Towards a concerted EU approach to cyber security

An EOS White Paper

July /2010

Version 5.0 – draft July 23rd 2010

EOS ICT / Cyber Security Working Group

EUROPEAN ORGANISATION FOR SECURITY

EUROPEAN ORGANISATION FOR SECURITY

Table of Contents

Executive Summary

This EOS White Paper aims to contribute to **a global "EU Cyber Security Approach",** an approach whose importance is directly related to the huge impact that disruptions to the information networks, including the Internet, can have both in cyber space and on the physical world.

This contribution focuses on **defining cyber security, understanding the threats, evaluating their impact and proposing concrete actions at national, European and international level.**

Cyber security is a term that emerged over the last decade, in parallel with the increased outreach and usage of the Internet and private networks. Cyber security encompasses all issues related to the disruption of these networks and their impacts, in a context where cyber threats are gaining on all counts, from increased visibility to increased impact and coordinated organisation and planning.

While cyberspace can be defined as a virtual world of interconnected networks, it has in effect created a domain much broader than the physical space, without physical boundaries and hence also without a single legislative and regulatory framework. Furthermore, the multiple interconnections of cyberspace with the real world through strategic infrastructures have created the basis for major disruptions, an opportunity that is increasingly taken up by coordinated malevolent organisations.

The motivations that drive the perpetrators of cyber attacks or cyber crimes in the cyberspace are fairly standard, ranging from recreational, activist, illegal, criminal to business or state-sponsored, including terrorism. However, **their means of actions are specific to the cyberspace**, with specificities that make cyber security unique, such as the speed of disruption spreading, the dynamic nature of cyber threats, the asymmetric nature of small threats leading to huge impacts etc.
Today, conservative estimates put European cost of **the impact of cyber threats at over €350 billion**, while the parallel **underground economy** built around the creation and deployment of cyber threats is evaluated at **over €100 billion**. Accurate evaluation of the impact of disruptions is anyway fairly difficult to establish; while direct costs linked to the time to normal operations, the down time of computer systems etc can be quantified, indirect costs linked to the theft of information and of intellectual property, damages to reputations can occur long after the initial disruption and are difficult to repair and evaluate.

Cyber security therefore requires a comprehensive approach, including governance, organisational, legal, tactical and educational strategies supported by technology. In creating this approach, it is fundamental to keep in mind that **it is not the existence of cyberspace but its usage that leads to the need for cyber security.**

There is today a clear political awareness, based on facts, **that cyber threats are becoming a major issue and can impede operations, economic growth and competitiveness. Cyber Security is recognised as strategic for Europe and its Member States,** and the need for **European stakeholders to master the key tools to fight cyber threats** is clearly recognised**.**

However, securing cyberspace introduces a level of complexity that has never been experienced before, and **while Europe and European Member States have taken different initiatives to tackle the issue of cyber security, an integrated approach based on a global EU cyber security policy is missing.** This becomes also

fundamental at the international level, with other regions of the world putting coordinated strategies in place, including collaborations between military and civilian control structures. The need for Europe to tackle this issue in an integrated approach therefore stems not only from its internal reality, but also from the importance of being able to display a single, external representativeness on the international scene.

The 2001 Convention on Cybercrime, the 2008 directive on Critical Infrastructures Protection, the 2009 EC Communication on increasing the protection of Europe from large scale cyber attacks and disruptions, the EU Directive on Data Protection, the on-going creation and networking of CERTs, the 2010 EC Communication on Digital Agenda, the EC research on security and trust are all valuable approaches, but these initiatives lack several important dimensions: the integration of legal and processes aspects with an EU cyber security policy, an enhanced technological education, the public and private commitment to develop an EU Cyber Security Approach and the financial support for its implementation. **How can all these activities be consolidated into a single, coherent EU Cyber Security Approach?**

To foster the development of an EU Cyber Security Approach, EOS focuses its recommendations on two major elements:

- an EU Cyber Security Programme and
- a European Cyber Security Coordinator.

The roles of the **European Cyber Security Coordinator** would be to supervise the Cyber Security Programme; inform Member States of the evolution of cyber threats and solicit them to increase awareness; establish and ensure that the cyber security regulatory framework and the different funding R&D programmes are aligned in terms of policy objectives; develop with EU institutions cyber security policies; monitor and define cyber security exercises; represent the single cyber security contact point of EU Institutions at an international level; define cyber security capacity building needs; increase the collaboration between civil and military handling of cyber threats.

The EU Cyber Security Programme involving all stakeholders, should take place in two steps:

- The creation of a *Public Private Dialogue* for global outreach and trust, allowing the identification of public policy priorities, societal issues, economic dimensions of challenges and means.
- *The creation of a Public Private Cooperation (or Partnership when suitable*) to elaborate and implement a common EU Cyber Security Approach.

Across these two steps, the Programme should be developed along 7 major directions:

1. Policy Definition and Coordination

- develop a **global EU cyber security policy**.

2. European and International Cooperation

- improved and coordinated **governance**;
- create an **European Public Private Dialogue** for trust and increased cooperation;
- common **understanding of cyber security issues** (across MS) **and interdependencies of infrastructures leveraging on the cyberspace**;
- **sharing of best practices** at different levels: **operational, judicial, financial;**
- Member States to increase their level of collaboration: **network of national CERTs having similar levels of capability**.

3. Threat Assessment and Vulnerability Reduction

- develop an **EU risk management methodology for cyber threats** and elaboration of **cyber security incident response plans**;
- **identification and measure of the impacts of cyber security threats and incidents** across all domains.

4. Legal and Societal Issues / Privacy

- **analyse** existing **legal frameworks** and propose evolutions for the establishment of an **EU cyber security legislation / regulatory framework**;
- **EU Charter for development and use of Privacy aware cyber solutions**.

5. R&D, Certification, Implementation

- develop **common architecture frameworks, secure open standards, procedures and secure / trusted tools for sharing data** (EU Model for Data and Information Sharing) **and intelligence**;
- **coordinate R&D of solutions and processes in a "security & privacy by design approach" following a global EU cyber security policy**;
- **elaborate pilot deployments and demonstrations validating defined cyber security environments**;
- cyber security **EU certification programme identifying the level of preparedness and resilience of infrastructures to cyber threats**;
- **financial incentives to implement cyber security** solutions and services;
- **building competencies, implement capabilities and capacities across Europe for main EU security applications**: Border Surveillance (e.g. Common Information Sharing Environment for maritime Border Surveillance); Border Management / checks (e.g. SIS and VIS; cybersecurity-based ID management system at EU level); Civil Protection (secure emergency communications); Secure and legal use of Internet; Secure exchange of Data for Transport of People and Goods; Secure SCADA for Energy infrastructures.

6. Awareness, Education and Training Activities

- organisation of **national and European exercises**;
- **infrastructures to simulate** on a large scale sophisticated attacks, failure modes for common vulnerabilities and reaction means, used also to **test / validate the "security and privacy by design" solutions**;
- establish **professional cyber security certifications**;
- contribution to **citizens awareness and education**.

7. Monitoring & Response Capabilities

- **EU Rapid Cyber Security Capabilities for monitoring and response to cyber attacks coordinated by CERTs with the support of ENISA**: interoperable & interconnectable systems to create "on demand" a virtual network to monitor attacks; cyber security services as a centralised or **networked "watch-and-warning" system** to detect and prevent cyber attacks;
- **EU Cyber Security Capabilities for prevention and prosecution of cyber crime coordinated by EUROPOL** for monitoring information and intelligence; **creation of national "Cyber Polices"** linked to EUROPOL.

EOS, representing the major EU stakeholders active in security **intends to be part of this approach, and participate actively at the enhancement of the Public-Private Dialogue**, **the creation of an EU Cyber Security Programme; the development and validation of innovative technological cyber security solutions and services**; **the promotion of a "secure & privacy-by-design" education and approach; the development of competencies, capabilities and capacities across Europe.**

1. Preface

Following the first issue of the EOS White Paper on "Security and Resilience of Information and Communication Technology Networks for the Protection of Critical Infrastructures"[1], discussions with high representatives of the EU Institutions (Parliament, Council, Commission) made clear the need to enlarge the topic to a **global "EU Cyber Security Approach", better defining what cyber security is, understanding the threats, evaluating their impact and proposing concrete actions at national, European and international levels**.

2. Introduction

Over the last decade, all major communities, from European Institutions to the United States, have introduced cyber security policies to protect nations, organisations and citizens against cyber crime and cyber terrorism, addressing both intentional and accidental disruptions occurring in the cyberspace.

These policies and contributing bodies, ranging from European agencies to national ministries, are at various stages of definition and implementation. However, across all these strategies, **no single definition emerged to fully address what is covered by the term "cyber security"**. Some approaches consider the technological aspects of cyber security while others focus on the legalistic elements. The disconnect between these approaches is not sustainable, when the reality is that **there is no strict border between the real world and the cyberspace.**

As such, **cyber security's role is to protect and enable** the use of cyberspace, thereby enhancing the economy and the citizens' experience in vital sectors particularly when using digital communications and exchange of data, for instance in border control (surveillance and management); crisis management / emergency communications; protection of critical infrastructures (e.g. transport of persons and goods, energy, financial exchanges etc.); fight against illegal content and criminal activities on the web and ICT networks in general.

This key role of cyberspace, coupled with the existence of global threats through cyber crime and cyber terrorism create the need for a global approach, and this need reaches out beyond direct economic impact to national and homeland security domains. As stated in the latest "Virtual Criminology Report" [73], "*while there may be debate over the definition of cyber war, there is little disagreement that there are increasing numbers of cyber attacks that more closely resemble political conflict than crime*."
To implement a fully consistent cyber security strategy, policies have to operate in a holistic approach where the scope, targets, means and delimitations of what cyber security is addressing, are well understood.

The objective of EOS in putting forward this document is to contribute to implementing coherence and consistency in the on-going and upcoming policies and activities emerging in cyber security, with the intent of supporting European initiatives in the refinement of concerted strategies and concrete actions in cyber security.
Starting from the on-going policies and bodies as well as an analysis of the impact of cyber threats, the document concludes with a set of recommendations and practical contributions proposed by EOS as a body representative of main European organisations active in security and wishing to contribute to an **EU Cyber Security Programme** as well as to the emergence of a **European Cyber Security Coordinator**.

[1] http://www.eos-eu.com/Publications/WHITEPAPERS/tabid/225/Default.aspx

3. Scoping the problem

3.1. Defining cyber security

The simplest definition of cyber security is the "security of the cyberspace", which immediately brings forward the complexity of the problem:

- cyberspace is a **domain that lacks single and delimited frontiers**;
- the **interconnections with other infrastructures**, above all communication infrastructure, **are numerous**;
- the **points of access can be infinite**;
- the initial **impact of threats can be local** but the **spreading of threats can be virtually unlimited**;
- **users include**, potentially, **all individuals**, organisations and "intelligent" machines.

A first important element is that no link to technology emerges from this definition of the cyber environment. While ***cyberspace has been enabled through the use of Information and Communication Technologies, securing it does not rely entirely on technology***. Cyber security cannot be defined as "information security", "information assurance" or "computer security". While these three terms are interrelated and share common goals of protecting the confidentiality, integrity and availability of information, there are subtle differences between them and most importantly, none of them addresses completely cyber security. **Information security**, for example, is concerned with the confidentiality, integrity and availability of data; **information assurance** is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes; **computer security** (sometimes referred as "IT system security") focuses on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

> ***Cyber security targets the entire cyberspace making it, by definition, much broader than the physical space and therefore requiring a comprehensive approach, including governance, organisational, legal, tactical and educational strategies supported by technology, but not embodied by technology.***

A second important factor contributing to the scope of cyber security, is its usage, which includes:

- a **public Internet, public mobile and fixed telecommunications networks** and **other shared infrastructures** such as localization services on which citizens, private and public organisations increasingly rely (while at the same time the issue of how to use them securely is often neither fully understood nor well managed);
- the approach by the private sector to outsource operational infrastructures to decrease fixed costs appearing on their balance sheets using "Cloud Computing"[1] for their data and operations, without fully understanding the associated risks in terms of potential theft, resilience and loss of data or operational capacity;

[1] Cloud Computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand

- the **approach by public authorities to build a full range of "cyber services"** for citizens ranging from optional ones such as the request for administrative documents, to services that are increasingly becoming available only via Internet thereby **creating "cyber benefits"** (fast access to information, documents etc.);
- the expansion of online education and training;
- the voluntary addition of private user data to cyberspace, through social networks, job-related networks, governmental networks inducing personal privacy issues;
- the **sharing of a single Internet infrastructure by all users** ranging from home users to industrial corporations, critical infrastructures and public administrations;
- the **future extension of the "always online" paradigm** to more and more objects and systems (**Internet of things**, Intelligent mobility, etc.).

> ***It is not the existence but the usage of cyberspace that creates the need for cyber security. With usage moving from optional to compulsory, cyber threats are emerging in tandem with cyber benefits*** *[57].*

A third contributing factor is the **dynamic nature of cyber security** driven by the constant evolution of its components and its potential contributors, with over 1.8 billion people connected worldwide in 2009 and an unprecedented growth rate of 400% over the last decade. [58]

This dynamic nature is highlighted in one of the classic books on Cyberwar [63], in which authors define cyber security as a "comprehensive approach to conflict based on the centrality of information" and highlight the need to ***rethink the dynamics of future conflicts in the information age***. These dynamics are made complex by the fact "With low barriers to entry, coupled with the anonymous nature of activities in cyberspace, the list of potential adversaries is broad"[13].

Defining cyber security therefore requires

- continuous watch over the evolution of the services and their content provided by and in cyberspace, and
- ***understanding of-*** and ***response to-*** related needs ensuring that the services and their usage are protected

> ***In our approach, we will use the term "cyber security" as the need to prevent from, prepare for, detect, respond to and recover from any hazard or illicit content in the cyberspace, covering networked infrastructures, including Internet.***

3.2. Cyber crime and cyber terrorism: categorization of cyber threats

To further refine the role and actions required for a concerted EU Cyber Security Approach, we have to better understand the threats to the cyberspace that we collectively address under the terms of "cyber crime" and/or "cyber terrorism".

What are the **motivations that drive the perpetrators of cyber attacks and cyber crime?**

Expanding on the initial segmentation into four categories of cyber crime given in the Cybercrime Convention document, Art 2-10[1], motivations can be classified into

- ***recreational*** - where the challenge is to **demonstrate the ability to hack into protected servers**, whatever their nature. The focus is more on the **technological demonstration** than on the target itself;
- *activist* – where the target is to use cyber attacks as a tool to advance a specific social or economic issue (anti-nuclear, anti-war etc);
- *illegal* – illegal sharing of information and data on internet, also with infringement of IPR (piracy) or use of internet with illegal content (e.g. sexual exploitation and child pornography etc.);
- ***criminal*** – where the motivation is driven by the **financial or personal gains**, either direct (stolen IDs, stolen data etc) or indirect (ransom requests etc);
- *business or state-sponsored, including terrorism* – where motivations range from obtaining sensitive data to disrupting public and private operations, including those of critical infrastructures.

These motivations are further complemented by the impact on information, with action modes falling in three categories:

- **actions *for* information**: intrusion in systems to collect data (includes confidentiality);
- **actions *against* information**: data modification to cause system malfunction, data destruction (includes availability);
- **actions *through* information**: broadcast of false information, propaganda, identity theft (includes integrity).

Whatever their motivations, the ***major disruptive methods*** **in the cyberspace** identified so far include:

- phishing
- botnets
- mass distribution of malware
- fake points of access
- spam.

[1] (1) offences against the confidentiality, integrity and availability of computer data and systems;
(2) computer-related offences;
(3) content-related offences;
(4) offences related to infringements of copyright and related rights.

Phishing	Phishing is a criminal mechanism employing both *social* engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords. Technical-subterfuge schemes plant crimeware (malware) onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords - and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes). These methods can have different impacts, and the following table highlights a few examples of impact according to the domains in which they are used. Phishing can be implemented through spam, botnets and malware. Source – the Anti-Phishing Working Group [52]
Botnet	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 for instance, to 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. These are now available as a service at a cost per day for a denial of service attack on a specified target. Source – EOS White Paper [62]
Fake Points of Access	While phishing can be considered as creating fake software access points, fake physical access points are used to capture real identities or data to make further criminal use usually within cyberspace. The methods related to this class which can be quickly and cheaply implemented include, among other examples, card-skimming devices and rogue access points. Set up and placement time is less than 30 minutes. Cost of each is around $50,00.
Malware	Malware represents software designed to infiltrate a computer system without the owner's informed consent. Following this infiltration, the computer can become part of a botnet, can participate to phishing attacks etc. It is important to note that innovations in cyber crime methods emerge daily: *"Just in 2009, more new malware appeared than in the entire history of computer viruses" [53].*
Spam	Spam emails are unwanted emails distributed in a large quantity (in 2009, 107 billion spams have been distributed every day globally on average, 85% were from botnets[68]). The typical examples are spam emails with content related to pornography, pharmaceuticals, dubious financial transactions etc. In most cases, spam emails are distributed with fraudulent intentions. Spam, apart from being irritating, can often expose users to inappropriate content, including pornography and unwanted marketing and can also be used to spread malware. Source – Safer Internet, http://www.saferinternet.org/c/journal/view_article_content?groupId=10131&articleId=36231&version=1.0

Table 1 - Disruptive methods in the cyberspace

3.3. Impact of cyber threats

In direct relation with the absence of a single definition of cyber security, quantified impacts are also difficult to establish. Different reasons impede the elaboration of fully accurate numbers, including

- the reluctance of many organisations to report information security breaches
- the combination of direct and indirect impacts of cyber attacks
- the lack of an agreed upon methodology to quantify the impacts

Furthermore, it is important to note that the impact of cyber attacks is by **nature asymmetric**: **a significant damage can be done on a large infrastructure with relatively modest means**.

This section elaborates a documented order of magnitude, based on a combination of sources and starting organisations' reluctance to reporting cyber attacks.

This reluctance is mainly due to one or more of the following reasons:

- ***Financial market impacts***. The stock and credit markets and bond rating firms may react negatively to security breach announcements.
- ***Reputation or confidence effects***. Negative publicity may damage a reporting firm's reputation or brand, or cause customers to lose confidence. These effects may give commercial rivals a competitive advantage.
- ***Litigation concerns***. If an organization reports a security breach, investors, customers, or other stakeholders may use the courts to seek recovery of damages.
- ***Liability concerns***. Officials of a firm or organization may face sanctions.
- ***Signal to attackers***. A public announcement may alert hackers that an organization's cyber defences are weak, and foster further attacks.
- ***Job security***. IT personnel may fear for their jobs after an incident and seek to conceal the breach from senior management.

While as mentioned earlier there are **no standard methods for measuring the costs of cyber attacks**, these **can be split between direct and indirect costs**.

Direct costs include:

- **loss of value in information assets** that are stolen, compromised, or otherwise degraded during an attack;
- the **expenses incurred in restoring a computer system** to its original, pre-attack state;
- additional **spending on labour and materials**;
- **costs for business interruption**: lost revenue and loss of worker productivity during the disruption;
- **productivity loss** (measure not always straightforward or uniform).

Indirect costs (which may continue to accrue after the immediate damage has been repaired) could be more significant than direct costs but often more complex to evaluate:

- **loss of reputation**, or damage to a firm's brand;
- **customers defecting** to competitors;
- financial markets raising firm's **cost of capital**;
- rising of **insurance costs**;
- possible **lawsuits**;
- **economic harm to individuals and institutions** other than the immediate target of an attack;
- possibility of **cascade effects** – disruption spreading from initial target computers to interlinked networks

- loss of intellectual property.

Quantified impact related information available from various sources include:

- the most recent estimate by Europol, Eurojust and Frontex of global corporate losses linked to cyber crime stands at approximately **€750 billion per year** [72]
- more than 150,000 viruses and other types of malicious code are in circulation, and 148,000 computers are compromised per day [72]
- cyber crime cost to the US was estimated at over **$400 billion** back in 2004 [74] and extrapolated to over **$1000 billion** in 2009 (the extrapolation procedure of the initial figures to find the final results could be questioned)
- other aspects of cyber crime with 2009 values estimated at **€ 10 billion for web-piracy** (video, music, games [75]), **€51 billion for software piracy** [76]

In addition, **cyber threats have in effect become a business of their own:**

- the shadow Internet economy was already worth **over $105 billion** in 2007 [67]
- botnets are available for "rental by the hour", with costs as low as a few Euros per hour [61] while stolen identities are sold online for a few dollars or Euros
- malware authors can produce new, unique malware every 45 seconds in order to keep it undetected".

Cyber security has become central due to the fact that threats initiated in cyberspace have considerable impact on the real-world, and all activity sectors from health and education to logistics and utilities can suffer from these attacks. Cyber crime could have a direct impact larger than €300 billion/ year with an even larger indirect impact whose evaluation is much more subjective.

The table in annex II provides examples of how the real and cyber worlds are linked, with some numerical information further helping to scope the size of the problem.

4. Specific challenges in protecting the cyberspace

4.1. Specificities of cyber threats

Threats in the cyberspace have specificities that bring totally new dimensions in security.
These specificities include:

- the virtually limitless size of the domain in which they can propagate;
- the ***exponential speed at which they can propagate***, building on their capacity to self propagate and multiply through the use for instance of the local addresses of an infected computer;
- the ***existence of "dormant" threats that can be activated on demand and at a distance***: this is the case for instance for botnets, which organisations use to create huge networks of computers that can then be used "on demand". Malware can also contain delayed or remote activations, making them hard to detect before they actually strike;
- the emergence of a ***cyber threats business***, through which cyber threats capacities are available for hire at very small prices;
- the *anonymity* that makes it virtually impossible, in the current configuration, to find the original perpetrator(s) of a disruption;
- the ***flexibility offered to organisations* in the capability of *spreading and rapidly changing their modes of operation***, and as concluded by the US Joint Forces Command[13], hierarchical organisations are probably not the best way to deal with these fast mutating network form of organisations: agility and flexibility became ever since the holy grail of cyber security field operations;
- the *lack of integrated legislations*, ranging from domestic to international laws. This is linked to the complexity of this borderless domain as well as to the *lack of an agreed definition of the cyber security needs and the difficulty to identify the identities of perpetrators as well as their location*. Even when the identities are uncovered, the separation between location of the origin of the threat and where the threat actually takes place introduces an additional complexity of operating across two different legal systems.

In addition to the specificities of cyber threats, the problem is made more complex due to:

- cyber technologies having direct impact on privacy & data protection;
- advanced cyber technology providing sophisticated and easily available tools that can be used for cyber attacks;
- the interconnectivity of our networks and infrastructure which have made the cyberspace a far reaching environment, not limited by national borders or other physical limitation
- the evolution from isolated to coordinated attacks

A final specificity is that the cyber and real worlds are not disconnected, and one major risk is linked to the vulnerability of industrial control systems [55], particularly the SCADA (Supervisory Control And Data Acquisition) systems that are used to control dispersed physical assets or devices from a central location. Historically, SCADA systems antedate the development of the internet; they were originally hard-wired systems primarily intended to control processes at a single site and not designed to be connected to the outside world. However, with the advent of cheap PCs, improved telecommunications and the internet, these individual sites have become linked to one another and, in many cases, to the outside world via the internet creating a bridge between the cyber and real world that has already been exploited to create real-world disruptions of major infrastructures ranging from transport to power and administrations.

4.2. An ambivalent context for Cyber Security

Cyber security approaches face an ambivalent context in which:

- on the one hand **public authorities are pushing to decrease the digital divide**, with different initiatives at European level supporting the increased connectivity of all citizens with current rates of over 50% connected users in Europe and over 70% in North America [58]; on the other hand **these same initiatives are creating and expanding the networks through which cyber attacks can spread** at unprecedented speeds, and with unprecedented outreaches;
- Member States aim to protect citizens' privacy and personal data, but at the same time they could need this data to prevent and / or prosecute criminal and illegal activities;
- each citizen user of the network could become an unaware new potential attack vector and/or victim;
- all economic sectors are increasingly using cyber solutions and services and our society has become totally dependent on them, yet the business models of our society still give a relatively low weight in reinforcing protection of these "vital" cyber solutions.

Indeed, infrastructures are increasingly interconnected and interdependent (via ICT technologies) and cyber solutions become too large and complex for one authority to handle alone: networks can thus propagate the negative effects of weak preparedness from one provider to the others. Incentives for investments in cyber security (equipment but also insurance) are hampered by uncoordinated approaches to control security interdependencies.

> ***Cyber Security is strategic for Europe and its Member States: the current usage of essentially non-European technologies for cyber security implementations create a dependency of Europe that could be critical when addressing the strategic impact of cyber threats and disruptions: European stakeholders need to master key tools to fight cyber threats.***

4.3. Challenges for the creation of an EU Cyber Security Approach

To face these threats and challenges we should **work in an international perspective taking into account European specificities**. For this reason, in the development of an **EU Cyber Security Approach** several specific challenges should be tackled, which we have classified in the following categories:

1. **Policy Definition and Coordination**
2. **European and International Cooperation**
3. **Threat Assessment and Vulnerability Reduction**
4. **Legal and Societal Issues / Privacy**
5. **R&D, Certification, Implementation**
6. **Awareness, Education and Training Activities**
7. **Monitoring & Response Capabilities**

Policy Definition and Coordination

- ***lack of a global EU cyber security policy:*** there are several sector specific policies on ICT security, but a global EU cyber security policy providing clear guidelines is missing;

- ***lack of coordination across the national cyber security approaches*** developed by Member States such as the UK Cyber Strategy, the French "Livre Blanc" etc

European and International Cooperation

- ***lack of sufficient response and cooperation on cyber security*** issues from the ***EU private sector*** due to sensitiveness, competition, lack of incentives and clear guidelines;
- ***insufficient level of understanding*** of the cyber environment, issues and threats;
- ***insufficient level of confidence / trust*** impeding effective data and information sharing for prevention and crisis management of cyber threats.

Threat Assessment and Vulnerability Reduction

- ***national security often supersedes international collaboration***, impeding the identification and assessment by each Member State of existing cyberspace weaknesses to the other Member States (MS sovereignty for own data, information and intelligence management to protect strategic decisions or influence international activities);
- ***lack of common EU assessment methodology of cyber risks***.

Legal and Societal Issues / Privacy

- ***lack of an EU legal framework*** for effective transnational cooperation on cyber crime;
- lack of a uniform approach across Member States towards privacy and its link with cyber security (e.g. IP addresses being considered in some cases as personal data);
- high ***sensitiveness of citizens perceiving limitations in the use of Internet*** as limitations of their freedom to share and access information; nevertheless a cooperation between Member States is needed to monitor criminal / inappropriate use of the Internet (including sexual exploitation and child-pornography etc) reinforcing existing activities (the EC has started a specific activity, the Safer Internet Programme[1], aiming at empowering and protecting children and young people online by awareness raising initiatives and by fighting illegal and harmful online content and conduct).

R&D, Certification, Implementation

- **lack of R&D contributing to a global EU cyber security policy (still to be developed),** based on common architecture frameworks, to develop consistent cyber tools and procedures;
- ***lack of a secure EU Information Sharing Model*** (also for other EU security sectors: e.g. border, CIP etc) as requested by the EU Security strategies;
- lack of coordinated capability development, capacity building and implementation approaches both at prevention and at response levels.
- lack of EU certified cyber security systems, procedures and services;
- lack of financial incentives for implementation of cyber security measures and services.

Awareness, Education and Training Activities

- ***lack of awareness and education on cyber security issues / threats***: all individuals and organisations should be trained, collectively, to a required minimum level of understanding of threats, impacts, ways of operation in terms of prevention and of action. There should be a continuous update of the different

[1] http://ec.europa.eu/information_society/activities/sip/index_en.htm

components and technologies of cyberspace, understanding the contributions by humans and machines, mobile and fixed devices and infrastructures;

- ***lack of training of economic operators**:* businesses which are currently in the process of increasing the outsourcing of their data and processes, effectively **making use of the latest technologies** such as software as a service and cloud computing should put in place the corresponding security education and processes.

Monitoring & Response Capabilities

- ***lack of coordinated (across Member States) continuous monitoring and update of cyber threats***, identifying the "who, what, where" and adapting the speed of monitoring to the spreading of threats as a defence and not as a re-active approach*;*
- ***lack of common / coordinated response capability to cyber threats**:* not all Member States can implement adequate capabilities and capacities to face evolving cyber threats (EU solidarity principle).

However, there are existing **examples of strategic domains where collaboration in exchanging data and information is moving forward in Europe**, and one of these is **maritime surveillance**, where coordination involves European agencies, European Commission DGs, and above all Member States.

To date, a roadmap for maritime surveillance has been elaborated (EUROSUR), two pilot projects involving the Member States have been launched, each of them involving 6 to 10 Member States and more than 20 different public administrations – leading to a first definition of both the data to be shared and the architecture used to federate different systems. One important element is that ***the sharing of data is elaborated based on a classification***, ranging from data available to all to data available bilaterally or multi-laterally on a "need to share" basis – thereby creating pre-defined processes and creating the confidence needed for this level of common information sharing environment to become effective.

While **maritime surveillance is obviously very different from cyber security, similarities exist in terms of** complexity due to the large number of intervening parties, the existence of legacy systems that have to be federated into a large, operational environment and the intent to create a Common Information Sharing Environment (CISE, as requested by the Council and under development under the coordination of DG MARE).

> ***As is the case in maritime surveillance, no single domain can fully address cyber security without the organised cooperation from a number of contributing activities providing clear EU added value.***

5. European approaches to Cyber Security

5.1. Overview of European activities

The first European initiative to face cyber threats is the ***Convention on CyberCrime*** [7]. This Treaty, issued in 2001 by the European Council in association with the European Committee on Crime Problems (CDPC), details a number of definitions and actions for each ratifying country, and provides the first basis for international cooperation. It is currently ratified by 30 countries (also non EU), but has only been put into force in a number of Member States (yet, this text should be updated to consider the most recent evolutions of cyber threats).

At the European Union level, different programmes and communications have emerged. In the 2007 EC communication "***Towards a general policy on the fight against cyber crime***"[5] proposed an important step forward in the recommendations that envisage, among other elements:

- the setting up of a central EU cyber crime contact point;
- the support of research in fight against cyber crime;
- concrete public-private projects;
- the raising of **awareness**;
- encouraging all Member States and relevant third countries to **ratify the Council of Europe's Cyber Crime Convention** and its additional protocol and consider the possibility for the Community to become a party to the Convention;
- examining, together with the Member States, the phenomenon of co-ordinated and large scale attacks against the information infrastructure of Member States in view of preventing and combating these, including **co-ordinating responses, and sharing information and best practices**.

In 2009, several key EU documents have provided guidelines for activities linked to security of the cyberspace:

- *the* ***Stockholm Programme*** [2][3] providing an integrated approach to "Delivering an area of freedom, security and justice for Europe's citizens" for the next 5 years;
- the ***Internal Security Strategy***[4], and the implementation of the COSI committee foreseen in the Lisbon treaty as a coordinator between the different agencies;
- the EC communication "***Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience***" [16] on CIIP;
- the EC communication on the ***Digital Agenda***[1] and its impact on the research programmes;
- the ***European Programme for Critical Infrastructure Protection*** – EPCIP and its 2008 directive [14], focused on Energy and Transport and its envisaged upcoming review and possible evolution for inclusion of IT networks; the action plan linked to the previous directive and communication;
- the ***data protection and privacy Directives*** (e.g. Directive 95/46/EC of the European parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data);
- ***operations of Agencies*** such Europol, Frontex, Cepol, Eurojust, ENISA;
- the effective ***interworking of CERTs*** (Computer Emergency Response Team) ***and CSIRTs*** (Computer Security and Incident Response Team), at prevention and at response levels;

- the FP7 supporting ***security, trust and critical infrastructure research*** (DG ENTR, DG INFSO, DG HOME);
- the ***CIP-PSP pilot deployments*** of identity related initiatives;
- etc.

Security policies elaborated in various EC services ("cyber" aspects of security of transportation in DG MOVE, security of satellite infrastructures in DG ENTR, etc.), as well as **specific policies deployed to serve the EU proper needs** (security of the Schengen networks, protection of communications between EEAS and delegations in third countries, etc. – DG RELEX) **add to the complexity of the picture**.

> ***How can all these activities be consolidated into a single, coherent EU Cyber Security Approach?***

As stated in the Internal Security Strategy, "Europe must consolidate a security model". We will address this element further in the final "recommendations" section.

To date, **different initiatives are already taking place in the EU to build an EU Cyber Security Approach**, these include:

- the **Public Private Dialogue** (PPD) dedicated to security and resilience of information and communication networks and critical infrastructures proposed in the EC March 2009 communication[15] which is now being developed by EC DG INFSO in a public private dialogue under the name **EP3R** (European Public Private Partnership on Resilience). The present approach of this PPD is quite interesting but **should be further enhanced,** as it currently targets CIIP (Critical Information Infrastructure Protection) and not to all cyber security issues (perhaps to avoid moving beyond the area of competence of DG INFSO: a further example of the fragmented approach due to the lack of a common EU cyber security policy). Its initial activity focuses on fixed and mobile telecommunications as well as the Internet, not considering cascading impacts on other sectors of cyber threats. It envisages establishing links between national authorities and private operators[17], yet European security solution and service suppliers are not presently envisaged at steering level, thus missing key stakeholders at this important decision level. At present, it has attracted representatives from the main US private sector companies but the participation of private EU stakeholders is still weak, while at the same time and as highlighted previously in this document it is of strategic importance to Europe to decrease its reliance for security solutions on non-European players. Furthermore, this initiative does not address the issues of financial support and incentives for implementation of cyber security policies, positioning the activity at the level of "dialogue" rather than implementation.
- the **envisaged Operator Security Plans** to be elaborated by Member States if and when (possibly 2012) the EPCIP directive will be adopted also for **ICT networks** [14]. It is important to note that development of these operators security plans will require a common EU risk assessment methodology and clear EU guidelines;
- the **creation of CERTs in each Member State** and **their envisaged networking across Europe and cooperation with law enforcement agencies** (as suggested also in the Digital Agenda Communication[1]), in cooperation with the private sector, yet with possible restrictions in the cooperation imposed by Member States for sovereignty issues;
- the envisaged reorganisation of ENISA possibly to enlarge and reinforce its role and its cooperation with the private sector: also in this case with possible restrictions in its activity according to Member States sovereignty issues;

- the **EC research on cyber security tools**, as supported by DG INFSO ("Trust"), DG ENTR (focussing on cyber security technologies for critical networks) and DG HOME (studies on cyber security issues): these research activities are each under the frame of their own programme, and require further **overall coordination operate efficiently under a common EU cyber security policy** (still to be developed).

> ***These initiatives lack several important dimensions: the integration of legal and processes aspects[1] with an EU cyber security policy, enhanced technological education, public and private commitment to develop an EU Cyber Security Approach and the financial support for its implementation (particularly in the case of operational Public Private Partnerships)***.

Present collaborations at EU level are being set up either in the process domain (operator plans) or in the technological domain. However, the existing lack of global guidelines and insufficient public and private commitment and support impede their evolution towards the required level of integration.

> ***Cyber security is still tackled in a segregate and reactive approach (reacting on incidents) rather than a collective and proactive (building up capability and capacity to prepare, prevent, react and recover) approach.***

Other important elements to assess the **status of cyber security are the approaches at international level. In Annex I** we describe a few initiatives on-going beyond the 27 Member States and that are of particular relevance to a coordinated European cyber security policy.

[1] Sometimes missing maturity also at national level

6. EOS recommendations

The previous sections highlighted the following important elements:

- cyber threats are in constant and fast evolution,
- cyber security approaches and solutions are sensitive to administrations, economic actors and citizens,
- there is a global awareness that cyber security is essential to protect national and international interests,
- both the civil and military authorities are involved in programmes and strategies to combat cyber crime,
- cyber security cannot be addressed in isolation, but requires extensive cooperation, for which we need to solve "sensitiveness" issues,
- there is an increasing international wish to collaborate,
- at EU level, the Stockholm programme and the EU Internal Security Strategy provide the ground for the creation of a framework for a coherent cyber security strategy and concrete activities.

In section 4.3 we listed the challenges to be overcome in order to create an EU Cyber Security Approach. The next steps are therefore how to foster integration and implementation of this EU Cyber Security Approach, ensuring that consolidation takes place and that international collaboration is set up under the auspices of this consolidation.

To foster the development of an EU Cyber Security Approach, EOS focuses its recommendations on two major elements:

- **an EU Cyber Security Programme and**
- **a European Cyber Security Coordinator, in a similar approach to that taken by nominating a European Counter-Terrorism Coordinator**

6.1. The EU Cyber Security Programme

EOS supports the setting up of an **EU Cyber Security Programme which would take place in two steps**:

A. **The creation of a Public Private Dialogue (PPD)** for **global outreach and trust,** allowing the **identification of public policy priorities, societal issues, economic and market dimensions of challenges and means** (including appropriate positive and negative incentives for stakeholders) as well as to identify responsibilities.

B. ***The creation of a Public Private Cooperation*** (or Partnership when suitable) to **elaborate and implement a common EU Cyber Security Approach** tackling the challenges described in § 4.3.

The **Cyber Security Programme should involve all stakeholders**, including representatives from National Administrations, the European Commission (DG Home Affairs, DG Justice, DG INFSO and DG ENTR), European Agencies (ENISA, EUROPOL, etc), European Industry (Operators of Critical Infrastructures such as Energy,

Telecoms, Finance; Security Solutions and Services Providers), CERTS[1], Law enforcement Agencies, Regulators and Intelligence agencies.

Concrete Actions for the EU Cyber Security Programme

A) Actions to be developed in a Public Private Dialogue

1. *Policy Definition and Coordination*

- **develop a global EU cyber security policy**, building upon existing or new sectoral policies, coordinating actions for their implementation;
- **propose updates to the Council of Europe's Cyber Crime Convention.**

2. *European and International Cooperation*

- **build up an improved and coordinated governance** for cooperation across EU Institutions, with Member States administrations and the private sector;
- **set up a European Public Private Dialogue to build trust and increase cooperation**, providing an organised process for different communities to work together to enhance protection of the cyberspace and promote a global "culture of cyber security". It would gather technology, policy, legal and social-economic actors (European institutions and Member States with the Private sector suppliers, providers and users / operators). This will also allow continuous availability of a cyber security aware community enabling the EU Cyber Security Coordinator to have an organised reference point taking into account all stakeholders;
- **build a common and comprehensive understanding by all parties of this community of cyber security issues (across Member States) and interdependencies of infrastructures** leveraging on the use of the cyberspace , developing comprehensive awareness to empower all businesses, the general workforce, and the general population, to secure their own parts of cyberspace;
- **share best practices in the cyberspace** at different levels: operational, judicial, financial, technological and educational;
- **encourage Member States to increase their level of collaboration**, e.g. through a network of national CERTs having similar levels of capability for detection and response to threats, and the possible creation of an EU CERT, considering the subsidiarity principle of the Lisbon treaty and the major elements on privacy.

3. *Threat Assessment and Vulnerability Reduction*

- **develop an EU risk management methodology for cyber threats**: risk assessment and elaboration of cyber security incident response plans (not only for telecom operators);
- **establish organised procedures for the identification and measure of the impacts of cyber security threats** and incidents across all domains, from energy to transport, from logistics to administrations etc.;
- **support the identification of critical infrastructures** depending on security of the cyberspace as initiated by the EPCIP directive [14], but ensuring that this definition is elaborated by the integrated community.

4. *Legal and Societal Issues / Privacy*

- **analyse the existing legal frameworks** applicable to cyber security;
- **propose evolutions for the establishment of an EU cyber security legislation / regulatory framework** to handle the specific dimensions of cyber

[1] CERT = Computer Emergency Response Team

crime across MS countries (threat identification and persecution) including a liability model to protect those operators that invest in security measures;

- **develop an EU Charter on Privacy versus cyber solutions** based upon precise and clear requirements defined by regulators to allow industry to develop compliant products, with established certification mechanisms and organisations.

B) Actions to be developed and implemented in Public Private Cooperation / Partnership

5. R&D, Certification, Implementation

- **develop common architecture frameworks**, **secure open standards, procedures and secure / trusted tools for sharing data** (EU Model for Data and Information Sharing) **and intelligence** (when requested by law enforcement agencies);
- **coordinate research and development of solutions and processes** in a **"security & privacy by design approach"** (architecture, procedures and cyber security privacy enhancing "tools" supporting EU policies): security must be integrated at the beginning of information technologies' infrastructure development life cycles[71], and should be upgraded and managed across the lifecycle of the product;
- **elaborate pilot deployments and demonstrations validating defined cyber security environments** for the different research and developments activities taking place across FP7/ FP8, CIP-PSP and other programmes;
- **define a cyber security EU certification programme** identifying the level of preparedness and resilience of infrastructures to cyber threats, including cyber incident contingency and response plans;
- **create financial incentives to implement** cyber security solutions and services. Products or services must integrate, from the start, simple and flexible security measures and mechanisms. Products should be well-documented and comprehensible and security mechanisms should be readily understood and configured easily by untrained users[71];
- **contribute to building competencies**, implement capabilities and capacities across Europe at all levels implementing services and systems for **an increasingly secured cyberspace linked to the main EU security applications**:
    - **Border Surveillance** (e.g. Common Information Sharing Environment for maritime Border Surveillance);
    - **Border Management / checks:**
        - e.g. major EU databases and ID systems: **SIS and VIS**;
        - cyber security-based ID management system at EU level to enable secured collaboration between MS and fostering cyber economy and services across the EU: a common EU framework for identity and authentication management ensuring compliance with legal frameworks on personal data protection and privacy and allowing for the full spectrum of activities from public administration or banking with strong authentication when required;
        - **a cybersecure EU ID**, complementary to national IDs, voluntary for EU national migrants across the EU and mandatory for non EU immigrants, facilitating the full spectrum of activities across the EU;
    - **Civil Protection** (e.g. **EU interoperable and secure emergency communication capability** to be deployed in case of crisis overruling local capacity linked with disaster management policy);

- **Secure and legal use of Internet** (monitoring and protection from illegal content or crime of cyber services for content, trade and exchange of financial flows);
- Transport of People (secure exchange of passengers information – e.g. PNR – and traffic information for security and safety of air, maritime, land transportation);
- Transport of Goods (secure exchange of goods information, e.g. for security of supply chain against theft and terrorism);
- **Energy** (**secure SCADA** for control of energy production, transmission and distribution).

6. *Awareness, Education and Training Activities*

- promote the organisation of national and European **exercises** on simulated large-scale network security incidents (cyber threat response training programmes);
- develop **"infrastructure simulators"** to simulate on a large scale sophisticated attacks, failure modes for common vulnerabilities (across countries, sectors or infrastructures) and reaction means, training national government agencies and CNI IT security administrators for a coherent approach to cyber threats. These simulators could also be used to test / validate the "security and privacy by design" solutions to counteract these attacks while considering citizens rights and data protection (when needed);
- establish **recognized professional cyber security certifications** (cyber security operators) which could then spread cyber education to other (non professional) users;
- **contribution to citizens' awareness and education**, supporting better usage but also building trust without which economic growth of ICT services will be continuously impeded, putting Europe at a clear competitive disadvantage in the world wide context.

7. *Monitoring & Response Capabilities*

- **EU Rapid Cyber Security Capabilities for Monitoring (dynamic watch of cyber threats and their evolution) and Response to Cyber Attacks:**
  - elaboration of a complete set of **cyber security services as a centralised or networked "watch-and-warning" system to detect and prevent cyber attacks** as they emerge;
  - **Rapid Cyber Security Capabilities coordinated by CERTs with the support of ENISA** (or via an EU CERT managed by ENISA): **interoperable & interconnectable systems to create "on demand" a virtual network to monitor attacks where exceeding local / national capacities & capabilities (EU solidarity)**: finding origin of attacks, persecuting and supporting restoration of cyber services in the hit country infrastructure (need for access center, clearance, interoperability, common definition of failure modes etc.).

- **EU Cyber Security Capabilities for Prevention and Prosecution of Cyber Crime:**
  - **Cyber Security Capabilities in an agreed architecture framework, coordinated by EUROPOL**, for **monitoring information and intelligence**, allowing interoperable data exchange between law enforcement authorities to fight cyber crime

- **Creation of national "Cyber Polices" linked to EUROPOL** with adequate capabilities to secure the cyberspace and prevent cyber crime[70].

6.2. The European Cyber Security Coordinator

In an approach similar to the European integrated approach to counter terrorism, we recommend the creation of the role of the European Cyber Security Coordinator.

The different **tasks of the European Cyber Security Coordinator** would include:

- supervising the Cyber Security Programme;
- informing Member States of the evolution of cyber threats, their economic and security impacts;
- collaborating with European Institutions to elaborate an integrated set of measures that effectively establish the cyber security regulatory framework;
- collaborating with European Institutions and Agencies to ensure that the cyber security regulatory framework and the different funding R&D programmes are aligned in terms of objectives of the EU cyber security policies;
- monitoring and soliciting Member States to increase the awareness of the required collaboration and national measures, including the evolution of operator security plans;
- **defining**, in collaboration with the relevant agencies, **cyber security exercises** (e.g. similar to the approach used by Frontex to coordinate cross-border tests and validation of measures);
- **representing the single cyber security contact point of EU Institutions at an international level**, fostering multi-lateral collaboration with other cyber security programmes, such as the one operated in the United States;
- **defining**, in collaboration with the relevant actors (users, operators, suppliers) **cyber security capacity building needs**;
- representing within Europe the civil cyber security initiative, linking civil with military cyber security operations and increasing the collaboration between civil and military handling of cyber threats.

7. Conclusion

Cyber crime is spreading at unprecedented speeds and reaches out far beyond the frontiers of a single country. At the same time, cyber and physical worlds are closely interlinked, with all activity sectors constituting potential targets for attacks.

The existing set of European and non-European policies, strategies and on-going activities create a good starting point.

However, the current programs do not address the fragmentation of efforts: it is urgent to move forward to implement an EU Cyber Security Approach, while at the same time clarifying how all these activities can be coordinated at European and at a world-wide level.

EOS representing the major EU stakeholders active in security intends to be part of this approach and participate actively to the implementation of the proposed concrete actions:

- enhancement of the Public-Private Dialogue, prerequisite to effective coordination;

- support the **development** of a **comprehensive EU cyber security policy** providing a clear view and guidelines for the implementation of security measures to protect the cyberspace and the EU economy;
- supporting the definition of an EU methodology for cyber threat assessment and definition of incident response plans;
- contribution to the creation of an EU Cyber Security Programme;
- development and validation of innovative technological cyber security solutions and services;
- **participation to pilot activities** of the different operators, in application domains ranging from transport to energy as well as more generally at the telecom infrastructure level;
- refining and promoting a "secure & privacy-by-design" education and approach;
- **building competencies, capabilities and capacities across Europe at all levels** (including the EU model for information sharing), **for EU security applications** (Border Control, Civil Protection, Protection of Critical Infrastructures) but also **for the creation of EU Cyber Security Capabilities for monitoring and response to cyber attacks and for the prevention and prosecution of cyber crime.**

8. References

8.1. Policies and strategies

[1] 19/05/2010 – A Digital Agenda for Europe – Communication from the European Commission – COM(2010) – 245

[2] 04/05/2010 - The Stockholm Programme – an open and secure Europe serving and protecting citizens - (2010/C 115/01) – European Council - published in the Official Journal of the European Union http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:01:EN:HTML

[3] 20/04/2010 – Delivering an area of freedom, security and justice for Europe's citizens - Action Plan Implementing the Stockholm Programme – Communication from the European Commission – COM(2010) - 171

[4] 23/02/2010 - Internal Security Strategy – Council of the European Union

[5] 22/05/2007 – Towards a general policy on the fight against cyber crime – Communication from the European Commission COM(2007) 267

[6] Towards a general policy on the Fight against Cyber crime – Summary of the impact assessment – Accompanying document to COM (2007) 267 – SEC (2007) 641

[7] 23/11/2001 - "Convention on Cyber Crime" - European Treaty Series - No. 185 – European Council http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&DF=03/06/2010&CL=ENG (and List of countries and status of the entry into force of the convention on cyber crime http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=03/06/2010&CL=ENG, updated 06/2010)

[8] 29/05/2009 – Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure (United States) - http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[9] 2007 – Global Cyber Security Agenda - International Telecommunications Union - http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf

[10] 2007 – Global Cyber Security Agenda – ITU – Global strategic Report http://www.itu.int/osg/csd/cybersecurity/gca/docs/global_strategic_report.pdf

[11] 04/2010 – Global Cyber Deterrence – Views from China, the U.S., Russia, India and Norway – published by EWI - http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf

[12] A Global Protocol on Cybersecurity and Cybercrime - Stein Schjølberg and Solange Ghernaouti-Hélie An initiative for peace and security in cyberspace - Cybercrimedata - http://www.ewi.info/global-protocol-cybersecurity-and-cybercrime

[13] US Joint Forces command, "The Joint Operating Environment", Report released, Feb. 18, 2010, pp. 34-36

[14] 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 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[15] ARECI Study – March 2007 http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm

[16] 03/2009 – COM 2009/0149 - EU Commission Communication – "Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness,

security and resilience" http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[17] EC Non Paper on the Establishment of a European Public-Private Partnership for Resilience (EP3R). Version 2.0; June 23, 2010.

[18] Understanding cybercrime: a guide for developing countries. ITU, April 2009. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

[19] RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society) - Trust in the Information Society

8.2. Impact of cyber crime

[50] 05/05/2010 - The negative impact of cybercrime on the financial sector and the economy, Francesca Bosco - Project Officer - Interregional Crime and Justice Research Institute (UNICRI)

[51] 02/2010 – the Symantec State of Enterprise Security – http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf

[52] 01/2010 - Phishing Activity Trends Report, 4th Quarter / 2009 - http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf

[53] Annual Report, PandaLabs 2009. Panda Security. January 2010, http://www.pandasecurity.com/img/enc/Annual_Report_PandaLabs_2009.pdf .

[54] 12/2008 - Cybercrime survey – ISSA Ireland http://www.issaireland.org/2nd%20ISSA%20UCD%20Irish%20Cybercrime%20Survey%20-%20Results%2017DEC08.pdf

[55] 05/2010 –The evolution of energy security http://www.ensec.org/index.php?option=com_content&view=article&id=243:canvassing-the-cyber security-landscapewhy-energy-companies-need-to-pay-attention&catid=106:energysecuritycontent0510&Itemid=361

[56] 07/2008 –ITU Study on the Financial Aspects of Network Security: Malware and Spam - http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf

[57] 17/02/2010 –Balancing Cyber Threats and Cyber Benefits – Peter Altabef, Keynote speech, Worldwide Security Conference, Brussels - http://www.ewi.info/balancing-cyber threats-and-cyber benefits

[58] 31/12/2009 – Usage statistics of the Internet http://www.internetworldstats.com/stats.htm

[59] 23/05/2010 – "Patient billed for liposuction as medical theft rises", http://www.bloomberg.com/apps/news?pid=20601103&sid=ahZGb0_dw5wM#

[60] 02/2010 – the Symantec Internet Security Threat – http://www4.symantec.com/Vrt/wl?tu_id=SUKX1271711282503126202

[61] 25/05/2010 – "Botnet price for hourly hire on par with cost of two pints" – ZDNet UK - http://www.zdnet.co.uk/news/security-threats/2010/05/25/botnet-price-for-hourly-hire-on-par-with-cost-of-two-pints-40089028/

[62] 09/2009 – "Security and Resilience of information and communication technology networks for the protection of critical infrastructures" – An EOS White Paper - www.eos-eu.com

[63] John Arquilla and David Ronfeld, "In Athena's Camp", RAND 1997

[64] JLS/2008/D1/018 : A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet (presentation Final Conference by Thales – June 8th 2010)

[65] The Economics of Online Crime - *Journal of Economic Perspectives—Volume 23, Number 3—Summer 2009—Pages 3–20* - *http://people.seas.harvard.edu/~tmoore/jep09.pdf*

[66] 2009 – Interview of the US Cyber Security chief, Philip Reintinger http://www.spacewar.com/reports/US_cybersecurity_chief_warns_of_market_in_malware_999.html

[67] A Billion Dollar Market For Malware - Maksym Schipka, Senior Architect of Development, MessageLabs, 2007 http://www.fstc.org/docs/articles/messaglabs_online_shadow_economy.pdf

[68] Cybercrime's Financial and Geographic Growth Shows No Slowdown During the Global Economic Crisis http://www.tradingmarkets.com/news/stock-alert/symc_cybercrime-s-financial-and-geographic-growth-shows-no-slowdown-during-the-global-economic-crisis-922450.html

[69] CRS Report for Congress - The Economic Impact of Cyber Attacks - April 1, 2004 http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

[70] FUTURE OF CIVIL AND NATIONAL SECURITY IT & COMMUNICATION – SIEMENS: H.J. Wieser and CT SE4 Team

[71] A Global Protocol on Cybersecurity and Cybercrime / Cybercrime Data 2009 - Stein Schjolberg and Solange Ghernaouti-Hélie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf

[72] May 2010- Joint Report by EUROPOL, EUROJUST and FRONTEX on the State of Internal Security in the EU http://euro-police.noblogs.org/gallery/3874/st09359.en10.pdf

[73] Virtually here: the age of cyber warfare – Virtual Criminology Report 2009, McAfee http://www.mcafee.com/uk/local_content/reports/virtual_criminology_report/uk_virtual_criminology_09_report.pdf

[74] Virtual Criminology Report 2005, McAfee http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf

[75] http://www.havocscope.com/

[76] 09 Global Piracy Study - Business Software Alliance http://portal.bsa.org/globalpiracy2009/studies/globalpiracystudy2009.pdf

Annex I – International Approaches to Cyber Security

A.1. ITU – the Global Cyber security Agenda

In 2007, the International Telecommunication Union issued the Global Cyber Security Agenda (GCA) [9], highlighting the need to tackle the issue of cyber security through five pillars:

- Legal Measures.
- Technical and Procedural Measures.
- Organizational Structures.
- Capacity Building.
- International Cooperation.

The ITU also defined "Cyber Security" (ITU-T Recommendation X.1205) as:

"*The collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.*
Organization and user's assets include connected computing devices, users, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
Cyber security ensures the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.
The security properties include one or more of the following: availability; integrity (which may include authenticity and non-repudiation); confidentiality".

The ITU has since then been moving consistently forward in building awareness and moving towards implementation of the GCA, constituting a major contribution to European cyber security strategies.
The 2009 ITU report "Understanding cybercrime: a guide for developing countries" [18] gives a comprehensive view and explanation of cyber crime.
The implementation of the GCA is operated through IMPACT (see next section).

A.2. IMPACT – a private-public coalition on cyber security

The International Multilateral Partnership Against Cyber Threats (IMPACT) is a not-for-profit public-private "coalition" against cyber threats, whose objective is to assist partner countries, especially developing nations who are broadening their Internet capabilities. It entered into collaboration with the ITU in September 2008, effectively becoming the operational body for the ITU's General Cyber security Agenda issued in May 2007.

As the centrepiece of IMPACT is the Global Response Centre (GRC), equipped with a crisis room, IT and communications equipment, a fully-functional "always-on" Security Operations Centre, fully-protected secure data centre, facilities for shift workers, on-site broadcasting centre, VIP viewing gallery etc. The GRC plays a pivotal role in realising the ITU GCA's objectives of putting technical measures in place to combat new and evolving cyber threats.

Modelled after the CDC in Atlanta, U.S., the GRC is designed to be the foremost cyber threats resource centre in the world. Working with leading partners from academia, governments and industry (current partners include Symantec Corporation, Kaspersky Lab, F-Secure, Trend Micro, Microsoft, the SANS Institute and many other private sector stakeholders), the GRC provides the global community with a near real-time

aggregated early warning system. The GRC's 'Network Early Warning System' (NEWS) helps partner countries identify cyber threats on the onset and provides critical guidance on what measures to take.

The GRC provides the ITU's Member States with access to specialised tools and systems, including NEWS and 'Electronically Secure Collaborative Application Platform for Experts' (ESCAPE). ESCAPE is a unique electronic tool that enables authorized cyber experts across different countries and verticals to pool resources together to collaborate with each other remotely, within a secured environment; this may include IT experts, regulators, Computer Incident Response Teams (CIRTs) and white hats. By converging resources and expertise from many different countries at short notice, ESCAPE will enable partner countries and the global community to respond immediately to cyber threats, especially during crisis.

IMPACT is dedicated to bringing together governments, academia, industry leaders and cybersecurity experts to enhance the global community's capacity to prevent, defend against and respond to cyber threats. IMPACT's Global HQ is located in Cyberjaya, Malaysia. http://www.impact-alliance.org/

To date only Austria, Bulgaria, Italy, Poland and Romania, among the EU countries, are receiving cybersecurity services from IMPACT.

A.3. The pillars of the United States cyber security programme

In the US, "Cyberspace" is formally defined by the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.

When US President Obama took office, he required a full policy review of the cyber security issues. Consequently, the US Cyber Security review policy document was issued in May 2009.

The relevance of this document lies in the fact that the United States faces similar issues as Europe does, namely the fact that cyber security is currently tackled in isolation by different agencies, that the vulnerability of infrastructures to a coordinated cyber attack is high and cyber security strategies have to also take into account the issues of privacy and data protection.

The Cyberspace Policy Review document[8] issued ten recommendations, among which the following are of direct relevance to the European cyber security policies, including:

- the need for education,
- the need to set-up an inter-agency coordination force,
- the need to prepare cyber security incident response plans,
- the need to support research in an overall framework fostering the development of coordinated solutions and processes.

The US have set up several initiatives and bodies to coordinate at national level the response to cyber threats.

The US now operates a Comprehensive National Cybersecurity Initiative (CNCI), and the military is responsible for operating a US Cyber Command centre which has received $139 million for operation in 2011.

At a the cyber security summit organized in the first quarter of 2010 by the EastWestInstitute (EWI) (http://www.ewi.info/worldwide-cybersecurity-summit), the CNCI reinforced the public role, stating that "*The government must also figure out its role in the cyber defenses of power grids, financial markets and other computer infrastructure that have become critical to daily life in this country*".

Another important US initiative is the US-DHS National Cyberspace Response System that seeks to protect the critical cyber infrastructure 24 hours a day, 7 days a week coordinating the cyber leadership, processes, and protocols that will determine when and what action(s) need to be taken as cyber incidents arise.

A.4. Other international initiatives

A.4.1. The EastWestInstitute initiative on cyber security

The EastWestInstitute is an international think-tank focusing on the critical challenges endangering peace. Among its programmes it has set-up a world-wide cyber security initiative and just organised a cyber security summit.
Of relevance to Europe are the different collaborations involving different parts of the world, including Russia, China, India, Norway and other European countries [11].

The EWI Interim report from the first Worldwide Cybersecurity Summit is proposing, among other, the following analysis of and recommendations on cyber security, quite similar to those made by the EOS ICT security working group the previous and the present White Paper.

Analysis:

- lack of a commonly-agreed definition and how threats and risks are evaluated and responses framed;
- ineffective integration of the necessary technical, business, legal, security and international policy competencies;
- appropriate domestic legal frameworks on which international cooperation has to be founded;
- inadequacy of the commercial drivers for building security into network equipment, software, networks and services, the inadequacy being the result in part of a lack of consumer awareness of the risks they face and a lack of leadership and commitment from those in control;
- national approaches to their online security are often too parochial for collaboration on crafting global cyber regulation;
- industry has been content to sell products without embedding adequate security measures into them and without adequate attention to the integrity of the supply chain for components. Many of the technologies we have in place are almost indefensible. So we are constantly patching the cracks and filling the holes;
- governments and private industry need to work collaboratively to develop the appropriate international framework to secure cyberspace but in a way that keeps our global information systems intact and secure;
- there is a preponderance of evidence that indicates cybercriminals, including terrorists, could inflict major outages to portions of our critical infrastructure with minimal effort (cyber security is asymmetric);
- there are important economic dimensions, especially when it comes to vulnerability, but also social and individual dimensions (the people operating the systems);

- mistrust is impeding collaboration needed to improve the cyber defenses that can help to underpin global economic prosperity and stability. The mistrust also plays out in restrictions on the market access of some ICT companies from one country in others.

Recommendations:

- new and effective public-public, private-private and public-private cooperation in a wide range of areas are urgently needed;
- the lack of effective common procedures for attribution is a key weakness in cybersecurity: we need to promote some type of global electronic architecture that allows cyber attacks to be traced back to their sources;
- we need to create market incentives to encourage the private sector, which owns and operates most of the world's digital infrastructure, to tackle minor crimes.

A.4.2. The UNICRI activities on cyber security

The United Nations Interregional Crime and Justice Research Institute – UNICRI –is a United Nations entity established in 1967 to support countries worldwide in crime prevention and criminal justice. UNICRI operates on the cyber crime arena as part of the Emerging Crimes domain, and is an important contributor to monitoring, understanding and training activities in cyber crime. [50]

A.4.3. The NATO policy on cyber security

A series of major cyber attacks on Estonian public and private institutions in April and May 2007 prompted NATO to take a harder look at its cyber defences.

NATO is continuously developing and enhancing the protection of its communication and information systems against attacks or illegal access. These efforts represent the practical implementation of NATO's 2008 policy on cyber defence.

The policy establishes the basic principles and provides direction to NATO's civil and military bodies for ensuring a consolidated approach to cyber defence and coordinated responses to cyber attacks. It also contains advice to individual Allies regarding the protection of their national communication systems.

The cyber defence policy is currently being implemented by NATO's political, military and technical authorities, as well as by individual Allies. A main aspect of the policy was the establishment of a Cyber Defence Management Authority (CDMA) with the sole responsibility for coordinating cyber defence throughout the Alliance. It constitutes the main consultation body for the North Atlantic Council on cyber defence and provides advice to member states on all main aspects of cyber defence.

NATO has developed mechanisms for assisting those Allies who seek NATO support for the protection of their communication systems, including through the dispatch of Rapid Reinforcement Teams (RRTs) However, the Allies themselves continue to bear the main responsibility for the safety and security of their communication systems.

The "Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, which was set up in 2003 and accredited as a NATO CoE in 2008, conducts research and training on cyber warfare and includes a staff of 30, including specialists from the sponsoring countries (Estonia, Germany, Italy, Latvia, Lithuania, Slovakia and Spain).

In mid-2002, the implementation of a Cyber Defence Programme was approved by the North Atlantic Council. The programme provided a comprehensive plan to improve the Alliance's ability to defend against cyber attacks by improving NATO capabilities.

In 2002 the NATO created the Computer Incident Response Capability (NCIRC) as a part of the Cyber Defence Programme.

The NATO Communication and Information Services Agency (NCSA), through its NCIRC Technical Centre, is responsible for protection of communication and computer security throughout NATO. NCIRC has a key role in responding to any cyber aggression against the Alliance. It provides a means for handling and reporting incidents and disseminating important incident-related information to system/ security management and users. It also concentrates incident handling into one centralized and coordinated effort, thereby eliminating duplication of effort.

The comprehensive plan is divided in three phases:

- The first phase covered the creation of the currently functioning NCIRC and establishing its interim operating capability;
- The second phase will make most NCIRC capabilities fully operational by 2012;
- The third phase identifies requirements and resources to eliminate or mitigate other vulnerabilities. This initiative broadens the cyber defence view for inclusion of CDMA capabilities and the identification of "Enterprise-wide solutions" and demonstrates how new technologies could be exploited to reduce the risks associated with cyber attacks.

ANNEX II -
Impact examples of cyber threats by sector

Activity sector	***Cyber method***	***Impact***	***Numerical information***
All sectors (payments, health etc)	Phishing and malware	Identity theft	- in 2009, 11.1 million US Citizens experienced identity fraud for a total cost of $54 billion Source - Javelin Strategy & Research
Payments	Phishing / Fake access points	Credit card information fraud through individual identity theft (individual, requesting information to be sent by individuals)	- in 2009 60 % of identities exposed were compromised by hacking attacks - the majority of these were the result of a successful hacking attack on a single credit card payment processor Source – Symantec Internet Security Threat report [60]
Payments	Malware / hacking	Credit card information fraud through identity theft (large scale -> all IDs are obtained through the credit card processing company)	
Banking	Bot nets / Fake access points	Banking information theft (banking account and credit card)	- The Mariposa botnet, believed to have been composed of 12.7 million PCs stole credit card and bank log-in data and infected computers in half of the Fortune 1000 companies and more than 40 banks
Healthcare	Phishing	Identity theft leading to false claims of medical treatment	- 275.000 thefts of medical identities in the US in 2009 - increased by 50% over 2008 Source - Javelin Strategy & Research / Bloomberg [59]
Public administration	Bot nets	Denial of services leading to unavailability of services	- in 2007, massive and prolonged denial of services attacked disrupted Estonia in the public sector, the banking domain and schooling. Computers involved in the bot net were identified all over the world, including United States, Canada, Brazil, Vietnam
Public administrations	Malware	Virus infection, stealing of information	- The Pentagon admitted in April that it had spent $100 million over the last six months of 2009 making good the damage done by cyber attacks and other related problems [53].

ANNEX III – 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 30 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, with the participation of:

ENGINEERING	**Veronique**	**Pevtschin**	**WP Editor**
ENGINEERING	Dario	Avallone	WG Chairman
ALTRAN	Jean-Philippe	Perin	
ALTRAN	Alexander	Heijnen	
ALTRAN	Sébastien	Renouard	
ATOS ORIGIN	Jose-Maria	Cavanillas	
ATOS ORIGIN	Pedro	Soria	
ATOS ORIGIN	Aljosa	Pasic	
BAE Systems	John	Bennet	
BAE Systems/ Detica	Nefyn	Jones	
BAE Systems/ Detica	Steve	Daniels	
BAE Systems/ Detica	Ben	Bridge	
BUMAR	Tomasz	Miroslaw	
CEA	Alain	Merle	
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	
FINMECCANICA/Selex S.I.	Eugenio	Creso	
G4S	Mike	Clarke	
HAI	Nikolaos	Priggouris	
HAI	Evangelos	Ladis	
INDRA	Fernando	Carvajal	
INDRA	Isabel	Bozzino	
IBM	Peter	Stremus	
IBM	Alessandro	Faustini	
IBM	Gerardo	Zuliani	
IBM	Jean Paul	Ballerini	
IBM	Marc	Le Noir	
IBM	Francesca	Ferretti	
KEMEA	Georgios	Leventakis	
KEMEA	Michael	Tsinisizelis	
RAYTHEON	John	Brading	
SIEMENS	Andreas	Seum	
SIEMENS	Hans Jürg	Wieser	
SMITH DETECTION	Michael	Andreas	
SMITH DETECTION	Raymond	Ray	
SMITH DETECTION	Magnus	Ovilius	
THALES	Paul	Theron	
THALES	Thomas	Hutin	
THALES	Milton	Yates	
THALES	Yves	Lagoude	
THALES	Lionel	Le Cleï	
THALES	Fabien	Cavenne	
EOS	Sophie	Batas	WG Support
EOS	Luigi	Rebuffi	WG Supervision