementation, the **available options are usually much more expensive: a fact that often prohibits their correct implementation**.

It is important to note that this factor varies significantly from one CI sector to another and from one class of system to another since the maturity level is not the same. For example, corporate information systems or transactional systems have been exposed to security considerations much earlier than SCADA environments.

### ***No incentives for the implementation of ICT security measures***

Today's reality is harsh: while security is always high on the wish list of Critical Infrastructure Operators, it is **rarely designed into the systems from the beginning**. Although the **"Secure-by-Design" approach** is not a new concept, **it is still not applied yet**. Indeed, **if security is not expressed as a requirement by a customer, it is unlikely that suppliers will include it in their proposed solution since the extra cost will make them uncompetitive** by comparison to a less secure option. Unfortunately, less security aware customers tend to work with **less security orientated providers,** thus **creating "niches" of particularly exposed infrastructures**.

In this approach, security is rarely perceived as an opportunity. However, when analysing the direct financial impact of security breaches, it is clear that the return on investment of security implementation and operations can be huge. In addition to the financial impact, the negative image generated by the often well-publicised malfunctions can be even more destructive to the operator than the direct financial cost.

Another factor is that **security design capabilities require stakeholders both to have developed the associated internal project management processes, and to have recruited people with appropriate skills to manage them.** These two factors make it challenging for most providers to be in a position to propose a robust security service as part of their general offer.

**Security is considered as a constraint rather than as a compulsory feature, and no incentive is provided to CI operators and to IT suppliers to ensure that it is built-in from the start and managed during operations.**

### *Lack of a common approach*

Although this situation is certainly not the reality for all CI operators, the fact that **Critical Infrastructures are largely interdependent propagates the issue of security and necessitates that the whole CI community stakeholders apply the appropriate security level to their infrastructure in order to ensure a collective level of resilience**.

Indeed, failure of one particular CI has an impact not only on its own sector, but also on other sectors.

In addition to cross-sector interdependencies, the **issue of propagation is further enhanced by the fact that the CI community nowadays expands far beyond national borders**. This was recognized by The Future Group Report[13] which highlighted that "An EU **Secure Management Information policy** would help promoting a coordinated development of information technology, providing a **coherent approach to the secure exchange of information**, for a professional, business-oriented and cost-effective use of information technology and information networks."

The recent EC Communication, proposing the "Stockholm Programme"[14] for the JLS security policy for the next 5 years, underlines that security in the EU depends on effective mechanisms for exchanging information between national authorities and other European players. *"To achieve this, the* ***EU must develop a European information model*** *based on a more powerful* ***strategic analysis capacity and better gathering and processing of operational information.*** *This model must take account of existing systems, including those in the customs field, and overcome the challenges of exchanging information with non-member countries."*

## *Administrative, Regulatory, Governance and Procedural issues*

### *Lack of a common EU Directives and regulations*

The concept of **Operator Security Plans (OSPs)** as defined by the European Critical Infrastructure Directive[15] and initially applied for Energy and Transport infrastructures (though at national level, without EU guidelines across countries and applications) is an example of practical progress already made towards collective resilience building based on an innovative approach that considers critical asset identification, risk assessment, the implementation of a risk mitigation strategy.

However, EU Member States are called to define a comprehensive concerted action and interoperability has to form an integral part of federated security. For instance, an EU Secure Management Information policy, e.g. through OSPs for the ICT sector, is in the making but will not be defined by the EU before 2012[16].

[13] Future Group, *"Freedom, Security, Privacy – European Home Affairs in an open world"*, June 2008. Future Group publications can be viewed at http://www.bmi.bund.de/cae/servlet/contentblob/128608/publicationFile/8341/European_home_Affairs_executive_summary_en.pdf

[14] COM (2009) 262 final "An area of freedom, security and justice serving the citizen".

[15] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 - "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[16] SEC(2009) 766 - JUSTICE, FREEDOM AND SECURITY IN EUROPE SINCE 2005: AN EVALUATION OF THE HAGUE PROGRAMME AND ACTION PLAN - An extended report on the evaluation of the Hague Programme.

The EC communication on Critical Information Infrastructure Protection (CIIP)[17] is a welcome step forward in promoting the involvement of the private sector in supporting the definition of the CII Directive and proposing measures for the implementation of the foreseen activities. It should consider all infrastructure connected via ICTs, Telecom, Scada, ATM (Air Traffic Management) etc, otherwise all the different approaches selected for the implementation of ICT security measures persist, affecting the overall security and resilience of Europe's infrastructure.

Actually, the present **situation is unsustainable** both **from a security point of view and from a macroeconomic perspective, as it contradicts the EU's vision of a common market, which requires that operators implement security to similar requirement levels across countries,** responding to the needs of an open, global market without frontiers or other limitations. A truly common market will avoid contingencies that may lead to undesirable effects such as the distortion of market competition arising from uneven costs of security risk mitigation requirements.

Deeper links between the private sectors and the National Administrations, CERTs and EU bodies (ENISA) should be established as the private sector is at last the sector where the security solutions are proposed and implemented. Also European institutions (EC DG INFSO and ENISA, but also other DGs active in Critical Infrastructure Protection – DG JLS, DG TREN, and DG ENTRE etc.) are important partners to support a European approach and coordination of activities.

Looking at traditional EU suppliers for ICT security solutions and services, we still see a low coordination and weak impact at EU / international level (though could be important at national level to protect sensitive MS networks). **Europe has still to create a strong and competitive ICT security industry to propose its solutions and services across the world.**

## *Technical and Services issues*

Today, technical solutions exist that adequately address the security needs. However, while technical issues could be considered as less important than the two previous topics, we highlight the need to ensure a system approach and a coordinated strategy for the deployment of technical solutions with a focus on the specific context of cyber security.

### *Lack of a system approach to the implementation of security*

Even when security is taken into account, it is often implemented in isolation or, worse, through an assorted set of dedicated or add-on modules: a firewall for network security, a VPN[18] for secure communications, a crypto circuit or boards for cryptography implementation, etc.

Such implementations often consider that these specialised subsystems are perfect, resistant and cannot be compromised. Sometimes, additional organisational measures are implemented, such as password policies, revocation, etc. However, experience has shown that there is no perfect system.

[17] COM(2009) 149 - on Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience".

[18] Virtual Private Network.

This subsystem approach does not take into account the system view, nor does it support the changes that are inherent to the dynamicity of real systems.

Even the most sophisticated hardware systems (smartcards or crypto modules) can be attacked and compromised.

Security issues, including attack possibilities and attack models, have to be taken into account in the early design phase of a system and be considered at its core. Redundant security is also a key element for complex and critical systems, as well as for ensuring the security of the security elements themselves.

The implementation of security requires a global view from both the process and technology aspects, supporting a clearly defined governance model.

***Missing coordination for the development of innovative cyber tools to prevent, counter and react to cyber threats***

Several research activities are ongoing at National and EU level for the development of solution to counter cyber threats. Yet these developments do not appear today as under a clear unique EU strategy and policy, with well defined and coordinated requirements for common issues across EU (and beyond).

Secure databases and data exchange are still unstructured in the EU. An increased coordination among MS is needed.

Cyber tools (e.g. encryption, OSINT intelligence for terrorism and economic knowledge, etc.) should also be developed and used in a closer coordination across MS in a more comprehensive view.

## *The need for an end-to-end approach*

To face current challenges to ICT security, stakeholders can already benefit from elements such as existing standards, tools and use of guidelines.

These elements have different purposes and can prove indispensable in various fields of application (e.g. software coding, hardware development, Information System architecture design) or at various stages of system life cycle (design, development, operations and maintenance).

- **Among processes for secure software development**, Microsoft's Security Development Life cycle (SDL), OWASP's[19] Comprehensive, Lightweight Application Security Process (CLASP[20]) and McGraw's Touchpoints[21], are recognized as the major players in the field.
- **Regarding the security of the data itself**, the set of standards and guidelines known as Federal Information Processing Standards (FIPS[22]) have been designed and are compulsory when compelling US Federal Government requirements such as security and interoperability are not met by existing standards.

[19] OWASP – Open Web Application Security Project at http://www.owasp.org/index.php/Main_Page
[20] CLASP – (Comprehensive, Lightweight Application Security Process) - http://www.owasp.org/index.php/Category:OWASP_CLASP_Project
[21] "Software Security: Building Security in " – Gary McGraw – Publisher: Addison-Wesley, 2006 - ISBN – 0321356705, 9780321356703.
[22] FIPS – Federal Information Processing Standards - http://www.itl.nist.gov/fipspubs/index.htm

- **Concerning methodologies for assurance**, the Common Criteria[23] provides assurance that the process of specification, implementation and evaluation of a product has been conducted in a rigorous and standard manner. But while Common Criteria can deliver fully valid results, its applicability is realistically limited to dedicated sub-systems. The use of Common Criteria applied to the security architecture of a system of systems would be arduous. Similarly, the Systems Security Engineering Capability Maturity Model[24] (SSE-CMM) covers all phases of the development cycle and thus can be used to evaluate and improve an existing process.

But while these elements already demonstrate that there is no lack of technical standards, none of them provides a simple answer to all the issues. Indeed, security cannot be addressed simply from the technical view point and in isolation.

On the contrary, **the implementation of security is fundamentally a governance issue**. The technical implementation of security is the consequence of strategic business requirements and/or regulatory frameworks. In this context, it would therefore be beneficial to act at this governance level to promote and foster the inclusion of security objectives for Critical Infrastructure operators concerning the deployed ICT infrastructures that support of their operations.

Therefore, while existing standards, tools and guidelines address specific security aspects, they do not address the complete security cycle which requires a comprehensive governance approach. This is what we intend to develop through the "Secure-by-Design" framework (further detailed in annexes I and II) and its supporting European policies.

## Proposals for Change: EOS recommendations

The ICT domain is critical in two different dimensions: as the underlying support to other critical infrastructures such as in the energy, transport, finance and other domains, as well as when the ICT infrastructures themselves are considered critical. Both dimensions are fundamental in targeting the future.

If we want to face the growing and global threats to infrastructures leveraging on ICT (Information and Communication Technologies), not only do **ICT security capabilities of national public and private users/operators need to be increased, but also the competitiveness and competence of the European ICT security providers has to be strongly supported.**

Based on the previous analysis, we focus our recommendations to address the **need of a common EU approach to enhance the security of ICT systems and ICT CIs, taking into account the cross-sectoral and cross-borders realities** while at the same time moving from an approach of security as a constraint to security as an opportunity and a positive discriminator.

[23] Common Criteria methodology at http://www.commoncriteriaportal.org/

[24] Systems Security Engineering – Capability Maturity Model - http://www.sse-cmm.org/index.html

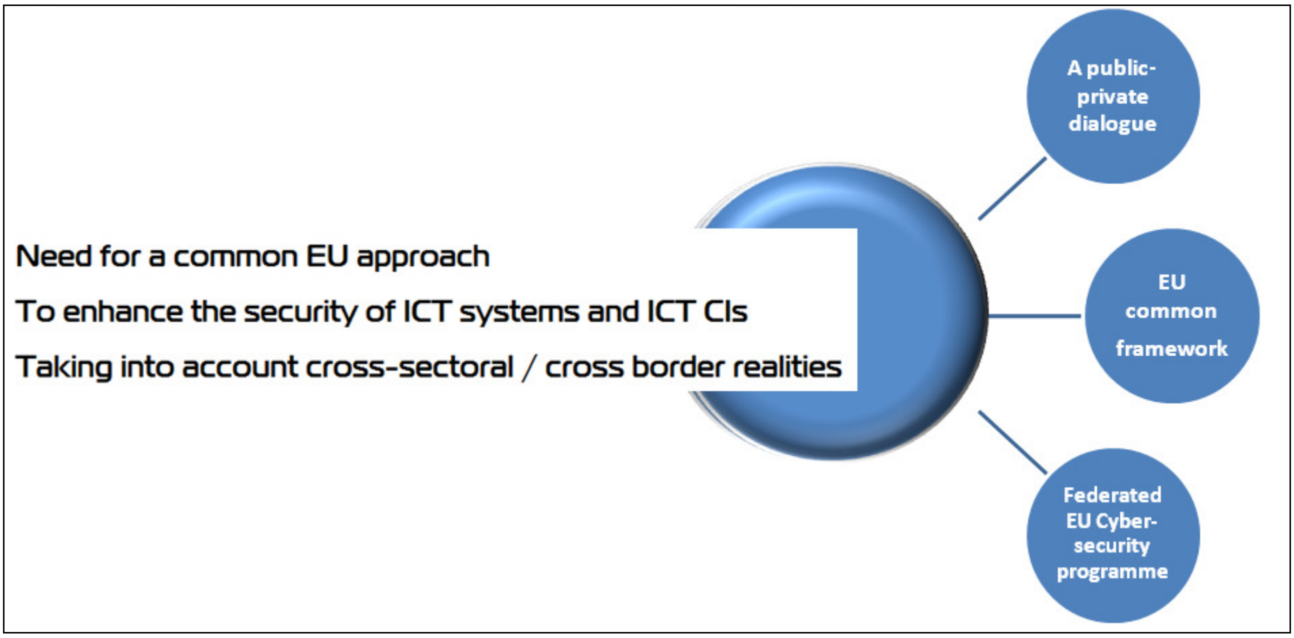

Need for a common EU approach
To enhance the security of ICT systems and ICT CIs
Taking into account cross-sectoral / cross border realities
A public-private dialogue
EU common framework
Federated EU Cyber-security programme

Figure 2 - the EOS recommendations

Such an approach would prove **beneficial for the interoperability of security solutions and enhance the consistency of the critical infrastructure landscape.**

Moreover, making an early move towards common requirements could give EU industries a competitive edge on the international market as being a step ahead on the security implementation.

Finally, implementing security in an integrated manner from the earlier stages of a project is more cost effective than late solutions.

Indeed, since the identification of risks is more accurate, it allows for more effective security budget allocation (i.e. implementation of the right security level at the right place), it aligns with security governance models and avoids expensive solutions which often provide limited efficiency in certain contexts.

In order to realise these benefits, thus remedying the above-mentioned gaps and needs, EOS proposes the following recommendations.

## Recommendation 1 – Build a comprehensive public-private dialogue with all relevant stakeholders (telecom, energy, transport, finance etc.) on the issues at stake

An increased **dialogue and cooperation between MS and EU Institutions as well as the private sector** (operators and suppliers) could **identify common issues across EU countries for cyber security and the protection of ICT networks, defining ways and means for the development of common tools and solutions** (including: technical standards / procedures, sharing of best practices etc) to allow, when requested, a secure exchange of data or reinforced ICT network protection. This dialogue should also allow the EC to elaborate a common framework to secure Europe’s information systems.

The **establishment of a Public-Private Dialogue to address the security and resilience of Information and Communication Networks and Critical Infrastructures based on ICT solutions** (i.e. all infrastructure networks leveraging on ICTs: transport, energy, finance, supply chain, but also the Internet, Administrations, etc.) has been proposed in the recent EC communication on Critical Information Infrastructure Protection (CIIP) of March 2009 with the **creation of EP3R** (European Public Private Partnership on Resilience).

Such a dialogue on CIIP should **lead to concrete actions for the development of common capabilities and processes, and facilitate the adoption of common solutions and/or procedures across different countries and their critical infrastructures for CIIP as an extension of the present EPCIP**[25]. It should be based on the following main principles: **Representativeness, Participation** and **Trust.**

It should build on the engagement with organisations already well established within the cyber security arena in order to fully understand the starting point, clearly define the targets and exploit existing best practices and tools.

In particular it should:

1.1 **define the Objectives, the Roadmap and the Agenda for the P-P Dialogue** as the first act of this initiative. Representatives / experts from public Administrations (national and EU / international) should gather with representatives / experts from the private sectors (users, operators, security solution suppliers) to define these major initial issues;

1.2 **support a well defined EU policy on protection of Europe from large scale cyber attacks and disruptions of CIIs.** Development of a policy on CIIs is a prerogative of Member States, but considering that a large part of CII are own or operated by the private sector and that the private sector is very competent in providing adequate measure to prevent and protect from cyber attacks, it should be **envisaged a consistent support from the private sector in the definition of this policy from the early stage** of the discussion via this P-P Dialogue;

1.3 **point out the role of ICT networks** as enablers of security, as well as the impact of interdependent Critical Infrastructures on security **to the critical infrastructure operators**;

1.4 **exemplify that many environments are candidates to further security**, and that failures have a large economic impact;

1.5 **increase the level of awareness and understanding** of how ICT underlying networks can contribute to raising the security of Critical Infrastructures;

1.6 **highlight the fact that increasingly interconnected or, at the minimum, interdependent Critical Infrastructures demand common security requirements** that in turn presuppose higher levels of managed interoperability – across countries, across organisations, across legislative environments and cultures;

1.7 **demonstrate** that when these points are not addressed or not fully understood, ICT components create **additional weaknesses that open the door to malicious attacks and human errors**;

1.8 establish an international observatory to clearly **monitor and identify** cyber-security threats in a credible, common and efficient manner;

[25] EPCIP : European Programme for Critical Infrastructure Protection. See also : http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm

1.9 **identify security activities and their scope for possible common requirements and interoperability**, and allocates the responsibilities for the implementation of these activities and requirements;

1.10 **raise awareness on the on current security threats of all users/operators,** and **technology solutions / capabilities that can already be offered** by the Industry;

1.11 **explain what a Secure-by-Design System is** and what benefits it brings;

1.12 **provide guidelines for the application of security solutions already at design level**;

1.13 **support the development common technical standards** for capabilities and processes;

1.14 **define a methodology for Operator Security Plans that address ICT issues**, as indicated in the European Critical Infrastructure Directive.

The dialogue should be developed under the **initial coordination of the EC Services, leveraging on an enhanced role of ENISA.** The initiative could then be developed into some specific structures, for instance in a **Joint Undertaking (not only for research activities but also for implementation of the policy and of solutions).**

EOS is ready to support this public-private dialogue, and will help by launching the debate with operators, national agencies, the European Commission and other associated stakeholders.

## Recommendation 2 – Define an EU common framework for secure European information systems on the basis of a "Secure-by-Design" system approach

**The EC needs to elaborate a common framework** for secure European information systems **that will:**

2.1 **clearly target the overall cyber security policies** emerging at European and Member States levels;

2.2 **recommend that security forms an integral part of all ICT systems from the initial design phases, and throughout all other stages**, including the capture of requirements, procurement, design, development, technical testing, user acceptance, "go live", operations and maintenance (evolution and interconnections), and the decommissioning phase;

2.3 **ensure a large adoption of approaches such as the Secure-by-Design approach by national administrations and the entire Critical Infrastructures community** as the suitable framework for design and implementation of resilient systems for critical infrastructures**, by incorporating this approach into the common framework, and by encompassing the complete cycle of operations from detection to reaction, recovery and resilience.** A Secure-by-design approach is not in itself a technology approach, nor is it novel – but what is new is the policy support towards its adoption as a process oriented strategy that directly addresses the change in mindset required to fully implement security throughout system implementation and operations. Only in the latter stage does it become specific to its target domain of application. The ICT Secure-by-Design approach is further detailed in the annex to this document, but it should be designed in a way that:

2.3.1 security requirements are captured from the earliest stages through for example the identification of use cases/ misuse cases, attack models, etc.;

2.3.2 risk assessments are implemented in a continuous, iterative approach at each stage of a system lifecycle;

2.3.3 the focus is not only given to isolated vulnerabilities but also considers cascading effects and the incorporation of interdependencies considerations by means of interoperability requirements;

2.3.4 tools are identified to support the approach (e.g. list of attacks, threats, secure coding practices, existing standards);

2.3.5 provisions are made to deal with conflicting requirements (e.g. business functionality vs. security requirement);

2.3.6 autonomous, adaptive security is facilitated;

2.3.7 the functionalities that implement security are themselves continuously assessed, ensuring through an iterative approach that the security level is not assumed to be adequate but extensively monitored;

2.4 **be consistently applied all over the EU, and possible be extended beyond** through internationally legally binding agreements;

2.5 **include a liability model** to protect those operators that invest in security measures in the case of a natural disaster of or a man-made attack, such as an act of terrorism. The actual definition of this liability model and the estimate of the amount of the investment in security that is necessary should preferably result from the above-mentioned public-private dialogue.

Such a common framework could form the basis of and feed into the directive on critical information infrastructure protection which the directive (2008/114/EC) foresees to be elaborated by 2012.

## Recommendation 3 – Establish a federated EU Cyber Security Programme allowing for an homogeneous level of investment in ICT security, while avoiding market distortions

The **development of the previous recommendations, linking different sectors and stakeholders, on common cyber security issues (ID theft, Denial of Service and System interference, cyber espionage, cyber defence etc.)** will bring a stronger support to the fight against terrorism and crime and the protection and resilience of critical infrastructures.

The coordination of means and of approaches could be enhanced with the **creation of a comprehensive EU Cyber Security Programme** to promote specific policies and the management of technical and operational controls necessary for security compliance.

Initial goals could be the creation of **a common understanding of EU readiness and resiliency and its connection with global infrastructures** (including use of innovative solutions on legacy systems) as well as a **common risk assessments methodology** enabling owner/operators, law enforcement officials, and other relevant stakeholders to assess, with a consistent approach, operational risks (including from organised criminal attacks), and that fostering a deeper understanding of how to mitigate and deter attacks**.**

Such initiative on Cyber Protection of Critical Information Infrastructures should of course be driven in the context of a **holistic/ comprehensive approach to security of Critical Infrastructure in order to understand the risks linked to ICT in the overall political, economic and societal context.**

In order to ensure an homogeneous level of investment in security, and to avoid market distortions, **the EC needs to provide financial guidance and support** to operators by elaborating a **methodology for coherent investments and market development.**

3.1. The EC should define **a comprehensive EU Cyber Security Programme**, which **would ideally gather and coordinate EU activities on ICT security that are already ongoing** in the FP7 R&D programmes, EPCIP, the ICT and ICT PSP etc. This approach is **similar to the i2010 programme** which the EC proposed in 2005 and will run until 2010. Indeed, the i2010 strategy brings together all European Union policies, initiatives and actions that aim to boost the development and the use of digital technologies in every day working and private life. This federation approach which has been extremely successful in the environment of the i2010 policies is exactly the one which we recommend for the security policies.

3.2. This Programme could support the **development** of **the basis for an effective common EU information framework in order to increase intelligence capabilities and provide for an effective strategic analysis capacity and processing of operational information to prevent and react to illegal activities, as envisaged in the Stockholm Programme**.

3.3. The EU Cyber Security Programme could be comprehensive also of **EU "Cyber Tools" activities** (gathering, enhancing and coordinating some activities already ongoing in FP7 R&D programmes, ICT PSP etc.) **targeting the development of common criteria, methodologies and possible solutions (**Capacity Building in general) **for**:

- **ICT risk evaluation and risk management, contingency and recovery planning,**
- **improvement of evidence and forensic through the analysis of a huge amount of unstructured data and the tracing of illegal activities,**
- **intrusion detection and protection tools,**
- **fast reaction procedures to cyber attacks and self healing systems,**
- **identification of attack patterns,**
- **systems and data back-up and restoration,**
- **data encryption,**
- **digital identity management,**
- **intelligence (on specific sensitive issues as well as on new threats vectors and attacker communities),**
- **innovative technologies** that enable automated data analysis and improve real-time collaboration,
- **training and support** (including exchange of good practices),
- **global / international cooperation.**

3.4. **Adequate funding should also be foreseen by the EC to support operators in implementing ICT security measures**, facilitating the adoption of these measures across different countries and their critical infrastructures.

3.5. **Member States should prioritise investment** by giving priority to investments in innovative technologies that enable automated data analysis and improve real-time collaboration**, in coherence with the EU approach given by the EU Cyber Security Programme**. These technologies should enable a multitude of stakeholders to join and conglomerate their capabilities to ensure that the right information gets to the right person so that effectiveness and security will be fostered – further highlighting the importance for interoperability across organisations, borders, legal environments and cultures.

To support these recommendations, the EOS ICT Working Group is addressing technological domains that will enable CI operators and ICT stakeholders to deliver a comprehensive implementation of security.

The first challenge is the definition of a Secure-by-Design framework. The EOS ICT Working Group is finalising a Green Paper devoted to this topic and will conduct a survey of Critical Infrastructures Operators to provide an up to date analysis. An annex to this White Paper provides a first insight of the "Secure-by-Design" Green Paper.

# Roadmap

In order to ensure a satisfactory level of implementation and investment in security measures for the protection of Europe' s critical ICT infrastructure, EOS is ready to actively support the EU's efforts and actions deemed necessary to achieve this. We envision the following roadmap.

- **Short term measures at EU level [2010-2012]**
    - Establish a Public-Private Dialogue between the telecom, energy, and finance etc. sectors with defined Objectives, Roadmap and Agenda: establishment of the EP3R Forum for information sharing between Member States involving EOS.
    - Define and EU policy on protection of Europe from large scale cyber attacks and disruptions of CIIs.
    - Establish an International Observatory on cyber security that monitors threats and delivers accurate, credible statistics on incidents.
    - Elaborate the basis for a Federated EU programme on Cyber Security leveraging on existing operational needs and security solutions.
    - Raise awareness on the on current security threats of all users/operators, and technology solutions / capabilities that can already be offered.
    - Provide elements to the new European Commission, the European Parliament and Member States to justify the creation of an EU Cyber Security Programme and a consequent financial support to be envisaged in the 2014 – 2020 EU financial perspectives.

- Initiate definition of common security requirements that in turn presuppose higher levels of managed interoperability – across countries, across organisations, across legislative environments and cultures
- Define a methodology for Operator Security Plans that address ICT issues following ECI Directive needs

- **Medium term measures at EU level [2013 - 2016]**
  - Define a Directive on the protection of critical information infrastructure (CII) to be adopted by 2012 (on the basis of the directive 2008/114/EC). EOS will support help the EC with the preparations of this directive by providing technical insight and guidance to the EC, Member States and the operators based on the Secure-by-design framework.
  - Define an EU common framework for secure European information systems on the basis of a "Secure-by-Design" system approach
  - Implement Phase 1 of the EU Programme on Cyber Security (Definition /Feasibility /Threat and Risk Assessment Phases). EOS will provide support for the effective implementation of this EU programme on Cyber Security.
  - Build on the International Observatory to develop a common EU information framework in order to increase intelligence capabilities and provide for an effective strategic analysis capacity and processing of operational information
  - Develop EU "Cyber Tools" activities targeting the development of common criteria, methodologies and possible solutions
  - Implement the CII directive. EOS will support the implementation of these initiatives by providing technical guidance to the operators.

- **Long term measures at EU level [2016- 2020]**
  - Implement Phase 2 of the EU programme on Cyber Security (Pilot projects & deployment of solutions within operators' infrastructures)
  - Update and integrate the existing systems and services, while adding new components.
  - Introduce the newly developed infrastructures, embedding security solutions (Secure-by-Design)

# About EOS

***The European Organisation for Security*** – EOS – was created in July 2007 by European private sector suppliers and users from all domains of security solutions and services. EOS has today 34 members, representing 12 European Countries. EOS focuses on the market side, and seeks to develop a close relationship with the main public and private actors.

***The main objective of EOS*** is the development of a consistent European Security Market, while sustaining the interests of its Members and satisfying political, social and economic needs through the efficient use of budgets, and the implementation of available solutions in priority areas, in particular through the creation of main EU Security Programmes.

To develop the security market we:

- support the ***development of civil security & resilience systems and related services*** with innovative European approaches that can be used in the global security market;
- support the ***effective implementation of existing/future solutions and services*** (developing interoperable and consistent architectures, interfaces, innovative methodologies and/or common procedures, best practices, pilot projects, etc) by focusing resources on market priorities.

In order to achieve these objectives, and ***believing in the benefit of an effective dialogue between all relevant stakeholders***, EOS welcomes any suggestions and comments to its White Paper.

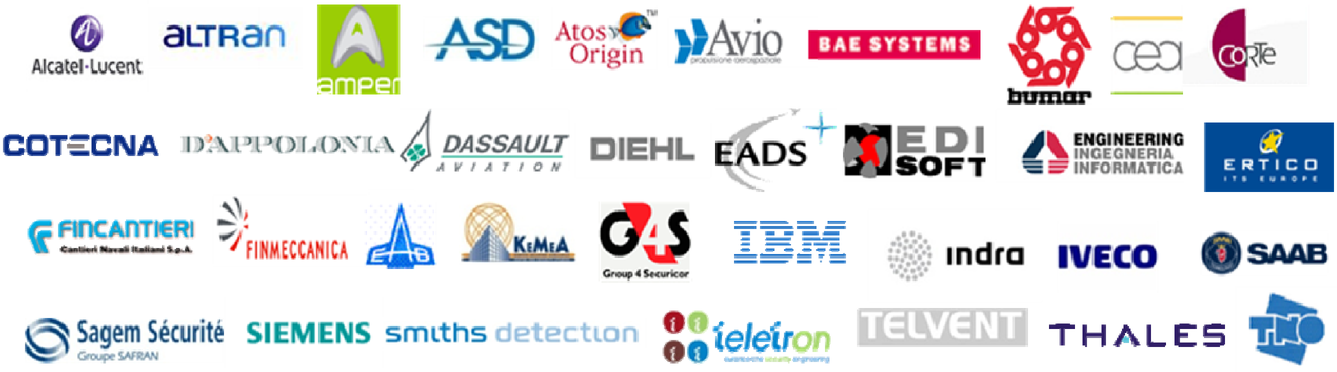
**HOW TO REACT TO THE WHITE PAPER**

Reactions to this White Paper may be sent directly to info@eos-eu.com

Alternatively, you could mail your comments to:

**European Organisation for Security (EOS)**
**270 Avenue Tervuren**
**Bruxelles 1150**

***EOS Members***



**EOS ICT Working Group Participants**

This White Paper is a collective endeavour of the EOS ICT Security Working Group during the last 2 years, with the participation of:

| | | | |
|---|---|---|---|
| ENGINEERING | Veronique | Pevtschin | WP Editor |
| THALES | Fabien | Cavenne | WP Editor |
| ENGINEERING | Dario | Avallone | WG Chairman |
| ALTRAN | Jean-Philippe | Perin | WG Co-Chair |

| | | |
|---|---|---|
| ALCATEL LUCENT | Christophe | De Maindreville |
| ALCATEL LUCENT | Christophe | Mathieu |
| ALTRAN | Cecile-Liv | Müller |
| ALTRAN | Pascale | Lardin |
| ATOS ORIGIN | Jose-Maria | Cavanillas |
| ATOS ORIGIN | Pedro | Soria |
| ATOS ORIGIN | Aljosa | Pasic |
| ATOS ORIGIN | Beatriz | Perrote |
| ATOS ORIGIN | Isabel | Vinaigre |
| BAE Systems | John | Bennet |
| BAE Systems | Peter | Sayce |
| BAE Systems - Detica | Nefyn | Jones |
| BAE Systems - Detica | Steve | Daniels |
| BAE Systems – Detica | Ben | Bridge |
| BUMAR | Tomasz | Miroslaw |
| CEA | Alain | Merle |
| CORTE | Alessio | Sitran |
| CORTE | Rémy | Russotto |
| COTECNA INSPECTION | Mark | Miller |
| D'APPOLONIA | Lorenzo | Falciani |
| D'APPOLONIA | Fabio | Bagnoli |
| DIEHL | Michael | Langer |
| EADS | Bryan | Lillie |
| EADS | Robert | Havas |
| EDISOFT | Filipe | Custodio |
| EDISOFT | Antonio | Sousa |
| ENGINEERING | Giuseppe | Paladino |
| ERTICO | Paul | Kompfner |
| ERTICO | Gary | Bridgeman |
| FINCANTIERI | Gianmaria | Gambacorta |
| FINCANTIERI | Paolo | Lotti |
| FINMECCANICA/Selex S.I. | Gustavo | Scotti di Uccio |
| FINMECCANICA/Selex S.I. | Eugenio | Creso |
| G4S | Mike | Clarke |
| HAI | Nikolaos | Priggouris |
| HAI | Evangelos | Ladis |
| INDRA | Fernando | Carvajal |
| INDRA | Carlos | de Miguel |
| IBM | Peter | Stremus |
| IBM | Alessandro | Faustini |
| IBM | Gerardo | Zuliani |
| KEMEA | Georgios | Leventakis |
| KEMEA | Thalia | Tzanetti |
| SIEMENS | Karl-Heinz | Wocker |

| | | | |
|---|---|---|---|
| SIEMENS | Andreas | Seum | |
| SIEMENS | Hans Jürg | Wieser | |
| SMITH DETECTION | Michael | Andreas | |
| SMITH DETECTION | Raymond | Ray | |
| THALES | Thomas | Hutin | |
| THALES | Milton | Yates | |
| THALES | Lionel | Le Cleï | |
| EOS | Sophie | Batas | WG Support |
| EOS | Luigi | Rebuffi | WG Supervision |

## EOS' competence

*(a list of EOS Members' competences/areas of knowledge relevant to the domain, based on the STACCATO taxonomy)*

**Technologies-Components**

| | |
|---|---|
| 104 | Survivability and hardening |
| 109 | Opto-electronics: Laser, optics and related devices |
| 110 | Sensor Technology and Components |
| 111 | Electronic components |
| 112 | Signal processing technologies |
| 113 | Information technologies |
| 114 | Artificial Intelligence & Decision support |
| 115 | Simulation tools and technologies |
| 116 | Computing Technologies |
| 117 | Information Security Technologies |
| 118 | Communication technologies |
| 120 | Human sciences, including research and studies |

**Equipments and sub systems**

| | |
|---|---|
| 200 | Sensor Equipments |
| 201 | Signal Protection |
| 202 | Identification equipment |
| 203 | Biometric equipment |
| 212 | Forensic technologies, others |
| 219 | Physical access control and Electronic Authentication Equipment |
| 220 | Human Resources |

**Systems-Services Functions**

| | |
|---|---|
| 300A | Risks assessment, modelling and impact reduction |
| 301A | Risks and vulnerabilities assessment |
| 302A | Risk reduction |
| 303A | Protection |
| 304A | Exercise and simulation, training |
| 306A | Identification |
| 307A | Localization |
| 308A | Surveillance |
| 300A | Intelligence |
| 310A | Neutralization |
| 311A | Interoperable secured communications (Security systems architecture) |
| 312A | Crisis Operations / Management – C3I |
| 316A | Psychological and Social aspects |

**Design-Manufacturing**

| | |
|---|---|
| 300B | Operating Environment Knowledge & Modelling Technology |
| 301B | Systems Engineering and Design Management |
| 302B | Systems Certification and Failure Investigation |

| | |
|---|---|
| 303B | Systems Engineering and Integrated Systems Design |
| 305B | Software design validation and maintenance |
| 306B | Simulation and design tools |
| 307B | Installations and Facilities |
| 308B | Ergonomic and Human factors |

**Integrated platforms and systems and HFs**

| | |
|---|---|
| 405 | Simulators, Trainers |
| 407 | Identity management systems |
| 408 | Integrated Surveillance Systems |
| 411 | C2, Information and intelligence systems |
| 412 | Networks and information security systems |
| 413 | Communication Systems |
| 414 | HFs Services to Security |
| 416 | Integrated systems of systems |

**Mission Capabilities**

| | |
|---|---|
| 500A | Preserve the functioning of the State |
| 501A | Ensure Identification and control of goods and people |
| 502A | Ensure and Maintaining Law and Order |
| 503A | Ensure Economic Security |
| 504A | Protection of citizens (goods and people) |
| 505A | Avert and foreseen Catastrophes |
| 506A | Avert and prepare themselves against aggression |
| 507A | Control and surveillance of areas |
| 508A | Protection of areas and infrastructures |
| 509A | Protection of networks |
| 510A | Protection of environment (before, during and after) |
| 511A | Security of transport |
| 512A | Crisis management |
| 513A | Ensure restoration and reparation |
| 514A | Security of nationals abroad |
| 515A | Lead operation for external security |

**Policy and Support**

| | |
|---|---|
| 500B | Security Analysis |
| 502B | Human resources (HR) management for security personnel |
| 503B | Training |
| 504B | Scenario and decision simulation |

# Annexes

## Annex I - Contributing to a "Secure-by-Design" framework: the EOS approach

### I.1 Objectives

The Secure-by-Design framework aims to ensure that:

- security requirements are captured from the earliest stages through for example the identification of use cases/ misuse cases, attack models, etc.;
- risk assessments are implemented in a continuous, iterative approach at each stage of a system lifecycle;
- the focus is not only given to isolated vulnerabilities but also considers cascading effects and incorporates the interdependencies through interoperability requirements;
- tools are identified to support the approach (e.g. list of attacks, threats, secure coding practices, existing standards);
- provisions are made to deal with conflicting requirements (e.g. business functionality vs. security requirement);
- autonomous, adaptive security is facilitated;
- security is implemented in an iterative manner to ensure the security of the "secure functions" which have been introduced;
- the approach allows enough granularity to adapt to the required level of trust;
- the approach is generic / flexible enough to fit almost any context and has the ability to integrate the adequate available standards or tools to specific technical contexts.

### I.2 Take up of advanced secure system engineering practices by industry

The following points are proposed for further consideration and up-take of advanced secure system engineering practices by industry:

- the development of risk based development processes. Risk assessment is a key factor in capturing, specifying, implementing and monitoring security in software systems. Risk-driven development also implies methods for assessing impact and evaluating underlying security costs beforehand and at each level / iteration of software system development. It also underlines the use of common metrics, e.g. impact or security cost;
- the use of common experimental facilities and test data sets for testing and benchmarking new solutions and possibly "European Reference Solutions"[26]
- the transfer and application of best practices from other domains (e.g. from development of defence software systems to civil protection systems);
- the certification of software as a business enabler and EU differentiator from the security perspective, (secure software assurance business models);

[26] "European Reference Solutions" as promoted by EOS as key elements of EU Security Programmes: technologies and capabilities developed and validated following common operational needs, criteria and EU security strategies, for specific missions to increase, when needed, interoperability or compatibility of solutions.

- the support for easier composition of security properties, at run time and in a secure manner, in an environment in which, increasingly, a software system incorporates components provided by different software companies;
- the alignment of the approach to the Architecture Framework structure and procedures to build on existing foundations and increase the acceptance and adoption of the framework;
- the stimulation of accountability and good governance by integrating secure software engineering practices into the IT governance of organisations.

## I.3. Foundations for a "Secure-by-Design" framework

### *I.3.1. Synchronising and integrating security activities in the lifecycle of ICT systems*

As mentioned earlier, our approach is not only to build resilience into Critical Infrastructures as a first line of defence, but also to support, monitor and address security throughout the entire operation of these infrastructures.

To ensure this comprehensive approach to security, security needs to be introduced at the earliest design & development stages of systems and to be maintained through the entire operational life including time of decommission. The complexity stems also from the inherently dynamic aspects introduced by:

- the continuous appearance of new vulnerabilities and threats created by new attack strategies;
- the changes in the existing critical infrastructures implemented by the operators to address evolutions in usage and requirements, such as increasing number of users, changing partnerships etc;
- the additional requirements emerging from the interconnections of Critical Infrastructures;
- the technological evolution through which new innovations and regulations impact the security components and lead to their replacement or additions.

As a consequence, security needs to be addressed at all stages, including:

a) capture of requirements,

b) procurement,

c) design,

d) development,

e) technical testing,

f) user acceptance,

g) go live,

h) operations and maintenance, including evolution and interconnections,

i) decommission.

At each one of these stages, the associated security activities, responsibilities, inputs, outputs, supporting tools and methods need to be identified and typical security activities (like Security Risk Assessment, Security Objectives identification, Security specifications, Security Mechanisms development, penetration testing) need to be clearly synchronised with the system lifecycle. This encompasses:

- *who* is responsible to conduct the activity e.g. responsibility of the business, the security development team, a third party security assessor, etc?

- *how* should the activity be implemented, i.e. what specific available standards or tools should be applied?
- *what* should be covered by the activity?

The purpose is not to reinvent security standards but to make sure that all activities and responsibilities are identified, properly allocated and that their scope is clearly defined.

This approach is still a very initial view, since at this stage of development; the White Paper contributions are limited to EOS partners. It is expected this view will be fully revised and extended following the survey.

#### *I.3.2.2 Expressing & communicating security*

Standards of security evaluations (Common Criteria, FIPS, etc) are based on the idea of a clear description of the security of systems in terms of assets, security policies, security objectives, etc. However, attack strategies and weaknesses equally need to be understood and described and are currently often poorly expressed and therefore overlooked and underestimated. A really secure system needs to integrate various security components, ensuring that they are used in a best fit configuration, but also that the inherent and known security weaknesses of one component are compensated at the system level. In addition, the composition process of security components can introduce new weaknesses that need to be understood, managed and avoided.

The "Secure-by-Design" framework intends to address this lack and enhance the global security level of Critical Infrastructures by adding the identification and subsequent modelling of attack strategies, vulnerabilities and other weaknesses. While the unpredictable will always exist, our goal is to use governance and technology to reduce it as much as possible.

### I.4 Benefits

The primary benefit of the "Secure-by-Design" framework proposed by EOS is to increase the security of Critical Infrastructures and therefore strengthen the protection of EU citizens against a wide variety of threats including terrorism or organised crime targeting cyber infrastructures. This approach clearly targets the overall cyber security policies emerging at European and Member States levels.

The secondary benefit is to ensure that the underlying ICT networks of information and data contribute to enhancing and maintaining high security levels rather than bringing an additional weakness and creating back doors for criminal attacks. This is a preliminary step to contribute to the extension of the European Critical Infrastructures directive to the ICT domain foreseen in 2010, following its current applicability to energy and transport.

To reach such benefits, three major issues have to be addressed:

a) the role of ICT networks as enablers of security has to be fully understood by the Critical Infrastructure operators;

b) operational security needs have to be comprehensively expressed as described in section 3 and easily transferred in terms of requirements to the ICT networks designers and operators; and

c) the impact of interdependent Critical Infrastructures on security has to be fully understood and incorporated at all phases of their lifecycle.

Moving to the next level of details, these benefits have a wide impact across many different aspects ranging from cost efficiency to competitiveness, including:

- Adopting such an approach on a European basis will prove beneficial for the *interoperability* of security solutions and enhance consistency across a critical infrastructure landscape which does not stop at Member States' borders;

- Getting an early move towards a standard could give EU industries a competitive edge on the international market as being a step ahead on the security implementation;
- Implementing security in an integrated manner from the earlier stages of a project is more cost effective than late solutions. Since the identification of risks is more accurate, it allows for more effective security budget allocation (i.e. implementation of the right security level at the right place) and avoids expensive solutions which could prove to actually provide limited efficiency in given contexts;
- Allowing for proactive security versus a reactive approach. Considering that security is a perpetual race between vulnerabilities discovery and countermeasure implementation, this constitutes a very valuable advantage;
- Integrating security as a core capability of the ICT systems also contributes to develop the awareness of the risks an organisation faces by identifying clearly the managed risks, and as importantly the residual risks. This awareness creates an associated security culture that although intangible in itself, is pervasive and a key asset for the resilience of Critical Infrastructures;
- Addressing security as a core feature of any system will also contribute to decreasing the huge economic impact of non-functional systems due to security breaches or accidents.

## Annex II - A possible Secure-by-Design high level framework

Below is a first high level view of what could be a candidate generic security framework. The table is not fully developed at this stage but provides an illustration of the goals to achieve and can serve as a first reference for feature brainstorming- discussion.

| System Life Cycle | Security activity | Responsibilities | Input | Output | Supporting tools and methods |
|---|---|---|---|---|---|
| **Requirements Gatherings And Analysis** | Security requirements analysis and specification – At the requirements gathering and analysis phase, security requirements should be considered at the earliest stage of the definition of business requirements for the information system. Depending on the value of the information assets involved, the nature of the IT system and its business purpose, an appropriate risk assessment process will define the security controls to be considered.<br><br>System requirements for information security and processes for implementing security should be integrated in the early stages of information system projects. Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation. | Business Management<br>Security Officer<br>Business User | Business requirements, information assets value, objectives of the information system and context of operations | High level security objectives | ISO/IEC 27001<br>ISO/IEC 27002<br>ISO/IEC TR 13335-3 |
| **Procurement** | Introduction of clear, measurable, adapted security requirements | Business<br>Procurement Function<br>Security Officer | High level security objectives<br>Business requirements | Security requirements | ISO/IEC 27001<br>ISO/IEC 27002<br>ISO/IEC 15408 |
| | Raising security as a formal factor in the solution selection process | Business<br>Procurement Function<br>Security Officer | Bids from providers | Security evaluation of solutions (tenders) | Security assessment of tenders |
| **Design (activities need to be iterated several times)** | Technical risk analysis implementation | Security lead in design team | First system design elements | | |
| | Validation of risk analysis | Security steering committee meetings (business representatives, technical representatives, security practitioners, etc.) | Draft risk assessment | Validated risk analysis | |
| | Choice of security controls | Security lead in design team | First system design elements<br>Validated risk analysis | System design including security design + identification of residual risks | |
| **Development** | Development of security functions | Development team | Security requirements<br>Definition of security controls | | |

| System Life Cycle | Security activity | Responsibilities | Input | Output | Supporting tools and methods |
|---|---|---|---|---|---|
| | Code security review | Security auditor (external to the development team) | Business requirements<br>Information systems design and technical specifications<br>Source code | Security analysis of code.<br>Identification of potential vulnerabilities and recommendations for risk mitigation. | ISO/IEC 27001<br>ISO/IEC 27002 |
| **Technical Testing** | Security Assessment | Security auditor (external to the development team) | Business requirements<br>Information systems design and technical specifications | Security analysis of final implementation.<br>Identification of possible vulnerabilities and recommendations for risk mitigation. | ISO/IEC 27001<br>ISO/IEC 27002 |
| | Penetration testing | Security auditor (external to the development team) | Final (pre-production) system | Security analysis of final implementation.<br>Identification of possible vulnerabilities and recommendations for risk mitigation. | ISO/IEC 27001<br>ISO/IEC 27002 |
| **User Acceptance** | Security accreditation, approval of residual risks | Business Management<br>Security Officer | Security assessment reports | | |
| **Go live** | Initialisation of security functions (e.g. activation of crypto keys, secure migration of data, etc.) | Security Officer | | | |
| | Secure migration from test to operational environment | Security Officer | | | |
| **Operations and Maintenance** | Development and operation of an ISMS (Information Security Management System) covering:<br>• Incident management,<br>• Regular review s of Risks<br>• Change management,<br>• Business continuity,<br>• Access control management,<br>• Etc… | Security Officer | | | ISO 27001<br>ISO 27002 |
| **Decommissioning** | Secure disposal of sensitive materials | Security Officer | | | ISO 27001<br>ISO 27002 |

Figure 3 - “Secure-by-Design” in system lifecycle matrix