EUROPEAN
COMMISSION

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

Brussels, XXX
[…](2012) XXX draft

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 have 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 human 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 malicious activities and misuse; and governments have a significant role in defending a free and safe cyberspace. Governments have several tasks: to safeguard access and openness, to respect and protect human 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 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.

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 shown that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity incidents are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, sanitation, electricity or mobile networks. Threats could originate from many different areas—including criminal, politically motivated or terrorist attacks. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threat for EU governments and companies.

The EU economy is already seriously affected by vast numbers of cybercrime activities against the private sector. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom.

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.

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

1.2. Objectives

The EU is determined to 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, EU-level activities that can enhance the EU's overall performance, namely:

- explaining the principles and values that will guide EU action in the field of cybersecurity.
- becoming "cyber resilient", by increasing capabilities, preparedness, cooperation, information exchange and awareness in the field of Network and Information Security, for the public and private sectors and at national and EU level.
- drastically reducing cybercrime by strengthening the expertise of those in charge of investigating and prosecuting it, by adopting a more coordinated approach between Law Enforcement Agencies across the Union, and by enhancing cooperation with other actors.
- developing an EU Cyber Defence Policy and capabilities in the framework of the Common Security and Defence Policy.
- fostering the industrial and technological resources required to benefit from the Digital Single Market: to stimulate the emergence of a European industry and market for secure ICT; contribute to the growth and competitiveness of the EU economy; and to increase the public and private spending on cybersecurity Research and Development (R&D).
- enhancing the EU's international cyberspace policy to promote the respect of EU core values, define norms for responsible behaviour, and advocate the application of existing international laws in cyberspace.

- assisting countries outside the EU, through building cybersecurity capacity, strengthening the resilience of information infrastructures.
- clarifying the roles and responsibilities of the various actors in the field of cybersecurity.

1.3. An open and free Internet

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, requirements for transparency, accountability and security are becoming more prominent.

This strategy clarifies which principles should guide cybersecurity policy in the EU and internationally. It considers that cybersecurity can only be successful if it is based on the European fundamental rights and values (human dignity, freedom, democracy, equality, solidarity, the rule of law and justice). Reciprocally, citizens' rights cannot be secured without safe networks and systems, for example capable of protecting freedom of expression, personal data and privacy; those rights also depend on norms, laws and values framing state behaviour.

In that context, the strategy reaffirms the importance of all stakeholders in the current Internet governance model. EU actions in the field of cybersecurity should be guided by values and existing frameworks rather than new international treaties.

The EU's core values apply as much in the digital as 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. Human rights, freedom of expression and information, the right to privacy and the protection of personal data must be guaranteed. Measures to ensure cybersecurity must respect fundamental rights and freedoms.

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: with access to an open Internet to enable 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 supports this multi-stakeholder governance approach[3], which safeguards individual rights, accountability, transparency and an adequate level of cybersecurity.

A shared responsibility to security

The growing dependency on information and communication technologies in all domains of human life has led to vulnerabilities which need to be thoroughly analysed, and remedied or

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

reduced. All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility and ensure a coordinated response to strengthen cybersecurity.

2. STRATEGIC PRIORITIES AND ACTIONS

The EU vision presented in this strategy is articulated in five strategic priorities, which address the challenges highlighted above. A number of short and long term actions are announced under each priority.

2.1. Becoming cyber resilient

To promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and cooperate effectively. 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 incidents. This is why the Commission has developed a policy on Network and Information Security (NIS)[4]. The **European Network and Information Security Agency** (ENISA) was established in 2004[5] and a new Regulation to strengthen ENISA and modernise its mandate is being negotiated by Council and Parliament[6]. In addition, the Framework Directive for electronic communications[7] requires providers of electronic communications to appropriately manage the risks to their networks and to report significant security breaches.

Despite progress based on voluntary commitments, there are still gaps across the EU: from the fight against botnets and malware, to public sector capabilities, to security and resilience of industrial control systems. This strategy proposes to introduce legislation to establish common minimum requirements for network and information security (NIS) at national level which would oblige Member States to: designate national competent authorities for NIS; set up a well-functioning Computer Emergency Response Team (CERT); and adopt a national cyber incident contingency/cooperation plan and a national NIS strategy. 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.

As cyber incidents often span across borders, cooperation amongst EU Member States is necessary. This strategy proposes to introduce legislation to set up coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national competent authorities. National competent authorities will be asked to ensure appropriate EU-wide cooperation, notably on the basis of a European cyber incident contingency/cooperation plan, designed to respond to cyber incidents with cross-

---

4 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 a series of Action Plans on Critical Information Infrastructure Protection (CIIP) (COM(2009)149, endorsed by Council Resolution 2009/C 321/01; COM(2011)163).

5 Regulation (EC) No 460/2004

6 COM(2010)521

7 See http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf

border dimension. This cooperation will also build upon the progress made in the context of the European Forum for Member States, which has held productive discussions and exchanges on NIS public policy and can be integrated in the cooperation mechanism once in place.

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 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. This strategy proposes to introduce legislation to make 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 risks they face, ensure networks and information systems are reliable and resilient, and share information with the national competent authorities. Those entities would also have to report, to the national competent authorities, incidents with a significant impact on the continuity of services and supply of goods relying on network and information systems. National competent authorities should report incidents of a suspected criminal nature to law enforcement authorities.

The national competent authorities should regularly publish on a common 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. The European Public-Private Partnership for Resilience (EP3R[8]) is a sound and valid platform at EU level and should be further developed.

The Connecting Europe Facility (CEF)[9] will 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. The first exercise of this kind was carried out in 2010 ("Cyber Europe 2010") and a second exercise 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:

- Propose a Directive on a **common high level of network and information security (NIS)** across the Union, to address national capabilities, EU-level cooperation, take up of risk management practices and information sharing on NIS.

[8] This platform initiated work on identifying 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.

[9] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility

- Launch an EU-funded pilot project in the beginning of 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**, build expertise on security and resilience of industrial control systems and smart grids and examine the feasibility of creating specialised Computer Security Incident Response Team for Industrial Control Systems (ICS-CSIRTs) capabilities for the European Union.
- Continue supporting the Member States and the EU institutions in carrying out **pan-**European **cyber incident exercises** which will also constitute the operational basis for the EU participation in international cyber incident exercises

The Commission asks industry to:

- Take leadership in **investing** in a high level of cybersecurity, developing best practices and information sharing at sector level and with public authorities, in particular through public-private partnerships like EP3R and Trust in Digital Life (TLD)[10].

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 is 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[11] is taking forward, and also for the Safer Internet Programme[12] (focused on the safety of children online).

The Commission asks ENISA to:

- Propose a roadmap for a "Network and Information Security driving licence" for those professionals who play a role in enhancing the security of the Internet (e.g. website administrators).

The Commission will:

10 http://www.trustindigitallife.eu/

11 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.

12 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.

- 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 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, introducing:** mandatory training on NIS in schools by 2014; mandatory training on NIS and secure software development for computer science students; and mandatory 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 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 become 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, serves as an effective international instrument for the national legal foundation and also offers a model to be pursued at global level.

The EU has already developed legislation on cybercrime including a Directive on combating the sexual exploitation of children online and child pornography[13]. The EU is also about to agree on a Directive on attacks against information systems, especially through the use of botnets.

- The Commission will encourage swift implementation of the cybercrime related directives, and urge those Member States that have not yet ratified the **Council of Europe's Budapest Convention on Cybercrime** to do so as early as possible.

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

Enhanced operational capability

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 programs, 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 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 in terms of policy approaches to fight cybercrime; while at the same time work closely with the recently launched **European Cybercrime Centre (EC3), within Europol** to align such policy approaches with best practices on the operational side.

Improved coordination at EU level

The borderless nature of cybercrime requires international law enforcement cooperation to tackle it. The EU can complement the work of Member States by facilitating a coordinated and collaborative approach, bringing together law enforcement authorities and public and private stakeholders from the EU and beyond.

The Commission will:

- Continue to support the **European Cybercrime Centre** as the European focal point in the fight against cybercrime. It will provide analysis and intelligence, support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing with Member States, the private sector and other stakeholders, and gradually serve as a voice for the law enforcement community[14].
- Promote the Law Enforcement Recommendations for the Internet Corporation for Assigned Names and Numbers (ICANN) to make registrars of domain names more accountable by ensuring information on website ownership is accurate, with a view to seeing the Recommendations implemented by ICANN as soon as possible[15].
- Build on recent legislation to continue strengthening the EU's efforts to tackle

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

[15] In doing so, the Commission and the Member States will ensure that implementation of the Recommendations is compliant with Union law and notably with the rules on data protection

child sexual abuse online. The Commission has adopted a European Strategy for a Better Internet for Children[16] and has, together with EU and non-EU countries, , launched a **Global Alliance against Child Sexual Abuse Online**[17]. The Alliance is a vehicle for further actions from the Member States supported by the Commission and the European Cybercrime Centre.

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 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.

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

Cybersecurity efforts in the EU also involve the defence dimension. To increase the resilience of the communication and information systems supporting Member States' defence and national security, cyberdefence activities will concentrate on capability development to detect, respond and recover 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 in cyberdefence, 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 EEAS, the Member States and the European Defence Agency will focus on the following key activities:

- 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

[16] COM(2012) 196 final

[17] Council Conclusions on a Global Alliance against Child Sexual Abuse Online (EU-US Joint Statement) of 7th and 8th June 2012

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 civil-military dialogue in the EU and contribute to the coordination between all actors at EU level – 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 the 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. There are increasing concerns about the trustworthiness of hardware and software components produced in third countries used in critical services and infrastructures and increasingly in personal mobile devices.

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. Many players, however, regard security as little more than an additional burden and there is limited demand for security solutions. There need to be minimum 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. A Europe-wide market demand for highly secure products should also be stimulated.

This strategy proposes to increase cooperation and transparency about security in ICT products. It proposes a platform, bringing together 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 developing technical norms, standards and solutions, as well as the possibility for EU-wide certification.

The Commission has already announced that it will support the development of security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing, including for data protection. Work should start around security of supply chains, and critical economic sectors (Supervisory Control and Data Acquisition Systems, Smart Grids, Transport), building on the expertise of ENISA, the European Commission Joint Research Centre and other relevant players.

The Commission will:

- Launch a **platform on NIS solutions** to develop and adopt secure ICT solutions

and define minimum cybersecurity performance requirements to be applied to ICT products used in Europe.

- Propose recommendations to ensure cybersecurity across the ICT value chain, drawing on the work of this platform
- Support EU-wide certification schemes
- Examine whether major providers of ICT hardware and software should also provide information on detected vulnerabilities that could have significant security-implications to the national competent authorities.

The Commission asks ENISA to:

- Develop, in cooperation with national competent authorities, relevant stakeholders, International and European standardisation bodies and the 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 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

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 putting in place the appropriate policy conditions.

The EU should make the best of the Horizon 2020[18] Framework Programme for Research, to be launched in 2014. It contains specific objectives for trustworthy ICT, which will be defined in coherence 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.

[18] 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.

The Commission will:

- Use Horizon 2020 to address a range of areas in ICT privacy and security, from roadmap driven R&D to innovation and deployment.
- Establish mechanisms for better coordination of the research agendas of the European Union institutions and the Member States, and motivate 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 core EU values

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

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 human rights.

Mainstreaming cyberspace issues into EU international policies

The EEAS, the Commission and the Member States will 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. The 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 the EU

values. To address global challenges in cyberspace, EU will seek closer cooperation with organisations such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS.

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[19], 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 support the creation of new international legal instruments for cyber issues, but believes existing international law should be applied. If conflicts should extend to cyberspace, state behaviour should follow the long established principles of the Law of Armed Conflicts and International Humanitarian Law. To address cybercrime, the existing Council of Europe Convention on Cybercrime, also known as Budapest Convention, serves as an effective international instrument for the national legal foundation and offers a model to be pursued at global level.

The legal obligations enshrined in International Human Rights Law should be respected online, and the EU will focus on how to ensure that the existing obligations of this law are enforced also in cyberspace.

Developing capacity building on cybersecurity and resilient information infrastructures

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. This will be done while ensuring human rights and fundamental freedoms are respected and that the Internet remains a driver of political freedom, democratic development and economic growth, in line with existing initiatives such as the Action Plan on Human Rights and Democracy and the European No-Disconnect Strategy. Increased global connectivity can bring new security challenges, which should be prevented by the active engagement in cybersecurity capacity building.

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

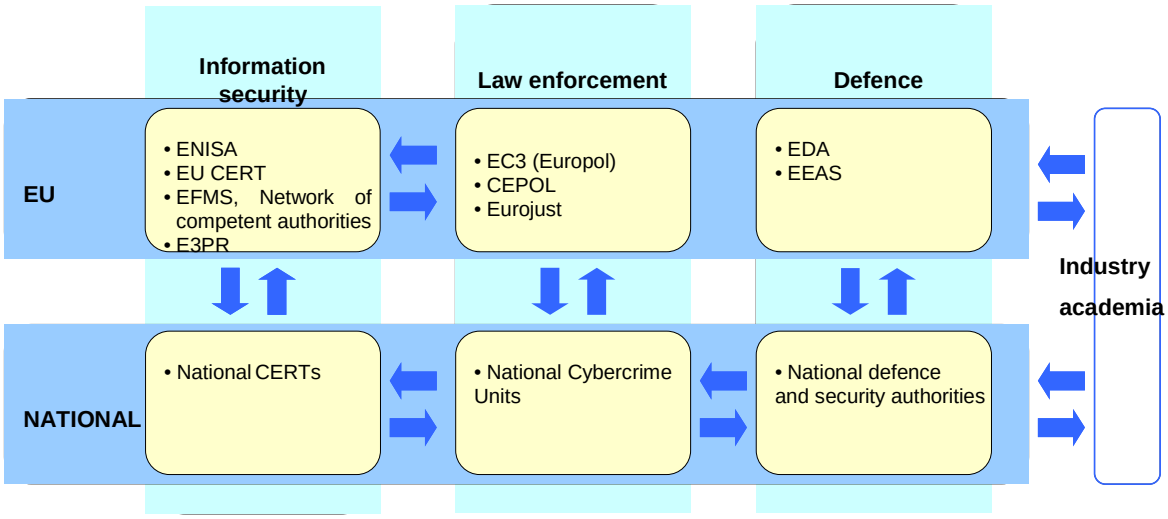
In cooperation with the Member States, the EEAS and the Commission will:

- Work towards a more 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 human 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 counter cyber threats 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 jurisdiction may co-exist, 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, central European supervision is not the answer. National governments are the best placed to organise the prevention and response to cyber 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, an effective national response requires EU-level involvement. A comprehensive response in cybersecurity must span across three key pillars—NIS, law enforcement, and defence—which also operate within different legal frameworks:



For the EU response to be effective, coordination and cooperation must take place both within and across these pillars. In addition, Member States, the European Commission and the European External Action Service will ensure coordinated EU international action in cyberspace issues.

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 express 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 contingency plans in the case of cyber incidents, 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, ENISA, Europol/EC3 and EDA are three agencies active from the perspective of NIS, law enforcement and defence respectively. These agencies have boards where Member States are represented, and offer platforms for coordination at EU level.

Coordination and collaboration will be encouraged between ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, threat assessment, training and sharing of best practices. They should collaborate while

preserving their specificities. A trusted community of technical and policy experts should be nurtured between them, and with CERT-EU, the Commission and Member States.

Informal channels of 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 EUROJUST, CEPOL, Member States[20], 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 create a network between competent authorities and facilitate information sharing between NIS and law enforcement authorities.

Specific attention should be devoted to coordination in the R&D area. While Horizon 2020 provides a Programme Committee for better coordination with Member States, 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 and EEAS will continue to work closely with the Council and European Parliament to develop cybersecurity policies. In addition, they will consider establishing a cybersecurity programme on training and exercises to be developed jointly between Member States, the Commission, the EEAS and the various agencies involved in that field.

International

The EU intends to increase cooperation in the field of cybersecurity with its international partners. In so doing, it will uphold EU core values in its international cybersecurity cooperation, and will promote a peaceful, open and transparent use of cyber technologies. Cooperation with the United States is especially important and will be further developed, notably on the basis of the EU-US Working Group on Cyber-Security and Cyber-Crime. The EU will deepen policy dialogue with international organisations such as UN, OSCE, Council of Europe, NATO and OECD.

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 the EU. As a result of this strategy, and in particular the proposed directive on NIS, the detection of cyber incidents should improve and Member States and the Commission should keep each other better 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 might have a serious impact on the continuity of business, the draft NIS directive proposes that national or European cyber contingency 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 information and support. This would normally enable preservation and/or restoration of affected networks.

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

If the incident seems to relate to a crime, the network of NIS competent authorities should inform Europol/EC3 so that they - together with law enforcement 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 very serious cyber incident or attack could form sufficient grounds for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union).

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

The 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 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.

This vision can only be realised through a true partnership to meet the challenges ahead: in cybersecurity, there are many actors that must contribute and take responsibility.

We invite the European Council and the European Parliament to endorse the strategy and to help deliver the outlined actions. We also need strong support and commitment from the private sector and civil society, who are key actors to enhance our level of security and safeguard citizens' rights.

The time to act is now. We 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, the Commission together with the EEAS will gather all relevant parties in a high-level conference and assess progress 12 months after this Communication is adopted.

ANNEX: GLOSSARY OF TERMS AND DEFINITIONS

Botnet is a collection of internet-connected computers whose security defences have been breached, and control ceded to a malicious party. The controller of a botnet is able to direct the activities of these compromised computers.

Computer Emergency Response Team (CERT) is a service organization responsible for receiving, reviewing and responding to computer security incident reports and activity. CERTs contribute to ensuring take-up of state-of-the-art technology and systems management practices to resist incidents and attacks on networked systems and to limit damage and ensure continuity of critical services.

CERT-EU is the Computer Emergency Response Team for the EU institutions, bodies and agencies. It was launched as a Pre-configuration Team in 2011 and was established on a permanent basis in 2012.

Common Security and Defence Policy (CSDP) is an integral part of the Common Foreign and Security Policy. It provides the European Union with an operational capacity drawing on civilian and military assets. The Union may use them on missions outside the Union for peace-keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter. The performance of these tasks shall be undertaken using capabilities provided by the Member States.

Cyber-attack: A malicious activity originating in cyberspace, directed against networks and information systems and affecting the confidentiality, integrity, and/or availability of the networks and information systems themselves or of the information they store, transmit, or process, and intended to achieve an effect in the network and information systems or causing effects or damage in the physical world. A cyber-attack involves one or a combination of the following actions: illegal access to information systems, illegal system interference, illegal data interference and illegal interception through the use of tools or devices that include computer programs designed for such purpose (e.g. botnets, malware) or codes allowing unlawful access to information systems.

Cybercrime: Cybercrime refers to a broad range of different criminal activities where computers and information systems are involved either as a tool or as a 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).

Cyberspace: For the purpose of this strategy “cyberspace” is understood as a man-made, global domain consisting of interdependent networks and information infrastructure, including the Internet, telecommunications networks, globally interconnected computer systems, embedded processors and controllers (comprising relevant hardware, middleware and software). In some related discussions and literature this term is also referred to as "Cyber sphere”, “Cyber domain”, “Digital world”, "Digitised world”, or ”Digital ecosystem".

Cyber Incident is an action, activity, or other occurrence, intentional or accidental, that is expected to, or has been confirmed to, have an adverse effect on Network and Information Security.

Cyberdefence: All activities carried out by operational phase of military information and communication technology functions to ensure the delivery and management of ICT services in response to potential and actual malicious actions or attacks of a military nature that originate from cyberspace.

Cyber resilience is the ability of a network or information system to sustain and recover from intentional or unintentional incidents, either back to its original state or an adjusted state based on new requirements. Building resilience requires a long-term effort involving reengineering fundamental preventive processes, both technical and organisational.

Cybersecurity: Cyber-security 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. The term cyber-security covers also prevention and law enforcement measures to fight cybercrime.

European Defence Agency (EDA) is an EU Agency tasked to support the Member States and the Council in their efforts to improve European defence capabilities.

EU Cybercrime Taskforce (EUCTF) is composed of the heads of high-tech crime units of the Member States and has the task to optimise work on fighting cybercrime.

European Police College (CEPOL) is an EU Agency that provides EU-wide police training and, by developing specialised cybercrime-investigation training, can collate, share and expand the knowledge and expertise needed by law enforcement to successfully prosecute cybercrime.

European Union Military Staff (EUMS) provides military expertise to the EEAS under the direction of the Military Committee of the Member States Chiefs of Defence. The EU Military Staff is responsible for the coordination of the military components in executing the Common Security and Defence Policy.

EUROJUST is an EU Agency that supports judicial cooperation in cybercrime investigation, for instance by facilitating coordination and providing advice on legal and regulatory frameworks issues of jurisdiction.

European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice will be in charge of operating a number of highly sensitive EU-wide large-scale IT systems in the area of border control and law enforcement, (e.g. Visa Information System, SIS II and EURODAC). One of the Agency's key challenges will be to ensure the protection of the communication infrastructure on which these systems rely.

European Forum for Member States (EFMS) on public policies for security and resilience in the context of Critical Information Infrastructure Protection (CIIP) is a platform dedicated to officials from competent national public authorities of Member States of the EU and of the European Free Trade Association (EFTA) to informally discuss, initiate common actions and share information and good policy practices on security and resilience of Critical Information Infrastructure.

European Network and Information Security Agency (ENISA) was created "for the purpose of ensuring a high and effective level of network and information security within the

Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market".

European Public-Private Partnership for Resilience (EP3R) is an EU-wide platform for cooperation between the public and the private sector tasked to develop coordinated strategic policy objectives as well as tactical/operational measures to strengthen security and resilience of Critical Information Infrastructures.

Europol is an EU Agency that provides criminal intelligence analysis and operational support to the Member States to tackle cybercrime and links with each Member State through Europol National Units. Europol has set up a European Cybercrime Centre (EC3) in 2013 that will act as the focal point in Europe's fight against cybercrime by pooling expertise, supporting criminal investigations and promoting EU-wide solutions while raising awareness of cybercrime issues across the EU.

Joint Research Centre (JRC) is the Commission in-house science service with the mission to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle. Working in close cooperation with Commission policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Malware is computer software designed to infiltrate or damage a computer system without the owner's consent. It is distributed through a variety of means (emails, computer viruses, and botnets). Intention is to obtain data (passwords, codes) in a fraudulent way, or to integrate this computer in a computer network destined to be used for criminal actions.

Network and Information Security (NIS) means the ability of a network or an information system to resist, at a given level of confidence, to accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.