EUROPEAN
COMMISSION

HIGH REPRESENTATIVE OF THE
EUROPEAN UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

# JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

## Cybersecurity Strategy of the European Union:

## An Open, Safe and Secure Cyberspace

**JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS**

**Cybersecurity Strategy of the European Union:**

**An Open, Safe and Secure Cyberspace**

## 1. INTRODUCTION

### 1.1. Context

Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies - most strikingly during the Arab Spring.

For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role.

Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems.

By completing the Digital Single Market, Europe could boost its GDP by almost €500 billion a year[1]; an average of €1000 per person. For new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication[2], citizens will need trust and confidence. Unfortunately, a 2012 Eurobarometer survey[3] showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases. An overwhelming majority also said they avoid disclosing personal information

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] For example, plants embedded with sensors to communicate to the sprinkler system when it is time for them to be watered.

[3] 2012 Special Eurobarometer 390 on Cybersecurity

online because of security concerns. Across the EU, more than one in ten Internet users has already become victim of online fraud.

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity[4] incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

The EU economy is already affected by cybercrime[5] activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.

In countries outside the EU, governments may also misuse cyberspace for surveillance and control over their own citizens. The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online.

All these factors explain why governments across the world have started to develop cyber-security strategies and to consider cyberspace as an increasingly important international issue. The time has come for the EU to step up its actions in this area. This proposal for a Cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.

### 1.2. Principles for cybersecurity

The borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent. This strategy clarifies the principles that should guide cybersecurity policy in the EU and internationally.

**The EU's core values apply as much in the digital as in the physical world**

The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain.

---

4 Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

5 Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).

**Protecting fundamental rights, freedom of expression, personal data and privacy**

Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field.

**Access for all**

Limited or no access to the Internet and digital illiteracy constitute a disadvantage to citizens, given how much the digital world pervades activity within society. Everyone should be able to access the Internet and to an unhindered flow of information. The Internet's integrity and security must be guaranteed to allow safe access for all.

**Democratic and efficient multi-stakeholder governance**

The digital world is not controlled by a single entity. There are currently several stakeholders, of which many are commercial and non-governmental entities, involved in the day-to-day management of Internet resources, protocols and standards and in the future development of the Internet. The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach[6].

**A shared responsibility to ensure security**

The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities which need to be properly defined, thoroughly analysed, remedied or reduced. All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity.

## 2. STRATEGIC PRIORITIES AND ACTIONS

The EU should safeguard an online environment providing the highest possible freedom and security for the benefit of everyone. While acknowledging that it is predominantly the task of Member States to deal with security challenges in cyberspace, this strategy proposes specific actions that can enhance the EU's overall performance. These actions are both short and long term, they include a variety of policy tools[7] and involve different types of actors, be it the EU institutions, Member States or industry.

The EU vision presented in this strategy is articulated in five strategic priorities, which address the challenges highlighted above:

- Achieving cyber resilience
- Drastically reducing cybercrime

[6] See also COM(2009) 277, Communication from the Commission to the European Parliament and the Council on "Internet Governance: the next steps"

[7] The actions related to information sharing, when personal data is at stake, should be compliant with EU data protection law.

- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

### 2.1. Achieving cyber resilience

To promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and cooperate effectively. Building on the positive results achieved via the activities carried out to date[8] further EU action can help in particular to counter cyber risks and threats having a cross-border dimension, and contribute to a coordinated response in emergency situations. This will strongly support the good functioning of the internal market and boost the internal security of the EU.

Europe will remain vulnerable without a substantial effort to enhance public and private capacities, resources and processes to prevent, detect and handle cyber security incidents. This is why the Commission has developed a policy on Network and Information Security (NIS)[9]. The **European Network and Information Security Agency ENISA** was established in 2004[10] and a new Regulation to strengthen ENISA and modernise its mandate is being negotiated by Council and Parliament[11]. In addition, the Framework Directive for electronic communications[12] requires providers of electronic communications to appropriately manage the risks to their networks and to report significant security breaches. Also, the EU data protection legislation[13] requires data controllers to ensure data protection requirements and safeguards, including measures related to security, and in the field of publicly available e-communication services, data controllers have to notify incidents involving a breach of personal data to the competent national authorities.

Despite progress based on voluntary commitments, there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders, and in terms of private sector involvement and preparedness:. This strategy is accompanied by a proposal for **legislation** to notably:

- establish common minimum requirements for NIS at national level which would oblige Member States to: designate national competent authorities for NIS; set up a well-functioning CERT; and adopt a national NIS strategy and a national NIS cooperation plan. Capacity building and coordination also concern the EU institutions: a Computer Emergency Response Team responsible for the security of the IT systems of the EU institutions, agencies and bodies ("CERT-EU") was permanently established in 2012.

---

8 See references in this Communication as well as in the Commission Staff Working Document Impact Assessment accompanying the Commission proposal for a Directive on network and information security, in particular sections 4.1.4, 5.2, Annex 2, Annex 6, Annex 8,

9 In 2001, the Commission adopted a Communication on "Network and Information Security: Proposal for A European Policy Approach" (COM(2001)298); in 2006, it adopted a Strategy for a Secure Information Society (COM(2006)251). Since 2009, the Commission has also adopted an Action Plan and a Communication on Critical Information Infrastructure Protection (CIIP) (COM(2009)149, endorsed by Council Resolution 2009/C 321/01; and COM(2011)163, endorsed by Council Conclusions 10299/11).

10 Regulation (EC) No 460/2004

11 COM(2010)521. The actions proposed in this Strategy do not entail amending the existing or future mandate of ENISA.

12 Article 13a&b of Directive 2002/21/EC

13 Article 17 of Directive 95/46/EC; Article 4 of Directive 2002/58/EC

- set up coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national NIS competent authorities. National NIS competent authorities will be asked to ensure appropriate EU-wide cooperation, notably on the basis of a Union NIS cooperation plan, designed to respond to cyber incidents with cross-border dimension. This cooperation will also build upon the progress made in the context of the "European Forum for Member States (EFMS)"[14], which has held productive discussions and exchanges on NIS public policy and can be integrated in the cooperation mechanism once in place.
- improve preparedness and engagement of the private sector. Since the large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cybersecurity is crucial. The private sector should develop, at technical level, its own cyber resilience capacities and share best practices across sectors. The tools developed by industry to respond to incidents, identify causes and conduct forensic investigations should also benefit the public sector.

However, private actors still lack effective incentives to provide reliable data on the existence or impact of NIS incidents, to embrace a risk management culture or to invest in security solutions. The proposed legislation therefore aims at making sure that players in a number of key areas (namely energy, transport, banking, stock exchanges, and enablers of key Internet services, as well as public administrations) assess the cybersecurity risks they face, ensure networks and information systems are reliable and resilient via appropriate risk management, and share the identified information with the national NIS competent authorities The take up of a cybersecurity culture could enhance business opportunities and competitiveness in the private sector, which could make cybersecurity a selling point.

Those entities would have to report, to the national NIS competent authorities, incidents with a significant impact on the continuity of core services and supply of goods relying on network and information systems.

National NIS competent authorities should collaborate and exchange information with other regulatory bodies, and in particular personal data protection authorities. NIS competent authorities should in turn report incidents of a suspected serious criminal nature to law enforcement authorities. The national competent authorities should also regularly publish on a dedicated website unclassified information about on-going early warnings on incidents and risks and on coordinated responses. Legal obligations should neither substitute, nor prevent, developing informal and voluntary cooperation, including between public and private sectors, to boost security levels and exchange information and best practices. In particular, the European Public-Private Partnership for Resilience (EP3R[15]) is a sound and valid platform at EU level and should be further developed.

---

14 The European Forum for Member States was launched via COM(2009) 149 as a platform to foster discussions among Member States public authorities regarding good policy practises on security and resilience of Critical Information Infrastructure

15 The European Public-Private Partnership for Resilience was launched via COM(2009) 149. This platform initiated work and fostered the cooperation between the public and the private sector on the identification of key assets, resources, functions and baseline requirements for resilience as well as cooperation needs and mechanisms to respond to large-scale disruptions affecting electronic communications.

The Connecting Europe Facility (CEF)[16] would provide financial support for key infrastructure, linking up Member States' NIS capabilities and so making it easier to cooperate across the EU.

Finally, cyber incident exercises at EU level are essential to simulate cooperation among the Member States and the private sector. The first exercise involving the Member States was carried out in 2010 ("Cyber Europe 2010") and a second exercise, involving also the private sector, took place in October 2012 ("Cyber Europe 2012"). An EU-US table top exercise was carried out in November 2011 ("Cyber Atlantic 2011"). Further exercises are planned for the coming years, including with international partners.

**The Commission will:**

- Continue its activities, carried out by the Joint Research Centre in close coordination with Member States authorities and critical infrastructure owners and operators, on identifiying NIS vulnerabilities of European critical infrastructure and encouraging the development of resilient systems.
- Launch an EU-funded pilot project[17] early in 2013 on **fighting botnets and malware,** to provide a framework for coordination and cooperation between EU Member States, private sector organisations such as Internet Service Providers, and international partners.

**The Commission asks ENISA to:**

- Assist the Member States in developing strong **national cyber resilience capabilities**, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure
- Examine in 2013 the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs) for the EU.
- Continue supporting the Member States and the EU institutions in carrying out regular **pan-European cyber incident exercises** which will also constitute the operational basis for the EU participation in international cyber incident exercises.

**The Commission invites the European Parliament and the Council to:**

- Swiftly **adopt** the proposal for a Directive on a **common high level of Network and Information Security (NIS)** across the Union, addressing national capabilities and preparedness, EU-level cooperation, take up of risk management practices and information sharing on NIS.

**The Commission asks industry to:**

- Take leadership in **investing** in a high level of cybersecurity and develop best practices and information sharing at sector level and with public authorities with the view of ensuring a strong and effective protection of assets and individuals, in

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. CEF Budget line 09.03.02 – Telecommunications networks (to promote the interconnection and interoperability of national public services on-line as well as access to such networks).

17 CIP-ICT PSP-2012-6, 325188. It has an overall budget of 15 Million Euro, with EU funding amounting to 7.7 Million Euro.

18 http://www.trustindigitallife.eu/

particular through public-private partnerships like EP3R and Trust in Digital Life (TDL)[18].

**Raising awareness**

Ensuring cybersecurity is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them.

Several initiatives have been developed in recent years and should be continued. In particular, ENISA has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships. Europol, Eurojust and national data protection authorities are also active in raising awareness. In October 2012, ENISA, with some Member States, piloted the "European Cybersecurity Month". Raising awareness is one of the areas the EU-US Working Group on Cybersecurity and Cybercrime[19] is taking forward, and is also essential in the context of the Safer Internet Programme[20] (focused on the safety of children online).

**The Commission asks ENISA to:**

- Propose in 2013 a roadmap for a "Network and Information Security driving licence" as a voluntary certification programme to promote enhanced skills and competence of IT professionals (e.g. website administrators).

**The Commission will:**

- Organise, with the support of ENISA, a cybersecurity **championship** in 2014, where university students will compete in proposing NIS solutions.

**The Commission invites the Member States[21] to:**

- Organise a yearly **cybersecurity month** with the support of ENISA and the involvement of the private sector from 2013 onwards, with the goal to raise awareness among end users. A synchronised EU-US cybersecurity month will be organised starting in 2014.
- **Step up national efforts on NIS education and training,** by introducing: training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations.

**The Commission invites industry to:**

- Promote cybersecurity **awareness at all levels**, both in business practices and in

19 This Working Group, established at the EU-US Summit in November 2010 (MEMO/10/597) is tasked with developing collaborative approaches on a wide range of cybersecurity and cybercrime issues.

20 The Safer Internet Programme funds a network of NGOs active in the field of child welfare online, a network of law enforcement bodies who exchange information and best practices related to criminal exploitation of the Internet in dissemination of child sexual abuse material and a network of researchers who gather information about uses, risks and consequences of online technologies for children's lives.

21 Also with the involvement of relevant national authorities, including NIS competent authorities and data protection authorities.

the interface with customers. In particular, industry should reflect on ways to make CEOs and Boards more accountable for ensuring cybersecurity.

## 2.2. Drastically reducing cybercrime

The more we live in a digital world, the more opportunities for cyber criminals to exploit. Cybercrime is one of the fastest growing forms of crime, with more than one million people worldwide becoming victims each day. Cybercriminals and cybercrime networks are becoming increasingly sophisticated and we need to have the right operational tools and capabilities to tackle them. Cybercrimes are high-profit and low-risk, and criminals often exploit the anonymity of website domains. Cybercrime knows no borders - the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative cross-border approach to respond to this growing threat.

### Strong and effective legislation

The EU and the Member States need strong and effective legislation to tackle cybercrime. The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, is a binding international treaty that provides an effective framework for the adoption of national legislation.

The EU has already adopted legislation on cybercrime including a Directive on combating the sexual exploitation of children online and child pornography[22]. The EU is also about to agree on a Directive on attacks against information systems, especially through the use of botnets.

**The Commission will:**

- Ensure swift transposition and implementation of the cybercrime related directives.
- Urge those Member States that have not yet ratified the **Council of Europe's Budapest Convention on Cybercrime** to ratify and implement its provisions as early as possible.

### Enhanced operational capability to combat cybercrime

The evolution of cybercrime techniques has accelerated rapidly: law enforcement agencies cannot combat cybercrime with outdated operational tools. Currently, not all EU Member States have the operational capability they need to effectively respond to cybercrime. All Member States need effective national cybercrime units.

**The Commission will:**

- Through its funding programmes[23], support the Member States to **identify gaps and strengthen their capability** to investigate and combat cybercrime. The Commission will furthermore support bodies that make the link between

[22] Directive 2011/93/EU replacing Council Framework decision 2004/68/JHA

[23] For 2013, under the Prevention and Fight against Crime Programme (ISEC). After 2013, under the Internal Security Fund (new Instrument under MFF).

research/academia, law enforcement practitioners and the private sector, similar to the on-going work carried out by the Commission-funded Cybercrime Centres of Excellence already set up in some Member States.

- Together with the Member States, coordinate efforts to identify best practices and best available techniques including with the support of JRC to fight cybercrime (e.g. with respect to the development and use of forensic tools or to threat analysis)
- Work closely with the recently launched **European Cybercrime Centre (EC3), within Europol and with Eurojust** to align such policy approaches with best practices on the operational side.

**Improved coordination at EU level**

The EU can complement the work of Member States by facilitating a coordinated and collaborative approach, bringing together law enforcement and judicial authorities and public and private stakeholders from the EU and beyond.

**The Commission will:**

- Support the recently launched **European Cybercrime Centre** (EC3) as the European focal point in the fight against cybercrime. The EC3 will provide analysis and intelligence, support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders, and gradually serve as a voice for the law enforcement community[24].
- Support efforts to increase accountability of registrars of domain names and ensure accuracy of information on website ownership notably on the basis of the Law Enforcement Recommendations for the Internet Corporation for Assigned Names and Numbers (ICANN), in compliance with Union law, including the rules on data protection.
- Build on recent legislation to continue strengthening the EU's efforts to tackle child sexual abuse online. The Commission has adopted a European Strategy for a Better Internet for Children[25] and has, together with EU and non-EU countries, , launched a **Global Alliance against Child Sexual Abuse Online[26]**. The Alliance is a vehicle for further actions from the Member States supported by the Commission and the EC3.

**The Commission asks Europol (EC3) to:**

- Initially focus its analytical and operational support to Member States' cybercrime investigations, to help dismantle and disrupt cybercrime networks primarily in the

[24] On 28 March 2012, the European Commission adopted a Communication "Tackling Crime in a Digital Age: Establishing a European Cybercrime Centre"

[25] COM(2012) 196 final

[26] Council Conclusions on a Global Alliance against Child Sexual Abuse Online (EU-US Joint Statement) of 7th and 8th June 2012 and Declaration on the launch of the Global Alliance against Child Sexual Abuse Online (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)

areas of child sexual abuse, payment fraud, botnets and intrusion.

- On a regular basis produce strategic and operational reports on trends and emerging threats to identify priorities and target investigative action by cybercrime teams in the Member States.

**The Commission asks the European Police College (CEPOL) in cooperation with Europol to:**

- Coordinate the design and planning of training courses to equip law enforcement with the knowledge and expertise to effectively tackle cybercrime.

**The Commission asks Eurojust to:**

- Identify the main obstacles to judicial cooperation on cybercrime investigations and to coordination between Member States and with third countries and support the investigation and prosecution of cybercrime both at the operational and strategic level as well as training activities in the field.

**The Commission asks Eurojust and Europol (EC3) to:**

- Cooperate closely, inter alia through the exchange of information, in order to increase their effectiveness in combating cybercrime, in accordance with their respective mandates and competence.
-

### 2.3. Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)

Cybersecurity efforts in the EU also involve the cyber defence dimension. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyberdefence capability development should concentrate on detection, response and recovery from sophisticated cyber threats

Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, private sector and academia in the EU. To avoid duplications, the EU will explore possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures on which the members of both organisations depend.

**The High Representative will focus on the following key activities and invite the Member States and the European Defence Agency to collaborate:**

- Assess operational EU cyberdefence requirements and promote the development of EU cyberdefence capabilities and technologies to address all aspects of capability development - including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability;

- Develop the EU cyberdefence policy framework to protect networks within CSDP missions and operations, including dynamic risk management, improved threat analysis

and information sharing. Improve Cyber Defence Training & Exercise Opportunities for the military in the European and multinational context including the integration of Cyber Defence elements in existing exercise catalogues;

- Promote dialogue and coordination between civilian and military actors in the EU – with particular emphasis on the exchange of good practices, information exchange and early warning, incident response, risk assessment, awareness raising and establishing cybersecurity as a priority

- Ensure dialogue with international partners, including NATO, other international organisations and multinational Centres of Excellence, to ensure effective defence capabilities, identify areas for cooperation and avoid duplication of efforts.

### 2.4. Develop industrial and technological resources for cybersecurity

Europe has excellent research and development capacities, but many of the global leaders providing innovative ICT products and services are located outside the EU. There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers. It is key to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data.

**Promoting a Single Market for cybersecurity products**

A high level of security can only be ensured if all in the value chain (e.g. equipment manufacturers, software developers, information society services providers) make security a priority. It seems[27] however that many players still regard security as little more than an additional burden and there is limited demand for security solutions. There need to be appropriate cybersecurity performance requirements implemented across the whole value chain for ICT products used in Europe. The private sector needs incentives to ensure a high level of cybersecurity; for example, labels indicating adequate cybersecurity performance will enable companies with a good cybersecurity performance and track record to make it a selling point and get a competitive edge. Also, the obligations set out in the proposed NIS Directive would significantly contribute to step up business competitiveness in the sectors covered.

A Europe-wide market demand for highly secure products should also be stimulated. First, this strategy aims to increase cooperation and transparency about security in ICT products. It calls for the establishment of a platform, bringing together relevant European public and private stakeholders, to identify good cybersecurity practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions. A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally. The Commission will promote the adoption of coherent approaches among the Member States to avoid disparities causing locational disadvantages for businesses.

Second, the Commission will support the development of security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing, while taking in due

[27] See the Commission Staff Working Document Impact Assessment accompanying the Commission proposal for a Directive on network and information security, Section 4.1.5.2

account the need to ensure data protection. Work should focus on the security of the supply chain, in particular in critical economic sectors (Industrial Control Systems, energy and transport infrastructure). Such work should build on the on-going standardisation work of the European Standardisation Organisations (CEN, CENELEC and ETSI)[28], of the Cybersecurity Coordination Group (CSCG) as well as on the expertise of ENISA, the Commission and other relevant players.

**The Commission will**:

- Launch in 2013 a public-private **platform on NIS solutions** to develop incentives for the adoption of secure ICT solutions and the take-up of good cybersecurity performance to be applied to ICT products used in Europe.
- Propose in 2014 recommendations to ensure cybersecurity across the ICT value chain, drawing on the work of this platform
- Examine how major providers of ICT hardware and software could inform national competent authorities on detected vulnerabilities that could have significant security-implications.

**The Commission asks ENISA to:**

- Develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardisation bodies and the European Commission Joint Research Centre, **technical guidelines and recommendations for the adoption of NIS standards and good practices** in the public and private sectors.

**The Commission invites public and private stakeholders to:**

- Stimulate the development and adoption of industry-led **security standards**, technical norms and security-by-design and privacy-by-design principles by ICT product manufacturers and service providers, including cloud providers; new generations of software and hardware should be equipped with **stronger, embedded and user-friendly security** features.
- Develop industry-led standards for companies' performance on cybersecurity and improve the information available to the public by developing **security labels** or kite marks helping the consumer navigate the market.

**Fostering R&D investments and innovation**

R&D can support a strong industrial policy, promote a trustworthy European ICT industry, boost the internal market and reduce European dependence on foreign technologies. R&D should fill the technology gaps in ICT security, prepare for the next generation of security challenges, take into account the constant evolution of user needs and reap the benefits of dual use technologies. It should also continue supporting the development of cryptography. This has to be complemented by efforts to translate R&D results into commercial solutions by providing the necessary incentives and putting in place the appropriate policy conditions.

[28] Particularly under the Smart Grids Standard M/490 for the first set of standards for a smart grid and reference architecture.

The EU should make the best of the Horizon 2020[29] Framework Programme for Research and Innovation, to be launched in 2014. The Commission's proposal contains specific objectives for trustworthy ICT as well as for combating cyber-crime, which are in line with this strategy. Horizon 2020 will support security research related to emerging ICT technologies; provide solutions for end-to-end secure ICT systems, services and applications; provide the incentives for the implementation and adoption of existing solutions; and address interoperability among network and information systems. Specific attention will be drawn at EU level to optimising and better coordinating various funding programmes (Horizon 2020, Internal Security Fund, EDA research including European Framework Cooperation).

**The Commission will:**

- Use Horizon 2020 to address a range of areas in ICT privacy and security, from R&D to innovation and deployment. Horizon 2020 will also develop tools and instruments to fight criminal and terrorist activities targeting the cyber environment.
- Establish mechanisms for better coordination of the research agendas of the European Union institutions and the Member States, and incentivise the Member States to invest more in R&D.

**The Commission invites the Member States to:**

- Develop, by the end of 2013, good practices to use the **purchasing power of public administrations** (such as via public procurement) to stimulate the development and deployment of security features in ICT products and services.
- Promote early involvement of industry and academia in developing and coordinating solutions. This should be done by making the most of Europe's Industrial Base and associated R&D technological innovations, and be coordinated between the research agendas of civilian and military organisations;

**The Commission asks Europol and ENISA to:**

- Identify emerging trends and needs in view of evolving cybercrime and cybersecurity patterns so as to develop adequate digital forensic tools and technologies.

**The Commission invites public and private stakeholders to:**

- Develop, in cooperation with the insurance sector, **harmonised metrics for calculating risk premiums**, that would enable companies that have made investments in security to benefit from lower risk premiums.

### 2.5. Establish a coherent international cyberspace policy for the European Union and promote EU core values

Preserving open, free and secure cyberspace is a global challenge, which the EU should address together with the relevant international partners and organisations, the private sector and civil society.

[29] Horizon2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. Running from 2014 to 2020, the EU's new Framework Programme for research and innovation will be part of the drive to create new growth and jobs in Europe.

In its international cyberspace policy, the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyberspace. The EU will also work towards closing the digital divide, and will actively participate in international efforts to build cybersecurity capacity. The EU international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights.

**Mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy**

The Commission, the High Representative and the Member States should articulate a coherent EU international cyberspace policy, which will be aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and private sector. EU consultations with international partners on cyber issues should be designed, coordinated and implemented to add value to existing bilateral dialogues between the EU's Member States and third countries. The EU will place a renewed emphasis on dialogue with third countries, with a special focus on like-minded partners that share EU values. It will promote achieving a high level of data protection, including for transfer to a third country of personal data. To address global challenges in cyberspace, the EU will seek closer cooperation with organisations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS. At bilateral level, cooperation with the United States is particularly important and will be further developed, notably in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime.

One of the major elements of the EU international cyber policy will be to promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance. The EU should promote corporate social responsibility[30], and launch international initiatives to improve global coordination in this field.

The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments. The EU supports the efforts to define norms of behaviour in cyberspace that all stakeholders should adhere to. Just as the EU expects citizens to respect civic duties, social responsibilities and laws online, so should states abide by norms and existing laws. On matters of international security, the EU encourages the development of confidence building measures in cybersecurity, to increase transparency and reduce the risk of misperceptions in state behaviour.

The EU does not call for the creation of new international legal instruments for cyber issues.

The legal obligations enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should be also respected online. The EU will focus on how to ensure that these measures are enforced also in cyberspace.

To address cybercrime, the Budapest Convention is an instrument open for adoption by third countries. It provides a model for drafting national cybercrime legislation and a basis for international co-operation in this field.

[30] *A renewed EU strategy 2011-14 for Corporate Social Responsibility***;** COM(2011) 681 final

If armed conflicts extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights law will apply to the case at hand. **Developing capacity building on cybersecurity and resilient information infrastructures in third countries**

The smooth functioning of the underlying infrastructures that provide and facilitate communication services will benefit from increased international cooperation. This includes exchanging best practices, sharing information, early warning joint incident management exercises, and so on. The EU will contribute towards this goal by intensifying the on-going international efforts to strengthen Critical Information Infrastructure Protection (CIIP) cooperation networks involving governments and the private sector.

Not all parts of the world benefit from the positive effects of the Internet, due to a lack of open, secure, interoperable and reliable access. The European Union will therefore continue to support countries' efforts in their quest to develop the access and use of the Internet for their people, to ensure its integrity and security and to effectively fight cybercrime.

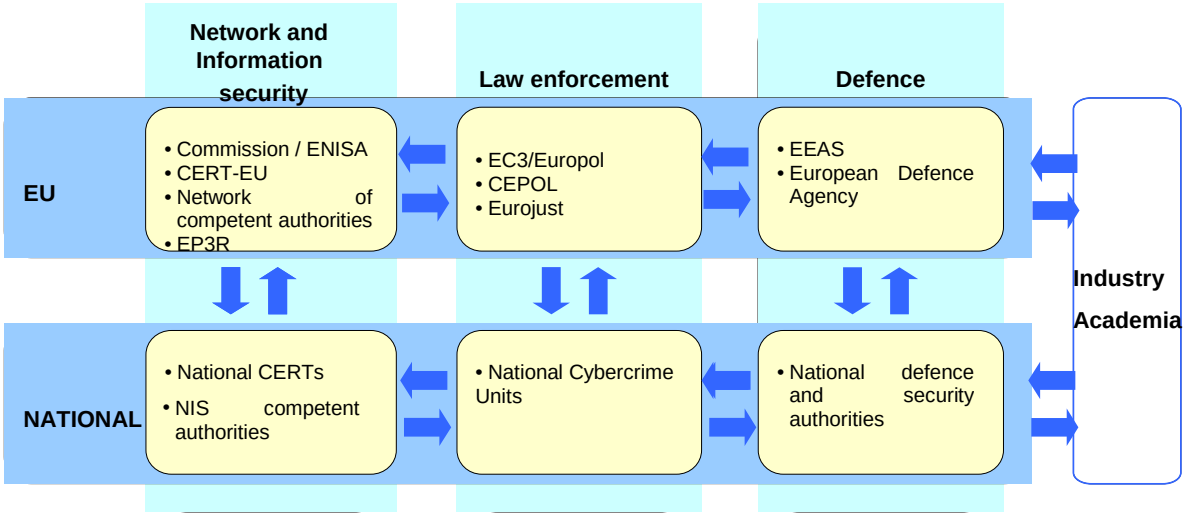
**In cooperation with the Member States, the Commission and the High Representative will:**

- Work towards a coherent EU International cyberspace policy to increase engagement with key international partners and organisations, to mainstream cyber issues into CFSP, and to improve coordination of global cyber issues;
- Support the development of norms of behaviour and confidence building measures in cybersecurity. Facilitate dialogues on how to apply existing international law in cyberspace and promote the Budapest Convention to address cybercrime;
- Support the promotion and protection of fundamental rights, including access to information and freedom of expression, focusing on: a) developing new public guidelines on freedom of expression online and offline; b) monitoring the export of products or services that might be used for censorship or mass surveillance online; c) developing measures and tools to expand Internet access, openness and resilience to address censorship or mass surveillance by communication technology; d) empowering stakeholders to use communication technology to promote fundamental rights;
- Engage with international partners and organisations, the private sector and civil society to support global capacity-building in third countries to improve access to information and to an open Internet, to prevent and counter cyber threats, including accidental events, cybercrime and cyber terrorism, and to develop donor coordination for steering capacity-building efforts;
- Utilise different EU aid instruments for cybersecurity capacity building, including assisting the training of law enforcement, judicial and technical personnel to address cyber threats; as well as supporting the creation of relevant national policies, strategies and institutions in third countries;
- Increase policy coordination and information sharing through the international Critical Information Infrastructure Protection networks such as the Meridian network, cooperation among NIS competent authorities and others.

## 3. ROLES AND RESPONSIBILITIES

Cyber incidents do not stop at borders in the interconnected digital economy and society. All actors, from NIS competent authorities, CERTs and law enforcement to industry, must take responsibility both nationally and at EU-level and work together to strengthen cybersecurity. As different legal frameworks and jurisdictions may be involved, a key challenge for the EU is to clarify the roles and responsibilities of the many actors involved.

Given the complexity of the issue and the diverse range of actors involved, centralised, European supervision is not the answer. National governments are best placed to organise the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks. At the same time, due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement. To address cybersecurity in a comprehensive fashion, activities should span across three key pillars—NIS, law enforcement, and defence—which also operate within different legal frameworks:




### 3.1. Coordination between NIS competent authorities/CERTs, law enforcement and defence

**National level**

Member States should have, either already today or as a result of this strategy, structures to deal with cyber resilience, cybercrime and defence; and they should reach the required level of capability to deal with cyber incidents. However, given that a number of entities may have operational responsibilities over different dimensions of cybersecurity, and given the importance of involving the private sector, coordination at national level should be optimised across ministries. Member States should set out in their national cybersecurity strategies the roles and responsibilities of their various national entities.

Information sharing between national entities and with the private sector should be encouraged, to enable the Member States and the private sector to maintain an overall view of different threats and get a better understanding of new trends and techniques used both to commit cyber-attacks and react to them more swiftly. By establishing national NIS cooperation plans to be activated in the case of cyber incidents, the Member States should be able to clearly allocate roles and responsibilities and optimise response actions.

**EU level**

Just as at national level, there are at EU level a number of actors dealing with cybersecurity. In particular, the ENISA, Europol/EC3 and the EDA are three agencies active from the perspective of NIS, law enforcement and defence respectively. These agencies have Management Boards where the Member States are represented, and offer platforms for coordination at EU level.

Coordination and collaboration will be encouraged among ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, risk assessment, training and sharing of best practices. They should collaborate while preserving their specificities. These agencies together with CERT-EU, the Commission and the Member States should support the development of a trusted community of technical and policy experts in this field.

Informal channels for coordination and collaboration will be complemented by more structural links. EU military staff and the EDA cyber defence project team can be used as the vector for coordination in defence. The Programme Board of Europol/EC3 will bring together among others the EUROJUST, CEPOL, the Member States[31], ENISA and the Commission, and offer the chance to share their distinct know-how and to make sure EC3's actions are carried out in partnership, recognising the added expertise and respecting the mandates of all stakeholders. The new mandate of ENISA should make it possible to increase its links with Europol and to reinforce links with industry stakeholders. Most importantly, the Commission's legislative proposal on NIS) would establish a cooperation framework via a network of national NIS competent authorities and address information sharing between NIS and law enforcement authorities.

**International**

The Commission and the High Representative ensure, together with the Member States, coordinated international action in the field of cybersecurity. In so doing, the Commission and the High Representative will uphold EU core values and promote a peaceful, open and transparent use of cyber technologies. The Commission, the High Representative and the Member States engage in policy dialogue with international partners and with international organisations such as Council of Europe, OECD, OSCE, NATO and UN.

## 3.2. EU support in case of a major cyber incident or attack

Major cyber incidents or attacks are likely to have an impact on EU governments, business and individuals. As a result of this strategy, and in particular the proposed directive on NIS, the prevention, detection and response to cyber incidents should improve and Member States and the Commission should keep each other more closely informed about major cyber incidents or attacks. However, the response mechanisms will differ depending on the nature, magnitude and cross-border implications of the incident.

If the incident has a serious impact on the business continuity, the NIS directive proposes that national or Union NIS cooperation plans be triggered, depending on the cross-border nature of the incident. The network of NIS competent authorities would be used in that context to share

[31] via representation within the EU Cybercrime Task Force, which is made up of the heads of the EU cybercrime Units of the Member States

information and support. This would enable preservation and/or restoration of affected networks and services.

If the incident seems to relate to a crime, Europol/EC3 should be informed so that they - together with the law enforcement authorities from the affected countries – can launch an investigation, preserve the evidence, identify the perpetrators and ultimately make sure they are prosecuted.

If the incident seems to relate to cyber espionage or a state-sponsored attack, or has national security implications, national security and defence authorities will alert their relevant counterparts, so that they know they are under attack and can defend themselves. Early warning mechanisms will then be activated and, if required, so will crisis management or other procedures. A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union).

If the incident seems having compromised personal data, the national Data Protection Authorities or the national regulatory authority pursuant to Directive 2002/58/EC should be involved.

Finally, the handling of cyber incidents and attacks will benefit from contact networks and support from international partners. This may include technical mitigation, criminal investigation, or activation of crisis management response mechanisms.

## 4. CONCLUSION AND FOLLOW-UP

This proposed cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, outlines the EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world.[32]

This vision can only be realised through a true partnership, between many actors, to take responsibility and meet the challenges ahead.

The Commission and the High Representative therefore invite the Council and the European Parliament to endorse the strategy and to help deliver the outlined actions. Strong support and commitment is also needed from the private sector and civil society, who are key actors to enhance our level of security and safeguard citizens' rights.

[32] The financing of the Strategy will occur within the foreseen amounts for each of the relevant policy areas (CEF, Horizon 2020, Internal Security Fund, CFSP and External Cooperation, notably the Instrument for Stability) as set out in the Commission's proposal for the Multi-Annual Financial Framework 2014-2020 (subject to the approval of the Budget Authority and the final amounts of the adopted MFF for 2014-2020). With regard to the need to ensure overall compatibility with the number of posts available to decentralised agencies and the sub-ceiling for decentralised agencies in each expenditure heading in the next MFF, the agencies (CEPOL, EDA ENISA, EUROJUST and EUROPOL/EC3) which are requested by this Communication to take on new tasks will be encouraged to do so in so far as the actual capacity of the agency to absorb growing resources has been established and all possibilities for redeployment have been identified.

The time to act is now. The Commission and the High Representative are determined to work together with all actors to deliver the security needed for Europe. To ensure that the strategy is being implemented promptly and assessed in the face of possible developments, they will gather together all relevant parties in a high-level conference and assess progress in 12 months.