Steps towards implementing a European cyber-security strategy

November 2011

An annual publication by the
EOS ICT / Cyber-Security Working Group

EUROPEAN ORGANISATION FOR SECURITY

Table of Contents

1. Executive Summary

In September 2010, EOS, representing European companies and research centers active in the security market, issued a white paper scoping the issue of cyber-security and calling for an integrated European programme and coordinator.

EOS is calling now on Europe and its Institutions to take a leap forward by ***implementing*** a ***consistent and integrated cyber-security strategy***, *whose goal is to* ***federate*** *the different stakeholders and* ***consolidate*** *the on-going initiatives, while* ***identifying the additional actions*** *required to improve the resilience, dependability and security of cyber-space*.

In implementing this strategy, Europe has to overcome traditional barriers between domains, as these boundaries do not reflect the reality in cyber space. It should also evolve from a purely ICT and network centric handling of cyber-security to an integrated view, taking into account the fact that cyber disruptions may seriously impact both the information and the physical worlds.

From our analysis, the reality of cyber space can be expressed in eight key points:

a) While **cyber-space** has been enabled by technology, the **human factor** is a major element when analysing its security. Cyber-space connects over 2 billion people not only together, but also to physical and information infrastructures – putting people at the forefront both as potential creators of disruptions and as targets for failures created through cyber-space.

b) ***Disruptions,*** whether occurring through unintentional errors or resulting of targeted threats, have been a reality for over a decade and their number is **increasing year after year.**

c) Europe needs to take stock of the current reality: Europe's **critical infrastructures are most probably already contaminated**, with logic bombs and trap doors possibly implanted in at least part of our energy, nuclear, transport and/or communication infrastructures.

d) Even if the political recognition of the dangers exists and if a number of key initiatives are on-going, ***Europe lacks a cyber-security strategy***, whilst cyber disruptions have the capability to destroy our ICT based and ICT connected infrastructures and our modes of operations within a few minutes or even seconds, thereby leading to a significant impact on the European economy, society and citizens.

e) All sectors are today using IT / cyber technologies and the majority of them are interconnected. As the **cyber-space is much larger than the Internet, a European cyber security strategy should be wider than an "Internet security strategy".** Key stakeholders from the private sectors for this global strategy include not only telecom operators and software manufacturers but also operators and users of other kinds of infrastructure and services as well as component, device, system manufacturers and cyber technology developers.

f) Compared to other nations and continents, the ***European*** context adds a ***specific complexity*** in that it is an alliance of ***27 Member States***, each with **different levels of preparation and capabilities** to address cyber-security challenges. However, this

complexity should be exploited as an advantage by building on existing competencies across Member States to share the required knowledge and skills.

g) In implementing a cyber-security strategy, Europe also has to ***bridge the gap*** between the civilian and military worlds, clearly understanding how to elaborate ***defensive "civilian" capabilities*** linked to intelligence and other data sources, while at the same time clearly separating it from "military" offensive capabilities.

h) Cyber-security is a source of continuous innovation, and by focussing on this aspect the market has the potential to **contribute to economic growth and to job creation** by bringing these innovations to market.

Our overall analysis is set in a ***context of urgency***: in the commercial sector, the financial market crisis introduced the concept of stress tests for the banking institutions, which is now also considered for nuclear installations following the Fukushima events. A similar concept could be extending to cyber-space, testing the different levels of resilience of infrastructures and systems to underlying networks and IT solutions to identify weaknesses and prevent major negative consequences.

In this 2011 edition of the EOS ICT white paper, we not only provide a more in-depth understanding of the needs, but also further elaborate on our 2010 proposal for:

- *The definition of a comprehensive **European cyber-security strategy**, spanning beyond Internet security, including also the introduction of a European approach to CIIP into the revised EU CIP Directive;*
- the definition of a **European cyber-space** federating national cyber-spaces where cyber-security services are assured by **(national) trusted cyber-security operators**;
- *the **implementation** of the European cyber-security strategy through a **European cyber-security public private - cooperation**, or as currently used but improperly – partnership;*
- *the creation of a **European Cyber-Security Coordinator**, based on the model of the terrorism coordinator, to coordinate with the Member States decisions and actions to address cyber threats and implement the strategy;*
- *the creation of a **European Cyber-Security centre to operationally coordinate** the preparedness, prevention and response to cyber-disruption by **complementing** the local levels of response by an EU coordination level. This centre could also be deployed by adding this coordination role to an existing agency through a mandate extension;*
- *the allocation of **resources to implement gap filler cyber-space control and real time protection capacities, bringing EU MS to a common protection level** of the cyber-space.*

Note: this is the 2011 annual and 3rd publication by the EOS ICT/Cyber-security working group, for reference:

- 2009 edition: Security and Resilience of Information and Communication Technology networks for the protection of critical infrastructures
- 2010 edition: Towards a concerted EU approach to cyber-security

2. Introduction

Over recent years and indeed months, the vulnerability of cyber-space has increasingly come to light.

Connecting over 2 billion people[156] as well as devices, information and physical infrastructures, cyber-space has introduced numerous benefits in terms of education, information exchanges, innovative industrial processes, researcher connectivity and more.

However, it also provides unprecedented levels of access to core infrastructures and data sources – opening the door to failures created through human error, malicious or even criminal intent. Cyber-space is also being used in the context of offensive approaches between nations.

Malicious intent cyber-attacks (i.e. voluntary action of cyber terrorism or cyber crime: cyber pornography, electronic money laundering, identity and personal data stealing as well as modifying the operations of critical infrastructures etc.) **have become *more professional*** and grown both in **magnitude** and **reach**.

In parallel, our increasing **societal dependence** has made us more vulnerable to (man-made or technical) mistakes and natural disasters cyber-threats, which can result from non-voluntary events such as electrical collapse, data center flooding etc.).

The reality today is that **cyber-space is both the key enabler of our economies and societies and one of its major weaknesses.** Cyber-space is a domain in which nobody, neither Europe nor other countries and continents, controls the current and future evolution.

Some nations have tackled cyber-space by building a strong offensive capability, enabling them to use this capability in replacement or complement to military operations. At the same time, nations have also built defensive capabilities.

For instance, while the United States seems to have a strong offensive capacity in cyber-space, it has also created a central command centre able to strengthen its capacity to increase the cyber-resistance of US critical infrastructures.

China has also created both offensive and defensive capabilities, and their controlling approach of Chinese cyber-space provides it with the capability to cut-off its cyber-space from outside attacks and to control content exchanges inside it [108].

Most advanced countries have also developed an *intelligence* capability for cyber-space.

The Council of Europe took the initiative to harmonize anti-cyber crime approaches by developing the Cyber Crime Convention, currently supported also by a number of nations outside the Council such as Australia, Japan and the United States. Other nations plan to join and adopt the agreement in their legislation.

Europe has also developed other major initiatives. As highlighted in the March 2011[100] communication by the European Commission, these are going through important evolutions, including:

- the enhancement of the role of ENISA as a support organisation in all aspects of security and resilience of information networks;

- the on-going work by the EFMS – European Forum for Member States, established in 2009 and the evolution of the CIIP directive in proposing a draft definition ICT critical infrastructures;
- the creation in November 2010 of the EU-US working group on cyber-security and cyber-crimes;
- the steps to establish a pan-European network of CERTs to support preparedness, information sharing, coordination and response;
- the EISAS roadmap, defining the steps towards the elaboration of a European Information Sharing and Alert System by 2013;
- the actions in the Internal Security Strategy and in the Digital Agenda for Europe addressing cyber-crime on the one hand, and trust and security on the other;
- the progressive ratification of the cyber-crime convention, as previously said;
- the recent study by the SEDE sub-committee of the European Parliament on cyber-security[101];
- the ongoing EP report on "cyber attacks against information systems";
- etc.

All these elements constitute key elements of support towards cyber-security. Yet, **they do not form an integrated approach**.

If tomorrow Europe faces a major cyber-attack, what will the response be? Who will coordinate this response? How will the local structures work together to ensure European wide implementation? Do we have differentiated approaches based on the sector (financial, logistics, transport, health etc) impact of these attacks? Where is the strategic decision centre? Where is the operational coordination centre?

Europe has not yet built a defensive policy and capability in coordination with its MS. While several MS have set up their own national programmes, the lack of a harmonized and defragmented approach across Europe is at risk of hindering any real cyber-security capability at higher coordination level.

This is the context in which EOS is presenting its 2011 white paper on cyber-security.

The white paper starts by detailing the role played by EOS and its members in cyber-security. It then analyses security as an underlying (missing) feature of cyber-space before moving to the real impact of cyber-disruptions. This includes the risk of cyber crime, cyber espionage, cyber activism, cybotage and ultimately cyber conflict/cyber war. Taking into account the on-going European initiatives and the numerous 2010-2011 developments, it then provides suggestions for the definition and the implementation of a **defensive cyber-security strategy for Europe**.

While this paper is put forward by organisations active in the security market, it is essential that all stakeholders are involved in this proposed strategy, from academia to industry, from SMEs to large corporations, from private to public institutions and agencies, at national, European and international levels.

It is also important to move beyond the traditional civilian / military separation to incorporate, in the strategy, what level of cooperation is needed and how it could be implemented. We need to facilitate ways of sharing best practices and information between law enforcement forces and the military, also with support of the expertise brought by the private sector. An example is the approach adopted by the Dutch strategy which includes the use of reserve military personnel with cyber-expertise for co-operation in resolving cyber-disruptions in the civilian society and which was used when bringing down the Bredolab botnet[161].

3. EOS's contribution to cyber-security

Following the 2009 issue of the EOS White Paper on "Security and Resilience of Information and Communication Technology Networks for the Protection of Critical Infrastructures"[106], discussions with high representatives of the EU Institutions (Parliament, Council of the EU, Commission) and of some Member States (MS), 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.**

This led to the 2010 issue of the EOS White Paper "Towards a concerted EU approach to cyber-security"[107], used as the basis for presentations to the European Commission, the European Parliament and the Budapest Ministerial conference on cyber-crime in April 2011.

It was also at the centre of the EU-EOS High Level Security Roundtable organised by EOS in February 2011 and attended by representative of the Hungarian EU Presidency, representatives of the Council of the EU, of the Parliament and of the European Commission (in particular, European Commissioners: C. Malmström, S.Kallas, A.Tajani), EU Agencies and experts from Ministers of Interior of some Member States and high level representatives from industry and research centers member of EOS.

In the 2010 edition, we defined **Cyber-Security as the protection of Cyber-Space.** Several other definitions exist, often linked to the separation of domains. Administrations in EU Member States and the European Commission are segmenting their activity according to their function and mandate: traditionally, ministries of interior deal with cyber protection of the government and its agencies, ministries of justice deal with "cyber crime", ministries of economic affairs / industry / telecom deal with "cyber-security" / trust and CIIP (Critical Information Infrastructure Protection), ministries of defence deal with "cyber operations".

However, as appears clearly in the study commissioned by the European Parliament - SEDE sub-committee[101], the **cyber space requires a complete rethink and adaptation to overcome the existing separation** between organisations and to move to a level of collaboration and integration without which effective cyber-security will never be achieved.

This 2011 edition of the EOS ICT / cyber-security white paper is the third contribution that EOS makes to the cyber-security debate, and in doing so, we are expressing on the one hand:

- the urgent need for coordination at a European level, building on the numerous existing initiatives[100] and moving to the next level of coherence and consistency without which cyber-security will never be achieved;

and on the other hand:

- the willingness of private organisations of the security sector to participate in this initiative.

4. Security is not an underlying feature of cyber-space

Cyber-space can be seen as a conglomerate of information, ICT-means and ICT-services. Cyber space comprises for example mobile telephony and data, medical equipment, the Internet, process control systems, in-car systems, etc. Through this approach, cyber-space essentially delivers unprecedented levels of interconnection, built on both private networks and the Internet.

In less than two decades, the Internet grew from linking together known and identifiable human beings (in a research context) operating in identified organisations into a means through which over 2 billion [156] people are connected and to which an increasing number of devices are also becoming connected.

In this growth, **security was not taken into account.** This is still often the case today, with new developments appearing every day, introducing new functionalities without considering security as a key enabling feature, or without fully evaluating the complexity of required security level. And these new developments appear **across all sectors** – as illustrated by, for instance, the introduction of "cyber-tire", a joint development in the automotive industry to incorporate an intelligent micro-chip based system in the tires, to report specific parameters and connect wirelessly to the car's computer [163] which opens many potential security concerns. As described in a March 2011 publication by MIT in its Technology Review journal, researchers recently demonstrated that they could control everything from a car's brakes to its door locks to its computerized dashboard displays through the Bluetooth connections intended for making hands-free phone calls. [164]

Overall, this has led to an interconnected world with little focus on important concepts such as the resilience of our key infrastructures and connected devices. Furthermore, while **cyber-space is much larger than the Internet**, Internet is an important component of the connectivity and the openness principles that govern it are sometimes not aligned with overall security needs of people, applications and processes.

Even after several decades of working to increase its security, the Internet is fundamentally vulnerable at many different levels [108]:

- *infrastructure level*, including routing and the Domain Name System responsible for the redirection to the correct Web site which can be hacked to misdirect to Web pages [156];
- *application level*, including access control, mashups or service compositions, usage of unencrypted information flows etc;
- *governance level*, lacking a single decisional body empowered to act as the "security responsible" of the Internet, which by essence, cannot be supervised by any kind of unique centralized entity;
- *usage level*, where users are manipulated to provide confidential information or simply are not aware of the risks they take through inappropriate behaviours;
- etc.

In parallel, the last two decades saw a *complete industrial (r)evolution* based on using IT to increase productivity and competitiveness of the European economy.

From just-in-time processes to remote control, these solutions were developed with **the main focus** on **improving process efficiency and cost reduction**, and not always with sufficient **security**. This evolution introduced in certain applications not only internal connectivity and dependency but very often also external connectivity, including with public infrastructures such as mobile telecommunication systems and the Internet which are essentially unsecure environments accessible to all.

The last decade also saw a revolution in the *interaction models of society*, with personal devices becoming pervasive across our lives, as well behavioural changes.

The complexity of information devices, systems, and networks, combined to non-deterministic factors, such as human behaviour, makes assurance of trustworthiness impossible. Instead, the **associated risks have to be managed**.

Today, the **lack of structured risk management** leaves the world in a situation where computers, infrastructures and personal devices are interconnected in a complex manner, to enable local and remote, fixed and mobile interactions (for instance, remote metering, car diagnostic and localisation, etc). And cyber-disruptions can occur at device level.

This element is key, in that the issue of security in cyber-space is **not only dependent on the connectivity** (and therefore ICT networks), but also on the connected devices themselves, bringing up as a major domain of cyber-security the completely different area of the **integrity of the connected devices**, an aspect that branches out from networks to microprocessors, system architectures, software design etc, i.e. all the components which are at the heart of our systems and which can also be compromised at different levels, right from their manufacturing and design to their deployment and operation until after their decommissioning (proper destruction of sensitive information is often forgotten).

For instance, the possibility exists that microprocessors are "equipped", at manufacturing time, with a "door" that would enable cyber-attacks on the systems in which they are incorporated. Cyber-security strategies should also address these aspects, leading to **novel approaches in evaluation, assurance, industry-led certifications and standards related to the incorporation, procurement and selection of the hardware and software incorporated in our products**.

Security is also an important element in **cloud computing**, a high-growth area that introduces many dimensions related to security. This is another example of an innovation whose key benefit is not security, but which will not be deployed *without* the underlying and compulsory security processes, approaches and guarantees.

Security issues associated with cloud computing fall into two broad categories:

- security issues faced by cloud providers (organizations providing Software, Platform, or Infrastructure-as-a-Service via the cloud) and
- security issues faced by their customers.

In most cases, the provider must ensure that its infrastructure is secure and that clients' data and applications are protected, while the customer must ensure that the provider has taken the proper security measures to protect his information, but also that his internal processes to access this information are themselves secure. In order to ensure that data is secure and that data privacy is maintained, cloud providers attend to the following areas:

data protection, identity management, physical and personnel security, availability (regular and predictable access to data and applications), application security (testing and acceptance procedures for outsourced or packaged applications), and privacy.

Security was not taken into account in the early years of cyber-space. Security is not a feature that can simply be built-in to cyber-space as it exists today.

Security of the cyber-space is much larger than the simple Internet security.

As demonstrated in the examples in cloud computing and in the automotive sector, tackling cyber-security requires moving far beyond networks security and resilience, and includes organisational aspects, physical security, personal security, electromagnetic security as well as verifying, guaranteeing and monitoring the integrity of connected systems and that of their underlying components such as hardware, software and services.

5. The impact of cyber-disruptions

In our previous 2010 publication, we outlined a number of techniques, from botnets to malware used to destroy or limit functional capabilities. But while understanding the techniques is of course of utmost importance, the real starting point for a European strategy is understanding the **full (potential) impact of cyber-disruptions**.

Cyber-disruptions can be created through multiple origins, from human error to cyber-attacks. But whatever their origin, cyber-disruptions have in common the impact on information source or physical infrastructures or both, ultimately leading to societal and economical impacts.

Over the last months, the impact of cyber-disruptions has evolved:

- ***from an ICT focused impact,***

  meaning that the disruption is caused by unauthorised access to privileged /personal information sources or structures. In the case of malicious intent, information can either be retrieved for further usage and / or destroyed. In other cases, information structures such as Web sites can be destroyed by limiting the communication capabilities of networks. A recent incident [162] combined human error and malicious intent and led to human, intelligence and economic impacts; in this incident, certificates were stolen from Diginotar, Dutch subsidiary of US company Vasco Data Security International. These certificates were then used to access information from CIA, Mossad, MI6 and more –leading to Diginotar filing for bankruptcy 3 months after the initial incident and Vasco moving out of the digital certificate authority market.

- ***to a physical world* impact,**

  in accessing process control systems, usually referred to as SCADA[1] systems. Malicious intent was behind the cybotage case with the Stuxnet[155] worm which was analysed as destroying Iranian nuclear facilities, where the approach used a Microsoft Windows flaw to access a SCADA system, modify its functionality and thereby the behaviour of the controlled system leading to damaged physical processes and extreme wear and tear and thereby its destruction. Another example of physical destruction capability was demonstrated in the United States under the Aurora[108] test conducted in Idaho that destroyed a large electric generator accessed through cyber-space. But these accesses can also be achieved through accidental mistakes, often involving human error and / or under-qualified personnel.

Therefore, while the theft of data such as logins, credit card numbers and more are the most publicised ones, the most dangerous ones are those who impact the infrastructures, from energy distribution to banks, from retail to supply chains, from personal devices to mobile transport, from health to public administrations and more.

Today, cyber-disruptions have the potential to destroy the operations of our so-called "critical infrastructures". This is where the European institutions initiatives on CIIP are fundamental, at directive, definition and support levels. However, the progress status of such initiatives is neither operational enough nor extensive enough to protect these infrastructures.

[1] SCADA - Supervisory Control And Data Acquisition

A comprehensive EU cyber security Strategy should also consider how to better include CIIPs in the revision of the EU CIP Directive.

The potential impact of cyber-disruptions goes far beyond the publicised data breaches, and affects the infrastructures without which our economy and society cannot function.

Understanding the extent of this impact and how it branches out into our economy, and most specifically into which sectors of our economy – financial, logistics, health, transport, information, public administrations etc- should guide the ambition of the European cyber-security strategy.

The human element is often a determining factor either as (willing or unwilling) initiator of a disruption or as target.

This requires moving to the right (top) level of strategy and then moving back to issues such as private-public "partnerships", regulations and directives, research and development, education and awareness, relationship to and embedding in other areas of advancement (e.g. smart energy grids, car-with-car/car-with-road infrastructure systems etc), network security and resilience and more.

---

6. Europe's approach is fragmented

The previous sections outlined a view of "the dangerous life" in cyber-space. Today, the question is **not whether** we are at risk, **but when** a large-scale cyber-disruption with serious impact to our economy, society and citizens will occur. Today, the reality is that cyber-disruptions have the potential, in the coming months (now, today, tomorrow), to damage the European economy and the world-wide economy.

In our 2010 edition of the EOS ICT/cyber-security white paper, we already underlined the fragmentation as a major challenge to address. Since September 2010, numerous activities have been on-going and Europe has acted already at many different levels.

At national level the definition of national cyber security policies across some Member States, the creation and development of national IT security agencies like ANSSI, BSI, CESG, etc., the deployment of CERT's, have increased the prevention and response to threats. Yet these policies and capabilities remain "patchy" across EU MS.

At EU level, legislative activities on "cyber security" are ongoing at the European Parliament; policy or development activities are managed by DG INFSO, DG HOME, DG ENTR; the intelligence activities of the EEAS (via the SITCEN) and at the EUMS, are particularly active in following links with national policies and activities, while EDA is now appearing on the scene.

The on-going work around the EU critical infrastructures directive and the needed Operator Security Plan – OPS - is extremely important. However, this is mainly focused in *acting after* an incident occurs, rather than *avoiding its occurrence*.

The role played by ENISA in taking stock of the current situation is of major importance, with many relevant on-going studies ("Industrial Control System/SCADA Security", the ''Cyber-Security aspects in the Maritime Sector'' etc). ENISA's activity as facilitator of the Cyber Europe exercise organised by the Member States has been key.

The contributions by ENISA are indeed very important, but how will these contributions effectively ***influence*** the security of cyber-space? The overall "support" role defined for ENISA is a major component – but the real *impact* and *uptake* dimensions are not yet sufficiently organised. Similarly, the role of Europol including its activities as a cyber-crime information centre is central, but how are the links between law enforcement and ICT, between sectoral aspects and cyber-crime response implemented?[1]

The annual Organised Crime Threat Assessment (OCTA) report [154] and the new Internet Facilitated Organised Crime (iOCTA) by Europol are also important contributions, as well as the creation of the European cyber-crime task force. Together, Europol and ENISA have the potential to form the backbone of cyber-security operations - but to date, their activities have remained largely separate. This backbone is for instance demonstrated by the recent creation of the ICSPA[2] – International Cyber Security Protection Alliance – of which Europol is a member and where ICT oriented aspects of cyber-security are also addressed.

The research and pilot oriented programmes under the FP7 and CIP frameworks have fostered a number of projects, such as Wombat, Demos or Syssec contributing to the

[1] http://europol.easyred.com/

[2] www.icspa.org

development and / or deployment of novel technologies that *could* contribute to cyber-security.

At EU policy level, the inclusion of concrete actions related to cyber-security in the EU Internal Security Strategy and the Digital Agenda is another major step forward.

The current issue is not the lack of initiatives, but on the contrary the multiplicity of different, unconnected activities. Across all these initiatives, *the* ***major drawback remains the lack of integration***: cyber-space has to be tackled as a whole, and security can only be achieved through an end-to-end approach.

Network issues cannot be tackled in isolation, the critical infrastructures cannot be addressed without strongly taking the IT and SCADA dimensions into account, the human factor has to be addressed through education and novel "integral" engineering methods etc.

A European cyber-crime centre is envisaged by the EU Internal Security Strategy but what will be its range of activities? Its mandate and link with other EU initiatives?

Cooperation in the cyber security area in Public – Private "Partnerships" is an effective need: indeed most of the ICT infrastructure belong to / are operated by the private sector, whilst having a public impact.

The private-public partnership of EP3R[1] focuses on network resilience, but how will its activities effectively impact cyber-security? For instance, in focusing the debate at network level, the participating network operators are often aiming to protect their own processes, but lack the cross-sectoral dimension required to effectively **implement a secure cyber-space**, which would include application level, service provision level, users etc.

At international level, NATO and the UN (also via the ITU) are major players to coordinate actions at wider scale.

Yet, we have to recognize that the links between civilian and military activities, between intelligence based approaches and information gathering processes are still weak.

The creation in November 2010 of an EU-US Working Group on Cyber-Security and Cyber-Crime and the definition of the issues to be tackled in April 2011 constitute a major step forward. But is this activity sufficiently connected to a similar activity on-going between NATO and the United States? In a recent announcement[2], NATO launched an activity with the Atlantic Council focused on cyber-security. But what is the cooperation with Europe on this? A similar group between the US and China recently issued a publication [113] detailing the collaboration on cyber-security between these two nations, US and India launched a similar activity – is the US-EU group advancing fast enough?

Cyber-space is at the heart of the entire European economy and society. Cyber disruptions of infrastructures, data and processes have the capability to damage the entire economy.

European Member States have developed national cyber-security programmes with different levels of advancement. Europe has initiated a

---

[1] European Public-Private Partnership for Resilience

[2] http://www.ibm.com/news/be/en/2011/06/29/s710043l16521n85.html

large number of activities.

The issue today is not the lack of activities, but the multiplicity of initiatives.

Protecting cyber-space requires a coordinated strategy matching the potential negative impact of cyber-disruptions.

7. The European Cyber-Security Strategy

The previous section outlined the importance of an end-to-end approach, taking all dimensions into account. This section focuses on ***consolidating the different elements*** of this **end-to-end approach towards a European cyber-security strategy**.

It details the different steps required to elaborate a European cyber-security strategy including:

- Goal
- Added value
- Scope
- Critical challenge
- Taking stock of the reality
- Identifying the key stakeholders
- Building on the European knowledge and skills
- Structure
- Areas of work

7.1. Goal

The goal of the European Cyber-Security Strategy is to protect Europe's society, citizens, infrastructures and economies from cyber-disruptions. This **protection covers all phases, from prevention to preparedness and response**. It has to deliver complete *sectoral* coverage, from financial to logistics, from transport to education, from public administrations to supply chains and more.

This goal requires delivering the correct levels of ***speed*** and ***reach*** capabilities, through an *end-to-end comprehensive* approach supported by efficient governance for implementation and management, leveraging on **appropriate tools, leading to the consolidation of present initiatives and competences and the defragmentation of the market.** Considering the **interdependence and complexity** of the cyber-security interests of both public authorities (institutional networks and systems, regulators and public agencies) and the private sector (operators, Internet Service Providers, security solutions providers, users), **public-private mechanisms** should play a prominent role in this consolidation**.**

As part of the envisaged European Cyber-Security Strategy, but worth mentioning specifically due to its importance, **a European approach to CIIP (Critical Information Infrastructures Protection) should be introduced into the revised EU CIP Directive.**

7.2. Added value

The main role of the European Cyber-Security Strategy is not to define a new strategy from scratch, but to:

- ***federate*** the different actors

and

- ***consolidate*** the numerous initiatives

into an integrated, dynamic, operational, transparent and agile approach, building upon on-going and upcoming activities and moving beyond network security and information sharing all the way to joint operations and efficient cyber-security protection, whilst taking into account subsidiarity principles and national security prerogatives.

The added value lies in building a comprehensive, structured and coordinated approach to the challenges posed by cyber-security:

- organising a global response,
- federating national efforts,
- respecting local logics,
- helping multiple stakeholders develop network-wide responsibility awareness,
- optimising the knowledge and skills available across Europe,
- coordinating across European initiatives

and overall building a European cyber-security capability without which Europe will never be able to ***deliver the speed and reach*** required to address cyber-threats and disruptions.

The benefits of this integrated view are numerous, including:

- creating the *decisional and operational governance* required to secure cyber-space, from prevention to preparedness and response,
- setting the *expected impact* of different actions, as well as the channels through which these actions contribute to cyber-security,
- identifying and filling the gaps across the different existing initiatives,
- defining the European channel(s) at *international level,*
- defining concrete targets for research,
- assessing funding requirements,
- allocating operational responsibilities and defining milestones to monitor progress.

7.3. Scope

The proposed European cyber-security strategy focuses on ***protection***, and therefore on ***building a defensive capability***. However, a pre-requisite to the development of this defensive culture and the associated policies, organisations and tools is to understand the very nature of offensive capabilities.

Offensive capabilities enable a nation to use cyber-weapons to infiltrate and destroy assets of another nation. As such, these capabilities are not at the heart of the European

construction. However, it is interesting to have in mind the multiple examples of using cyber-weapons such as for instance those described in "Cyber War- the next threat to national security and what to do about it" [108].

These examples provide on the one hand concrete views of the interaction between cyber-attacks and real-world infrastructures, and on the other hand provide a good (and scary) insight into the fact that cyber-attacks when taken to the level of a cyber-weapon can go much further than stealing identities online.

While the public image of hackers is often one of isolated individuals, the reality is very different. For instance, in North Korea current information[108] points to four units, totalling close to 1,000 hackers trained to conduct military cyber-attacks. In July 2009[1], one of these units, Lab 110 was suspected to be behind the attack that destroyed South Korea's communication networks.

The success of worldwide conferences such as Defcon[2], Black Hat[3] and RSA[4] also provide strong indications regarding the increasing knowledge (in size and innovation) that is shared around hacking techniques, flaws in largely deployed operating systems and more. In Europe, hackers part of the Chaos Computer Club hold a conference every four years – as recently as August 2011, in Berlin. This organisation analyses both the technological aspects but also the societal impacts.

This offensive versus defensive capability analysis is also at the heart of the latest publication[110] by the Belgian committee in charge of controlling information security, which points out that we need to **build a defensive capability relying on offensive knowledge**.

Building *defensive* capabilities therefore starts with the identification and understanding of the threats, including:

- **Who** are we defending against:
    - *cyber-warriors*, whose main intent is to destroy specific capabilities (weapons, infrastructures etc) of another nation,
    - *cyber-spies* focused on accessing (usually classified) information,
    - *cyber-criminals* often accessing private information to then make a personal benefit out of its access, publication or usage,
    - *activist hackers* supporting a social, political or other cause through accessing, modifying, replacing either public or private information,
    - *lone or community hackers* more focused on demonstrating their technological innovations.

Answering this first question immediately **opens up** different approaches, and therefore different **means of intervention and of organisation**.

- **What targets** are we protecting:

[1] http://www.guardian.co.uk/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks
[2] https://www.defcon.org/
[3] http://www.blackhat.com/
[4] http://www.rsaconference.com

- government infrastructures and networks, used essentially in the civilian (and military) management of one or more nations,
- infrastructures that have been identified as critical but are mainly managed and operated by private operators,
- classified data,
- sensitive and personal individual information (according to local cultures, legislations, etc.),
- economic value of entire sectors, ranging from roads to banks, retail to manufacturing, public administration services to education, health to tourism etc,
- etc.

Answering this second question leads to the **definition of the required collaborations between the private sector and the public sector**.

- **What approaches** are we protecting against:

  Based on a *simplified* taxonomy of cyber-threats, three action modes can be defined to categorize, at a high level, different approaches, namely:

  - actions performed ***against*** the information: the goal is to modify data to provoke material flaws and physical systems operational defects, or des-information campaigns,
  - actions performed ***for*** (getting access to) information: this is about stealing and collecting strategic data,
  - actions performed ***by*** (using) information, for propaganda, training, etc.

This basic classification helps detailing the scope and opens up the full list of topics, ranging from **governance to regulations, from strategic guidance to operations and more**.

7.4. The critical challenge is speed

The strategy has to take into account the critical challenge posed by cyber-security, the **speed** at which cyber-disruptions can spread, the **outreach** they can achieve. These two elements require a corresponding *reaction speed* to counter cyber-threats, and a matching outreach of these reactions both in geographical terms (across Europe and beyond) and infrastructure terms (across infrastructures linked by networks under attacks, across control systems linked by infrastructures etc).

Delivering this level of speed combined with the required outreach can only be achieved through a **high level decisional governance** for implementation and management of a commonly agreed "vision". This governance should be backed by Member States through their operational involvement and supported by an implementation body supporting coordination of national, regional and local levels of intervention.

The governance for monitoring and respond, at national or European level, should leverage on "**real time capabilities**" adapted to the "speed challenge". These capabilities are

missing or not adequate to the evolving threats in several administrations and private organisations within Europe. Further support to develop these capabilities in key sectors with high socio-economic impact (e.g. energy, communication, transport, public administration etc.) is needed.

This approach also requires that the EU encourages a **change in attitude of the most relevant stakeholders**: data sharing should be promoted with incentives; simulations should be systematic and cross-sectoral while the process improvement should move from a "traditional" Deming cycle (Plan-Do-Check-Act) designed to drive continuous improvement, towards a more agile Boyd cycle (Observe-Orient-Decide-Act) that can quickly process information, observing and reacting to unfolding events more rapidly than incoming threats and can thereby "get inside" the threatening decision cycle and gain the advantage. Instead of pursuing perfection in European cyber-security capability, which could be legally, politically and operationally impossible, the strategy should focus towards an EU engaged in operationally facing dynamic challenges and threats from invisible opponents.

The current fragmentation of efforts across different security programmes, policies and approaches, implemented at European or at national levels as well as the **lack of integration** across domains, **do not allow for the implementation of these rapid reaction models**. And while the existing efforts at European and national levels are often complementary, they are also, in some cases, overlapping.

The reality of speed and outreach of cyber-disruptions requires that Europe delivers similar (increased) speed and outreach in its response capability.

This cannot be achieved without a more structured and coordinated approach, embodied by a central organisation that can foster more efficient operations, from fast decision to immediate reaction.

It also requires a change in attitude of the most relevant stakeholders with respect to the sharing of information, the pooling of resources etc.

7.5. Taking stock of the reality

The scope and critical challenge can only be addressed after a detailed assessment of the starting point, a continuous monitoring of the situation and defined targets in terms of expected impact and improvements.

Two important dimensions should be analysed, for which we only have partial information so far:

- the **dependence of our society and economy on cyber-space**, key elements in prioritising the actions of the strategy, in refining activities in research, innovation, uptake measures, incentives, regulations etc,
- the **(quantified) impact of cyber-attacks** which complements the dependence information by providing concrete metrics and contributing to a better balancing of resources between the different pillars of the strategy

7.5.1. Analysing the dependence

The dependence should be analysed from four different angles and with all hazards in mind.

1. *From the critical infrastructure angle,*

We need to build a clear picture of the interconnection of Critical Infrastructures with the Internet and between themselves. **Can they be isolated in case of need** and still operate in a reduced mode, providing a pre-defined level of **resilience under stress**? When the connectivity of their controlling systems to the Internet is compulsory, has this been secured enough? Recent tests in the US[108] by six different cyber-security firms were all successful in accessing the control systems of power grid controls companies; these accesses took less than one hour, and were achieved entering through the public Web sites of the operators or their intranet and, from there, reaching the control systems through internal connections. What is the situation in Europe? What tests (*vulnerability*: access of attacks to the system; or *stress*: resilience of the systems to attacks) do we need to conduct? Following the financial crisis, Europe instituted bank stress tests – it is time for Europe to build a similar approach to get an effective measure of the stress resilience and resistance capability of our critical infrastructures. Whether by malicious intent or accidental errors, connected infrastructures can be disrupted – and we need to assess the impact of these disruptions.

2. *From the sectoral angle,*

We need to understand the different sectors' dependence on cyber space, as well as the specific objectives, means and impacts of the threats to each sector. The widely publicised attack suffered by Estonia in 2007 crippled its entire administration, banking and education system for weeks. Estonia in that sense is a clear wake-up call of what could happen across Europe (and beyond) should cyber-attacks be deployed to the same effect. The recent attacks[158] on the European Institutions information systems before a European summit and on the French finance ministry before a G20 meeting further demonstrated the vulnerability of Europe to cyber-attacks. But again attacks are not the only source of disruption – human mistakes in programming, mailing etc can also create major disruptions.

Therefore, we need to move beyond analysing disruptions at the network / information level and move to a more specific sectoral specific angle, which will enable to involve communities (private and public sectors) in a defensive strategy.

3. *From the education / awareness angle,*

The education angle can be analysed from different points of view.

On the one hand, the sheer size of cyber-space with over 2 billion people connected (and this number is growing every day), has also empowered a large number of users with means that they don't always fully understand. This requires large education campaigns, better support to users of different tools and services.

On the other hand, we need to measure the effective understanding of the *impact* of disruptions on each sector, on each critical infrastructure. This angle is extremely important in that over the last decade, Europe has and is continuing to push for the end

of monopolistic and state-controlled infrastructures. In the energy distribution, for instance, this has led to a separation of operations involving the power lines (transport) from the energy management and distribution (services). It has also led to a shift from public to private operators, operating in stringent competitive conditions. Today, these **operators** have to **balance the investments** they devote to cyber-security and profitability objectives, particularly when faced with a lack of direct financial **incentives** to spend resources on cyber-security, or when not fully considering the economic impact on their businesses that can occur if their own (or connected) infrastructures are under attack. Therefore, this education / awareness angle is an important element of the strategy.

4. *From the human factor angle,*

We need to integrate the evolutions of human behaviour of the numerous users, with elements such as **increasingly connected mobile users** and interaction models through social networks also known as "social media" and how these influence cyber-disruptions.

Social media opens up a whole world of insecurity and privacy issues; it also enables an increased capacity of speed and outreach of information, both good and bad. Social media can be put to positive use during natural disasters as demonstrated by the Ushahidi [1] model, the recent disaster in Belgium in August 2011 at the Pukklepop open air music festival where the SMS network was reserved for emergency while Facebook and Twitter were used to inform friends and relatives. On the opposite side, the negative use of social media was clearly demonstrated during the recent riots in London and Rome, where it was the basis of communication to organize criminal activities across groups of people.

Therefore, analysing social networks in the context of cyber-security contributes directly to the dimensions of speed and outreach of cyber-disruptions – and can support the deployment of counter-attacks to these disruptions.

Another key element of this human factor angle is that of mobility, leading again to both positive and negative elements. On the positive side, the use of mobility and related information can help build a clearer view of crowds when facing a disaster. It can also help in localising key stakeholders who can better intervene, in coordinating rescue team etc. On the negative side, users can take advantage of the mobile capabilities to launch cyber-threats from different geographical locations while remaining connected and coordinated.

Taking stock of the reality is of major importance in measuring our current level of risks, understanding our dependencies and moving beyond post-mortem quantitative studies to build a concrete strategy.

This activity also helps in identifying areas where we do not have (enough) information and where we need to act fast to gather this

[1] www.ushahidi.com – an initiative started to support crisis management based on information exchange through mobile phones of people on the scene, rescue teams and online information support

information which is a pre-requisite to the strategy implementation.

This element also leads to important education and behavioural components, addressing the human factor that forms an inherent part of cyber-space.

7.5.2. Quantifying the impacts of cyber-attacks

The previous point focused on information that is required to better prevent, prepare, and protect. This section focuses on **quantifying the impact**, an element used to **optimise the resources deployed in the cyber-security strategy**.

This quantification is not an easy task, and different studies exist that point out global numbers and statistics.

UK based Detica / BEA Systems issued a 2011 study[150] in collaboration with the Cabinet Office of the UK government, on the impact of cyber crime on the UK economy. This study identified close to **€ 30 billion /year** lost due to cyber crime in the **UK**, with almost **80% as a cost to the private sector due to theft of intellectual property and espionage**.

Symantec released its 2011 annual report on cyber-crime, for which it interviewed 20.000 people in 24 countries. The report indicates that in **2010**, worldwide cyber crimes claimed 431 million victims, cost **$ 114 billion in direct money losses** and $ 274 billion in the time lost to cyber-crime, leading to a **total annual cost of $ 388 billion**. While this survey does **not include and distinguish neither the sectoral impacts** nor the infrastructure ones, it revealed over **one million victims a day**.

A 2010 EOS analysis of the security market evaluated the annual impact of cyber crime at about € 340 billion[1].

Another element to consider is the value of the **security solution market**, and in particular that of **cyber-security** solutions and related services (not including intelligence), an evaluation of which has been made through EOS members. At world level, this market amounts to € 10 -12 billion /year, while at **EU level** it is of the order of **€ 2,5-3 billion / year.** Taking this figure of **€ 2,5 billion** for the annual cyber-security solution market in Europe, this would **correspond to about 25.000 highly skilled jobs** (a figure rapidly increasing in recent years), considering that, as is the rule for most electronic businesses, about 50% of the market is in manpower, and that average ICT services manpower cost is somewhat lower than in other electronic sectors.

Another interesting figure, is the **market for cyber insurance** (Lloyds estimation) which is of the order of **€ 400 million /year**, i.e. 0,05% of the impact at worldwide level, or 3,3% of the cyber-security solution market. Together, these numbers provide an initial estimate of the societal impact of the cyber-security strategy on job creation.

Quantifying the impact of cyber-disruptions is a key element in optimising the resources deployed to implement the European cyber-security

[1] http://www.eos-eu.com/LinkClick.aspx?fileticket=y0rpzCaYh7o=&tabid=318

strategy as well as in creating training, education and skill strategies that support the creation of jobs and the needs of the industries active in the security markets.

7.5.3. Evaluating the drawbacks of a fragmented security market

The fragmentation of Europe does not only impact the institutional level, but also the market, where the lack of agreed security levels, of incentives for private sector operators and the diversity of security approaches in different sectors create a fragmented market.

Furthermore, contrary to the situation in the US market, and despite efforts already made through European and national R&D tools, volunteering policies and financial schemes are not sufficiently in place to fully support and speed-up the process of moving from Research to Innovation and Market implementation – while at the same time over three million **new threats** were identified in 2010 – approximately one **every 10.2 seconds** [159].

This in turn hampers investments in new products, solutions and services, as the uptake path is not supported enough nor can it be deployed at a wide enough scale.

It also leads to a ***critical dependency*** for Europe in terms of sourcing its cyber-security technology, solutions and evolutions mainly from non-European organizations, a situation that can also increase the risk of cyber-threats.

7.6. The key stakeholders

Given the ambitious scope of the strategy, the identification of the key stakeholders and of their relative positioning is an important step in its implementation.

The latest European Commission Communication[100] lists a number of stakeholders, such as EFMS, ENISA, EP3R, Commission DG's specific units (INFSO, RTD, ENTR, HOME, MOVE, ENER, DIGIT,...) etc. However, these entities (agencies, partnerships, etc.) have each been set up individually, in response to specific needs rather than through a coherent, comprehensive and complementary approach. Their mutual interactions and the way their activities contribute to improving cyber security in Europe are still in a maturing / clarification phase.

On the other hand, the effective implementation of a cyber-security strategy relies on the **willingness** of many different parties **to collaborate**, to share information in a trusted way, to dedicate time and resources, to implement governance, processes and structural changes, to educate teams and continuously monitor on-going activities etc. The monitoring and information sharing processes advocated in the EISAS roadmap, by the ISS and the Digital Agenda require that issues such as privacy, data protection, and controlled access be addressed. This is in turn will require the participation of new stakeholders.

The latest incidents also highlight the **international nature of the problem** – for instance, the 2011 theft of 12.3 million credentials including personal identities and credit card information from the Sony Play Station network involved worldwide identities, 45% from US citizens (5.6 million credentials), and close to 50% from European citizens. The Europol "2011 Organised Crime Threat Assessment" [154] report also highlights the use of the Internet to defraud victims and to orchestrate crimes – bringing a law enforcement

component into the cyber-security issue that cannot be addressed without an over-reaching coordination.

From the current analysis, the list of stakeholders includes:

At international level:

- UN / ITU / Atlantic Council
- NATO
- US-EU working group on cyber-crime and cyber-security

At EU level:

- DG-HOME (EU Internal Security Policy and applications of secure cyber solutions to border control, fight against crime and terrorism)
- DG-ENTR (research on cyber crime)
- DG-INFSO (Digital Agenda, CIIP, research on trusted solutions)
- DG-Justice (Data protection)
- Sectoral DGs (application of secure cyber-solutions to specific domains, such as transport, health, energy, etc)
- EEAS
- Cyber-crime task force (Europol, Eurojust and the European Commission)
- Council of the European Union
- European Parliament (different Committees)

At EU agencies level:

- ENISA (information network, Cyber-Europe exercises, etc)
- Europol (law enforcement, cyber-crime, ICROS – Internet Crime Reporting Online System, IFOREX (Internet & Forensic Expert Forum, etc)
- Eurojust
- Frontex (border control, information sharing network between Member States, etc)
- EDA

At national and regional levels:

- Ministries (Interior, Telecom, Industry, Defence, etc.)
- CERTs
- Member States police forces
- Regulators
- Public procurement professionals
- Regional / local administrations
- National agencies

At industry level - enablers:

- Operators of infrastructure
- IT *service* providers

- Internet service providers
- Industry providers of security and safety technologies and solutions and services
- Industry manufacturers of devices and components
- Corporate CERTs

At industry level – sectors:

- Operators of energy, financial, health, telecommunication, transport, manufacturing and supply chains infrastructures etc
- Sectoral CERTs

At academic level:

- Research centres
- Universities

At citizen level:

- Citizen associations
- Privacy, data protection related associations

Others:

- NGOs

Identifying the key stakeholders and their interoperation is another important step, whose goal is to ensure that all the considered angles (critical infrastructures, sectoral, education / awareness) are covered, that the international aspect is integrated and that the strategy implementation will not be blocked by overlooking major issues.

This again is another element where the current level of fragmentation hinders progress on cyber-security.

7.7. The importance of knowledge and skills

Cyber-security in Europe has a specific dimension versus other nations, that of having **to set up a coordinated approach** across (today) **27 Member States**. And in these Member States, many have one or more strategies on cyber-security, while at the same time academic programmes exist that train engineers and managers on the important aspects of (cyber) security.

This certainly adds a level of complexity, but it also adds a major advantage, that of having a large base of knowledge and skills available in Europe even if these are spread out and not always well identified.

Moving to the private sector, many organisations have their own department working on internal and / or external impacts of cyber-security. But in this domain also, fragmentation is evident.

Just referencing the incident in the banking industry in Belgium in July 2011, a (small) number of citizens using online banking systems were hacked during normal operations of their software. Banks initially put the blame on the clients, identifying the lack of updated

virus protection software on the clients' computers. Even though individual cyber-security awareness must be developed (just as people are not supposed to walk in the streets with wallets wide open), this approach is not fully acceptable, in a world where banks, pushing for online systems, should also incorporate concrete support (beyond defensive warnings) to ensure that online accesses operate only in sufficiently protected environments. They should also enforce secured communications along the entire processes of online banking, an element that is not always implemented. While this clearly requires banks to move beyond their initial mandate, it also shows that working in cyber-space is removing traditional sectoral barriers that cannot remain if we want (and need) to deliver trusted environments to society.

Therefore, **Europe should address the dual aspects** of:

- **building on the large knowledge and skill base** already existing across its Member States, academia and business;
- **coordinating this knowledge towards a single strategy**, that enables this knowledge to *flow between private and public sector organisations.*

Just to get a glimpse of the complexity of this aspect, Figure 1 elaborated by ENISA provides a list of the institutions that should ultimately constitute a network of collaborating CERTs[1] across Europe and internationally. And this does not take into account the private sector, the academia educational programmes, the international conferences, the cyber-crime centre envisaged by the EU Internal Security Strategy and more. This variety is probably justified by many good reasons, such as national sovereignty, specialization in the different sectors, etc., but clearly points out the urgent need for strong coordination.

Furthermore, neither does it show how to integrate hacker communities, a knowledge base that is key, both in innovation and in protection.

Knowledge and skills also drive us to two other aspects.

First, as developed in the previous section, hacking focuses first and foremost on the forced entry using ICT capabilities, but cyber-disruptions can go far beyond information right into control systems, and **the knowledge base should extend into SCADA and hardware protection**. Therefore, the extent to which CERTs also operate in protecting this domain should be clarified.

Secondly, the **cyber-security market is growing**, and as such **is a source of job creation** that should also guide the European cyber-security strategy.

Europe has a strong knowledge and skill base existing across its Member States. It also has a large number of entities contributing to the CERT activity.

Linking this knowledge base together should be at the heart of Europe's cyber-security strategy.

Ensuring that the knowledge capability extends to all hazards, hardware, SCADA protection and next generation ICT (smart grids, in car, etc) dependent systems is key in integrating critical infrastructure and mobile devices

---

[1] Computer Emergency Response Team

protection.

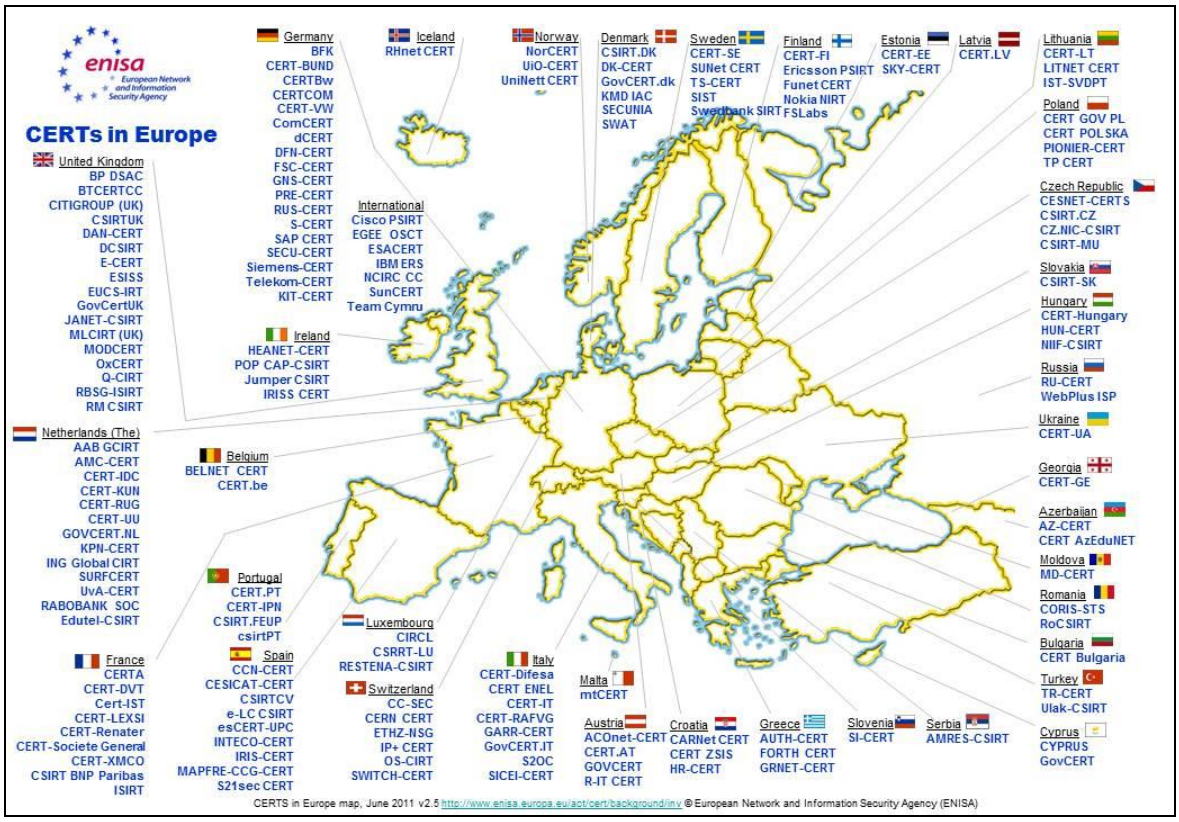

Figure 1 – CERTs across Europe (established by ENISA in 06/2011, online at http://www.enisa.europa.eu/act/cert/background/inv/files/certs-in-europe-map)

7.8. A European cyber-security coordinated structure

A European Cyber-Security Strategy has to incorporate both content and structure – ensuring that its definition includes the decisional and operational bodies without which the strategy will not be effective. It should address the full range of activities,

- Prevention
- Preparedness
- Response

EOS, representing the private cyber security sector industries and research centers) has a vetted interest in the rapid establishment of a sustainable public private cooperation on cyber security, considering the huge economic (and societal) impact of the cyber space. EOS is therefore proposing the following structure to support the implementation of these different phases:

- definition of a **European cyber-space** federating national cyber-spaces on the basis of transparent and commonly agreed rules. The responsibility of cyber-security services provision would be given to **(national) trusted cyber-security operators** whose

status, missions and regulations would be subject to a common agreement, within the limits of subsidiarity principles. Specific attention would be given to critical infrastructure operators for which a dedicated **certification policy on data integrity** could be set up to ensure a proper commonality in the level of protection across Europe.

- a **European Cyber-Security Partnership** – ECSP - **supporting the implementation of the European Cyber Security Strategy** in the prevention, preparedness and response phases. **The ECSP should not be limited**, as sometimes envisaged in the past, **to the experience of operators having suffered cyber attacks** (and their direct access to the network, when needing a fast response), but should exploit the competence of private solution and services suppliers to identify risks, evaluate vulnerabilities and suggest adequate solutions across all economic sectors of our society, from transport to power distribution, from education to infrastructure, from health to finance etc.
- a **European Cyber-Security Coordinator** empowered through a fast decision process to find agreement on the information and coordination means to **help securing cyber-space across Europe**. The coordinator should also play a key role in representing Europe's cyber-security policies and actions on the international scene, linking to other non-European strategies, a function modelled on the existing EU counter-terrorism coordinator. Today, different reports [101, 114] are also calling for this coordinator, albeit with different views on where, in the European Institutions, should such a coordinator be localised. It is not the role of EOS to judge on one or another solution, yet, for the sake of better supporting EU economic interests, we strongly advocate a model through which the EU cyber-security coordinator dialogues directly with Member States, the European Commission and to the Council of the EU supported by a decisional process that ensure effective and fast implementations.
- a **European Cyber-Security Centre** delivering the required level of operational coordination, ensuring that the local and national structures inter-operate through pre-defined and validated processes. This centre should operate in collaboration with the various European agencies involved in cyber-security, ranging from Europol to ENISA and Frontex, etc., and with national cyber-security centres.
- the creation (where needed) also with the support of EU funding, of **national / local cyber security centers** to fill-in capability gaps, monitoring the national / local cyber space and establish links / cooperation with the European cyber-security coordination center.

In calling for these components of an integrated strategy, EOS aims to **highlight the need and to propose specific roles**. However, with the upcoming cyber-crime center envisaged by the ISS and to be operated by Europol (which would be dedicated at building operational and analytical capacity for investigations and cooperation with international partners in the cyber crime domain), **finding the best localisation** and link for these different components is not an obvious task.

A stepwise approach to localising and scoping the comprehensive mandates and mechanisms for both the coordinator and the centre might be the best solution, with a first phase operated by a small group of experts delineating the activities across all dimensions

and processes – leading in a second phase to the setting up of the EU Centre and the Coordinator, whose best positioning might end up as inter-institutional bodies.

Today, we are calling upon the European Commission to implement the governance and organisation to federate such a strategy supported by a clear identification of areas of work and supporting structure.

Whether this structure aligns to an existing European instrument or is established as a new approach, the main focus is the urgency of getting this organisation to work.

The following figure provides a graphical overview of a proposed structure – the exact mandates and inter-relations require further analysis through the previously described two-step definition process.

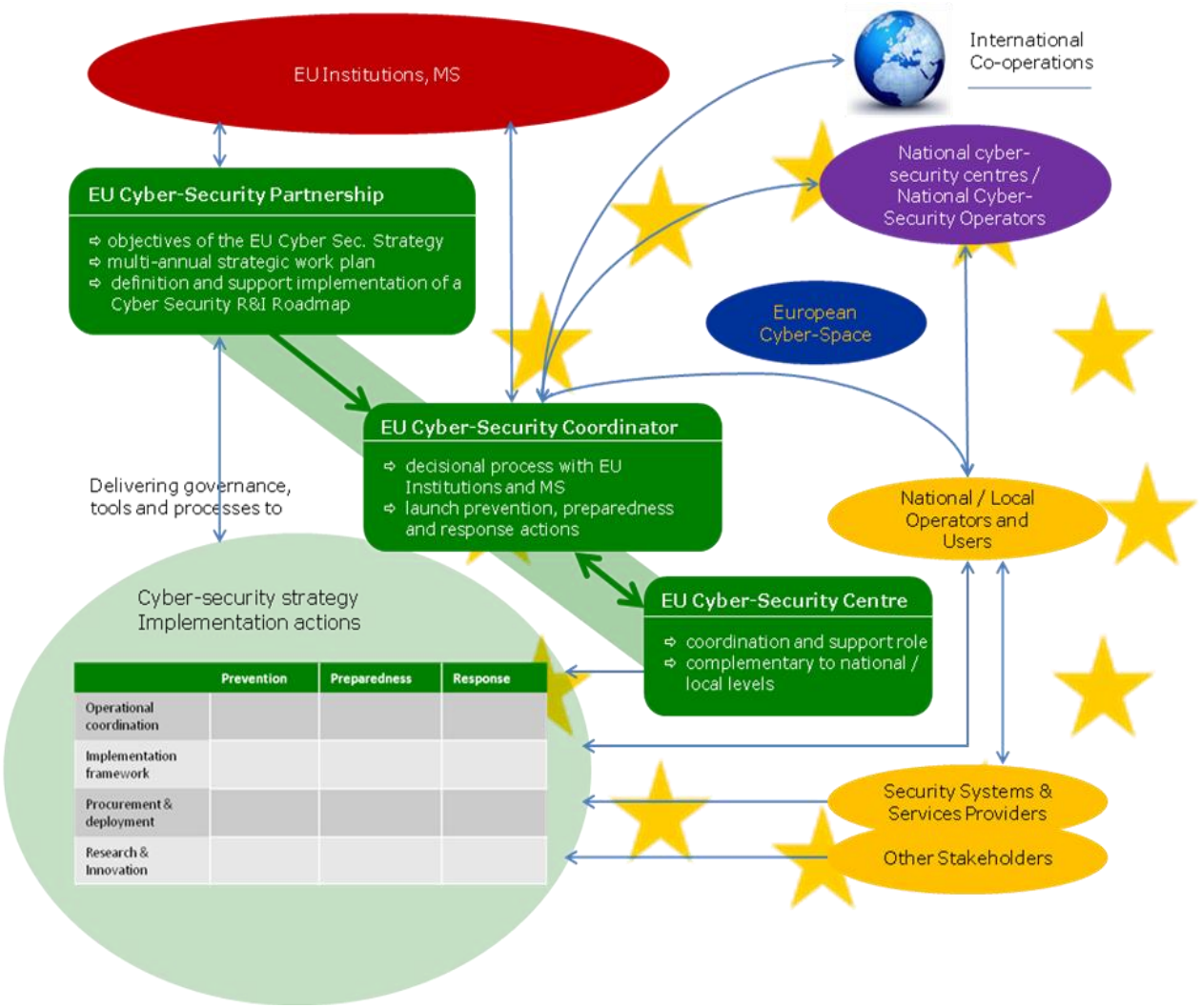

Figure 2 – proposed structure

7.8.1. Cyber Security European Partnership and Governance

Without being prescriptive, a possible configuration for the governance of a European Cyber-Security Partnership - ECSP – with participation of public and private stakeholders, could be a "partnership" (not necessarily a PPP in its formal definition), derived from existing EU instruments to provide all the support needed for the implementation and managempent of the commonly defined "vision" of the EU cyber security policy.

The **general objectives of this "partnership**", aligning and pooling public (European and national) and private resources, include:

- bridge the gap between law-enforcement approaches, economic sectoral impacts and technology focused efforts;
- build consensus and critical mass with participation of key (public & private) stakeholders in the cyber space to ensure the scale and scope required, associating national security operators in charge of providing cyber-security services at national and/or sectoral levels;
- contribute to the development of a joint vision, objectives and strategic agenda setting for the efficient deployment of a European Cyber Security Strategy;
- contribute to programming approach, pooling forces and focussing resources to achieve agreed objectives;
- provide a framework bringing together stakeholders across sectors and countries to integrate or initiate supply and demand side measures across the whole life cycle;
- foster standardized information exchanges and mutually recognized certification rules and bodies;
- encourage pan-EU exercises building upon existing endeavours and structures (ENISA);
- speed up innovations addressing major cyber security challenges (be they political, societal or economic) as well as their effective implementation and use;

The **governance of the ECSP** could be constituted by two level bodies (at coordination and at operational level).

At coordination level, the ECSP could be led by a representative Board chaired by the European Commission or Commissioners with lead portfolio responsibility for the policy area or areas concerned. From the EOS point of view, this would be an important feature, as it will clearly identify a guide of a European cyber security strategy, politically supporting economic initiatives in this domain.

The Board would be composed of Member States representatives, members of the EU Parliament, the Cyber Security Coordinator, high representatives from the private sectors (industry leaders – operators and suppliers, researchers and other key stakeholders – possibly not only in a role of Advisors as trust and commitment of these private sector stakeholders should be clearly established).

At the operational level, the ECSP could leverage upon:

- the work of the EP3R for the detailed definition of policy, governance guidelines as well as strategic objectives;
- the activity of a suitable "structured partnership" for all the detailed definition and implementation of Research & Innovation activities and tools;

- the law enforcement and European cyber-crime alert system announced by Europol in August 2011, and similar information and monitoring networks currently being set up across different activities;
- the ENISA activities in direct relation with cyber-security;
- etc.

Key private stakeholders for the ECSP, would come not only from telecom operators or software manufacturers but also from operators and users of other kind of infrastructure and services as well as component, device, system manufacturers and cyber technology developers.

The initialization of the ECSP work could be the definition (by the coordination level bodies) and the agreement by the Board of the high level objectives of the European Cyber-Security Strategy, including (but not limited to) definition of target sectors, legal and example based definitions of threats (supporting the implementation of existing and upcoming directives and revisions), attacks, etc. It would also include the harmonization of corresponding law enforcement tools, respective roles and duties of MS, EU institutions, national authorities and private stakeholders (CIIP owners, operators and users), global level of societal and economic continuity to be achieved, etc.

The ECSP's would then draw up at operational level, building upon the high level agreement, under the Board authority and subject to its approval, a ***multi-annual strategic work plan***, covering the complete working areas from operational implementation to research & innovation and uptake.

A suitable structured operational partnership could in parallel **define and support the implementation of a Roadmap for Research & Innovation for the Trust & Security** domain developing the needed tools, procedures and, when needed, architectures, for the most efficient implementation of the European Cyber Security Strategy.

7.8.2. The European Cyber-Security Coordinator - CSC

While this aspect was introduced in the 2010 EOS white paper, we want to reinforce the importance of this coordinator. EOS welcomes the European Parliament report[101] by the SEDE committee leading to the same conclusion.

The coordinator could have a **double perspective: internal** (coordination towards European stakeholders, taking care of the political link with MS, working with the European Commission and the Council of the EU, and supervising the activities of the operational arm – see next section) **and external** (international as well as civil and military defence dimensions).

The coordinator would have a clear leadership during the definition phase of the high level objectives in terms of proposals, MS positions harmonization and voicing, preparation of debates and negotiations. He would also be responsible of guaranteeing that these objectives are well understood by the operational level of the European Cyber-Security Partnership body in charge of the preparation of the working plan.

From the EOS point of view, the European Cyber-Security Coordinator would have a key role as he/she would facilitate the link between the Board, the European Cyber-Security Centre (see next) and the other public and private actors to support a decision process that, today, cannot be implemented through the many existing initiatives, bodies and policies. The European Cyber-Security Coordinator will leverage on experts from different EC DGs

and Agencies as well as, when needed on experts from the private sectors participating at the ECSP.

7.8.3. The operational arm of the European Cyber-Security Partnership: the European Cyber-Security Centre (CSCC)

To achieve the required speed at the level of implementation, the envisaged structure would need an ***implementation authority***, taking the responsibility for the deployment of the strategic work plan (approved by the Board).

While the CSCC will coordinate with the MS and other EU institutions (and when needed with the other members of the Board) the actions to be taken, the Cyber Security Center will be in charge of the *operational execution* of these actions in close cooperation with MS / local cyber security centers and national authorities under the supervision of the Cyber Security Coordinator.

Indeed, this implementation authority, proposed as the ***European Cyber-Security Centre***, should be THE single, **operational coordinating force** supporting the implementation and orchestration of rapid reactions and joint operations across MS (and internationally, when needed) to cyber-threats and attacks.

It should not supersede local structures, on the contrary fostering and supporting the collaboration mechanisms between structures.

Modelled on the Frontex model in terms of joint operations, the cyber-security centre would on the one hand implement the required exchange models and networks between cyber-security stakeholders –and on the other create joint operations similarly to those operated by Frontex with Member States.

Besides **implementing fast reaction operations**, the European Cyber Security Center would also play an operational role by supporting the implementation of the EU Cyber Security Strategy defined by the ECSP.

From the EOS point of view, the creation of such a European Cyber Security Center would not only help linking operational initiatives at MS level, but also strengthen cooperation with the private sector, both operators and suppliers of cyber security solutions and services.

Just as the ECSP organization should build upon existing initiatives (such as EP3R, EFMS, ad hoc meetings between MS for the preparation of cyber-exercises), the European Cyber-Security Center should obviously be defined and organised taking into account existing or future operational bodies (ENISA, Europol, cyber-crime center, EU-Cert etc).The idea again is not to duplicate or create new structures (except when needed), but to improve / facilitate integration and coordination.

7.8.4. Financial support for the European Cyber-Security Partnership for the creation of a common and adequate level of preparedness, prevention and response across Europe

All stakeholders involved in the ECSP will be expected to contribute with specific resources. The Commission will seek to leverage the EU budget to provide funding.

At EC funding level (contribution with EC funds), the ECSP would not be a new funding programme. On the contrary, its role is to streamline and focus existing resources and funding efforts, from existing programmes e.g. Framework Programme research funding (in the future "Horizon 2020" including also the present CIP PSP ICT), DG HOME CIPS and ISEC programmes in the future Internal Security Fund, Regional & Cohesion Funds, etc.

The private sector (security suppliers) would contribute with their own resources and expertise to the development of innovative solutions.

At global investment level, the partnership will require investment from the various members of the partnership (also envisaging support from the EIB), including the private operators, to implement the operational response force, to ensure the training network etc.

Beyond considering funding of EU level coordination structures and actions, a comprehensive assessment should be made of "weak links and gaps" at MS and local level. **Proposals should be made – along with adequate funds - to help Member States lagging behind in terms of real time cyber-security capabilities to implement the proper measures (national cyber security centers, training, etc.).**

7.9. The areas of work

Moving from structure to content, the next step to define the European Cyber-Security Strategy focuses on the three phases from prevention, preparedness and response.

However, this level of granularity is not sufficient to address the **critical challenge of speed**. Therefore, we have identified, for each phase, four areas of work:

- Operational Coordination
- Implementation Framework
- Procurement & Deployment
- Research & Innovation

and detailed below the contribution of each area to the speed dimension.

	Contributing to the speed dimension through
Operational Coordination	*Processes and governance to **share knowledge**, **monitor risks and threats** and enable **rapid reactions to cyber-attacks***
Implementation Framework	*Comprehensive framework to support the processes and governance and to ensure **rapid strategy decisions** to emerging threats and evolving context*
Procurement and Deployment	*Optimise the coherent use of funds and **speed up uptake** and impact through collaboration*
Research and Innovation	*Implement **the complete lifecycle** from research to deployment and **speed up uptake** through shorter innovation cycles*

Table 1 – how the European Cyber-Security Strategy contributes to the critical challenge of speed

The four areas of work are articulated to deliver:

- at the **decisional, implementation and rapid reaction levels**, the complete path from threat detection to coordinated actions;

- at the **supporting technologies and solutions dimensions**, focused resources towards clear common objectives from research to innovation, establishing a complete cycle from research to innovation and deployment, supported by procurement rules

Moreover, taking into account that the definition of the cyber-security strategy on the one hand, and the set-up of a EU Cyber-Security Centre on the other hand might imply significant preliminary discussions, and time being of the essence, "quick wins" should be implemented in each area, to give credibility to the overall approach, demonstrate its feasibility, and respond to the more urgent challenges.

Such **short-term initiatives** could encompass (among others):

- strong promotion of the **identification of a specific funding** within structural funds to finance the **setup of national cyber-security centers** (where needed);
- active support to the **inclusion of CIIP in the revision of the 2008 EU CIP directive**, along with a reinforcement of the prevention and preparedness measures to be taken for identified European critical information infrastructures;
- set-up of an **operational EU Cyber-Security Center** limited to the monitoring of the assets on which the EU has a legal outreach (Commission, Council and Parliament information systems and networks), for instance by extending the mandate of an existing agency;
- creation of a **structured partnership for defining the R&I Roadmap for Trust & Security**, also considering **privacy and data protection issues;**
- creation of a **European Cyber-Security Awareness Month**, an initiative that already exists in the US and whose aim is to making the users aware of the key roles they play in cyber-space and its security. In making it more specific to Europe, the month could, for instance, be replaced by periodic daily events across each of the 27 Member States.

The following pages detail, for each of the four areas, the set of proposed activities, organised around the EU Cyber-Security Partnership, EU Cyber-Security Coordinator and the EU Cyber Security Centre.

7.9.1. Operational coordination

Operational coordination				
		Prevention	*Preparedness*	*Response*
	***European Cyber-Security Strategy***	**EU Cyber-Security Partnership**: *federating* stakeholders around a single governance structure ◆ Sector per sector analysis and monitoring of risks level (*at connectivity level, at control systems level and at educational level*) ◆ Trusted governance model for secure information exchange and sharing	**EU Cyber-Security Partnership**: defining and piloting joint operational processes within a well defined governance ◆ Intelligence collaboration: private sector providing information to the cyber security center which will integrating intelligence into the overall operational process under supervision of the CS coordinator, reporting to MS ◆ Civil / military collaboration: sensitive to tackle in a such partnership, but sharing of some civilian experience could be envisaged to increase defensive capabilities	**EU Cyber-Security Coordinator** coordinating with MS and EU Institutions decision for use of rapid reaction capabilities **EU Cyber-Security Centre** implementing a rapid reaction *operational* capability, coordinating and cooperating with and between the MS/local structures ◆ Intelligence collaboration: integration of intelligence capabilities at operational level and law enforcement under supervision of the CSC ◆ International cooperation: joint rapid reaction operational capabilities with other (non-EU) bodies

7.9.2. Implementation framework

Implementation framework				
		Prevention	*Preparedness*	*Response*
	***European Cyber-Security Strategy***	**EU Cyber-Security Partnership**: scoping the metrics, voluntary and industry-led certification and standardisation at ICT and sectoral levels. Designing education programmes. ◆ Metrics definition for quantified impact measurements (including sectoral specificities) ◆ EU / international standardisation ◆ Certification programme for: solutions, processes, professionals ◆ Secure manufacturing capabilities (microprocessor, gateways, mobile devices, systems etc) ◆ Secure design process ◆ EU risk management methodologies for cyber threats ◆ Education / awareness programme ◆ Monitoring, identification / participation to hackers "communities", events, online forums etc ◆ Cyber-Security Awareness Month	**EU Cyber-Security Partnership**: organised knowledge and skill sharing and pooling environment ◆ Law-enforcement prosecution process ◆ Convention on cybercrime ratification and extension ◆ Liability regulation for solution suppliers and operators ◆ CERTs and EU-CERT implementation based on operational governance model ◆ Sector / CERTs network collaboration model ◆ Monitoring cyber-threats (at infrastructure level, per sector level) ◆ Code of conduct elaboration ◆ Law enforcement elaboration (including outreach, international, non-localised origin of cyber-attacks – linking to prioritised impacts) ◆ Introducing an "obligation to inform of incident" approach to increase level of awareness, sharing and risk evaluation ◆ Elaboration of cyber-security incident contingency and response plans in a "security & privacy by design" approach	**EU Cyber-Security Centre** delivering quantified impact analysis of cyber threats / crime / attacks (fed back into prevention and preparedness) ◆ Support to EUROPOL for forensic analysis processes ◆ Support to MS authorities and EUROPOL for implementation of law-enforcement prosecution process

7.9.3. Procurement and deployment

Procurement and deployment				
		Prevention	*Preparedness*	*Response*
	***European Cyber-Security Strategy***	**EU Cyber-Security Partnership**: defining target capabilities at EU / MS level ◆ Detailing pre-commercial procurement process in support of cyber-security certified solutions ◆ Monitoring centres ◆ Securing key nodes / protocols, e.g. BGP… ◆ Defining target capabilities at EU / MS level (leveraging on EU funds: cohesion, regional funds …) ◆ Integration with existing solutions ◆ Protection tools	**EU Cyber-Security Partnership**: structuring the *integration* of capabilities at EU / MS level, the leveraging on EU funds (cohesion, regional, research, innovation funds …) ◆ Defining a comprehensive incentives model to foster private sectors participation and investment ◆ Structuring participation of stakeholders to EU and international cyber-attacks exercises ◆ Supporting sectoral / infrastructure specific cyber-attacks exercises	**EU Cyber-Security Centre** deploying joint defensive capabilities ◆ Federation of the EU / international monitoring capabilities ◆ Participation to /organisation of sectoral level exercises (complementary to ICT network level exercises)

7.9.4. Research and Innovation

Research and Innovation				
		Prevention	*Preparedness*	*Response*
	***European Cyber-Security Strategy***	**EU Cyber-Security Partnership** ◆ Balance between short, mid and long-term R&I needs ◆ Innovation process tailored to the cyber-security ◆ Needs definition (trust, protection, sectoral needs) ◆ Procedures and secure / trusted tools for data and intelligence sharing: EU Model for Data and Information Sharing	**EU Cyber-Security Partnership** ◆ Best Practices ◆ Cyber resilience of key infrastructures and services based on homogeneous architecture frameworks (secure open standards) ◆ Development and pre-commercial procurement / Procurement Driven Innovation (pilot projects) to build local competencies and capacities to face cyber attacks ◆ Integrate research results in pan-European exercises (such as Cyber Europe)	**EU Cyber-Security Centre** participating to R&I projects, pilots and innovation uptake processes ◆ Providing requirements and validation as input to the R&I and innovation programmes ◆ Updated timetable and priorities for cyber-security needs ◆ Updated cyber-threats processes information input to the R&I programmes

8. Conclusion and recommendations

In this 2011 edition of the EOS ICT / cyber-security working group publication, EOS is calling on Europe to develop an **ambitious, extensive and integrated strategy for securing the cyber-space**.

The evolution over the last months in cyber-disruptions and cyber-threats has been extensive, and their impact has increasingly moved from information and data to physical infrastructures – transport, energy, logistics, banks etc - that form the backbone of our world. The reality today is that the means to inflict cyber-disruptions, whether through unintentional error or malicious intent, remain fairly small versus the enormous impact they may inflict to our economies, citizens and societies.

Cyber-space introduces specific dimensions that pose critical challenges, including the ***speed*** and ***reach*** with which cyber-attacks can spread, and which require **at least the corresponding speed and reach** in **prevention** and **response** capabilities. Moreover, advanced capabilities enabling efficient cyber-security risk management are needed in order to manage the required cyber-security measures at strategic, tactical, and operational levels.

These critical challenges cannot be met with the existing and fragmented approach, and the cyber-security strategy should be organised around two major dimensions:

- the *federation* of the different (and numerous) stakeholders
- the *consolidation* of the different initiatives, at policy, governance, innovation and operational levels

The recognition by the European Parliament of the importance of a Cyber-Security Coordinator is a very important step forward. The creation of the EU-US working group is another equally important step forward. The progressive ratification of the Cyber-Crime Convention is a positive evolution as well as the actions envisaged by the Digital Agenda and the EU Internal Security Strategy. The envisaged introduction of CIIP in the frame of the EU CIP Directive would also mark a step forward in the protection of the cyber space. The activities of ENISA and Europol constitute key contributions. But while individually each of these activities is important, they do not (yet) form an integrated approach.

Europe has to move far beyond this fragmentation not only to **define** but also to **implement**, with all stakeholders on board, a concerted and effective cyber-security strategy with clear paths at national, European and international levels.

It has to:

- incorporate in this strategy the many institutions, agencies, CERTs etc. active around Europe;
- integrate the knowledge base and skills that exist across Europe;
- entice Member States to bring their sometimes very advanced national strategies forward to set up an effective European one;
- to establish operational links with the private sector, in their roles as operators, innovators and solution suppliers;
- develop incentives and support programmes to encourage private operators' investments in securing critical infrastructures;

- ensure the **complete coverage of the strategy**, in terms of **speed, reach, prevention** and **real time reaction capabilities** that cannot be achieved through fragmented efforts.

Through this white paper, EOS is therefore issuing the following recommendations, detailed in section 7, to:

1. **define a comprehensive European Cyber-Security Strategy, including also the introduction of a European approach to CIIP into the revised EU CIP Directive,** leveraging on the ongoing work of EP3R, ENISA, Europol etc. **This European cyber security strategy should be wider than an "Internet security strategy"**;
2. define a **European cyber-space** federating national cyber-spaces where cyber-security services are assured by **(national) trusted cyber-security operators** and where critical infrastructure operators follows a dedicated **certification policy on data integrity**;
3. **implement the European Cyber-Security Strategy** through the creation of a European Cyber Security Partnership**.** Key stakeholders from the private sector for this partnership are not only telecom operators or software manufacturers but also operators and users of other kind of infrastructure and services as well as component, device, system manufacturers and cyber technology developers;
4. **appoint** a European Cyber-Security Coordinator to coordinate with MS the decisions for implementation of actions to face cyber threats and of the strategy;
5. **establish an operational European coordination center for cyber security (not only cyber crime), either via the creation of a "European Cyber-Security Centre" or via extending the mandate of an existing EU Agency, to coordinate** the preparedness, prevention and response to cyber-disruption by **complementing, when needed,** the **local levels of response** by an EU coordination level;
6. create (where needed) with the support of EU funding, **national / local cyber security centers** to fill-in capability gaps, monitoring the national / local cyber space and establish link / cooperation with the European Cyber-Security Center, **bringing EU MS to a common level** of preparedness, prevention and, possibly, response.

EOS, representing organisations active in the field of security, is ready to contribute to this strategy, at definition, governance and implementation levels. The fact that today, 38 different industries and research centers across 12 Member States, members of EOS, recognise the need to move beyond their own competitive world to dedicate resources to this task is yet another indication of the urgency of the situation – and an important step forward in the willingness of industry to contribute to this step.

For this reason, it is our intention to constitute a Task Force composed by experts from EOS Members working under an independent EOS banner to deliver advice and support to EU Institutions and, when needed, at MS / local level for the definition and implementation of a European Cyber-Security Strategy.

9. Acronyms

CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CSC	European Cyber-Security Coordinator
CSCC	European Cyber-Security Centre
ECSP	European Cyber-Security Partnership
EISAS	European Information Sharing and Alert System
EFMS	European Forum of Member States
ENISA	European Network and Information Security Agency
FISHA	a Framework for Information Sharing and Alertness (EU Project)
NSIE	Network Security Information Exchange

10. References

Please note that to remain consistent throughout our references, EOS ICT white papers include a unique numbering across the different issues, starting with the 2010 edition. Therefore, the 2010 edition uses references numbered from 1 to 99, the 2011 edition uses references from 100 to 199.

10.1. Policy & strategies

[100] 31/3/2011 - COM(2011) 163 on Critical Information Infrastructure Protection - 'Achievements and next steps: towards global cyber-security' – communication by the European Commission

[101] 15/4/2011 – Cyber-security and cyber power: concepts, conditions and capabilities for cooperation for action within the EU (study commissioned by the SEDE sub-committee – European Parliament)

[102] 27/5/2011 – European Council conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security"

[103] 01/05/2011 – Ensuring Hardware cyber-security, by the Brookings Institute

[104] 01/07/2011 – Strategic Cyber Security – NATO Cooperative Cyber Defence Centre of Excellence

[105] 12/08/2011 – Conflicting Policy Presumptions about Cybersecurity – Atlantic Council

[106] 01/09/2009 – Security and Resilience of Information and Communication Technology Networks for the Protection of Critical Infrastructures – EOS white paper by the ICT Working Group

[107] 01/09/2010 – Towards a concerted EU approach to Cyber Security – EOS white paper by the ICT Working Group

[108] 20/04/2010 – Cyber War- the next threat to national security and what to do about it – Richard A. Clark (Harper Collins - ISBN-13: 978-0061962233)

[109] 15/06/2011 – CYBERATTACKS – A new threat to EU´s security – Presentation by DG-Home

[110] 20/08/2011 – "Conclusions et recommendations de l'enquête sur la manière dont les services belges de renseignement envisagent la nécessité de protéger les systems d'information contre des interceptions et cyberattaques d'origine étrangère" online at http://www.comiteri.be/images/pdf/eigen_publicaties/rapport_181_%20fr.pdf

[111] 10/2010 – "A strong Britain in an Age of Uncertainty: The National security strategy"

[112] 02/2011 – The EISAS roadmap – published by ENISA at http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap/at_download/fullReport

[113] 05/2011 – "Fighting spam to build trust" – China US bilateral on cybersecurity online at http://www.ewi.info/system/files/reports/China-US-Fighting-Spam.pdf

[114] 02/2009 – "Cyber-security and politically, socially and religiously motivated cyber attacks" – http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

10.2. Quantitative / cyber threats information

[150] 01/03/2011 – The Cost of Cyber Crime – a Detica (EOS partner) report in partnership with the UK office of cyber-security and information assurance in the Cabinet Office

[151] 07/03/2011 – Botnets: Detection, Measurement, Disinfection & Defence - ENISA

[152] 02/08/2011 – Second Annual Cost of Cyber Crime Study – Benchmark study of US Companies - Ponemon Institute

[153] 25/07/2011 – Cyber was has begun – Bloomberg Business Week

[154] 27/04/2011 – 2011 Organised Crime Threat Assessment report by Europol (OCTA 2011)

[155] 24/09/2010 – Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes? – CBS News article – online at http://www.cbsnews.com/8301-501465_162-20017507-501465.html

[156] 24/08/2008 – Secret Geek A-Team Hacks Back, Defends Worldwide Web Wired.Com article online at http://www.wired.com/techbiz/people/magazine/16-12/ff_kaminsky?currentPage=all

[157] Internet usage statistics- updated on 31/3/2011 at http://www.internetworldstats.com/stats.htm

[158] 23/03/2011 - "Serious cyber attacks on EU before summit" at http://www.bbc.co.uk/news/world-europe-12840941

[159] 02/2011 - "2010 saw a new threat every 10 seconds; Zero-day viruses become more and more commonplace, according to Network Box" at http://www.network-box.com/press_2011_02_09

[160] 09/2011 - "Norton 2011 cyber crime report" at http://www.symantec.com/content/en/us/home_homeoffice/html/ncr/
Press release at http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

[161] 11/2010 - "Dutch police shut down Bredolab botnet" at http://www.zdnet.com/blog/security/dutch-police-shut-down-bredolab-botnet/7573

[162] 09/2011 - "Hackers steal security certificates, force Dutch company to bankruptcy" at http://www.moneycontrol.com/news/technology/hackers-steal-security-certificates-force-dutch-company-to-bankruptcy_588700.html

[163] 01/2009 - "Pirelli joins forces with Magneti Marelli and Brembo on new "Cyber Tire"" at http://www.motorauthority.com/news/1023007_pirelli-joins-forces-with-magneti-marelli-and-brembo-on-new-cyber-tire

[164] 03/2011 - "Taking Control of Cars From Afar" published in MIT Technology Review – available online at http://www.technologyreview.com/computing/35094/?mod=related

[165] 01/2011 - "Internet facilitated organised crime" – a Europol report available at https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf (public version)

11. Annex – 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 38 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 THIS DRAFT DOCUMENT
Reactions 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 / Cyber Security 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**
ATOS	Aljosa	Pasic	
BAE Systems / Detica	Nefyn	Jones	
BAE Systems / Detica	Ben	Rendle	
CASSIDIAN	Sébastien	Héon	
CASSIDIAN	Robert	Havas	
CEA	Alain	Merle	
ENGINEERING	Dario	Avallone	WG Chairman
FOI	Christian	Carling	
HAI	Evangelos	Ladis	
IBM	Corinna	Schulze	WG Vice-Chair
IBM	Martin	Borrett	
IBM	Peter	Stremus	
Raytheon	Vincent	Blake	
Rayteon	Jeff	Rogers	
SAAB	Lars	Jërnbacker	
Selex Sistemi Integrati	Marco	Donfrancesco	WG Vice-Chair
Selex Sistemi Integrati	Leonardo	Fiocchetti	
Thales	Yves	Lagoude	
TNO	Robin	de Haas	
Vitec	Jean	Visconte	
EOS	Sophie	Batas	EOS Team WG Coordinator
EOS	Luigi	Rebuffi	EOS CEO WG Supervision