Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"(JOIN(2013) 1)

Working document

28 February 2014

1. Achieving cyber resilience

1.1 Increasing network and information security

Actions proposed in the Cybersecurity Strategy	Progress to date and outlook
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 identifying NIS vulnerabilities of European critical infrastructure and encouraging the development of resilient systems.**	• The Joint Research Centre (JRC) of the European Commission deals with research activities on the identification of interdependencies between the ICT and energy sectors. The JRC also works towards raising cybersecurity awareness within the Thematic Network on Critical Energy Infrastructure Protection and will soon kick off activities to provide energy operators information on threats and incidents through the "Incident and Threat Information Sharing – EU" Centre. • Under the auspices of the **Smart Grids Task Force**, set up by the European Commission at the end of 2009, a dedicated Expert Group gathering stakeholders from the energy and ICT sectors, consumer associations and regulators, will deliver: 1) in March 2014 a Data Protection Impact Assessment template, possibly to be endorsed via a Commission Recommendation in 2014; and 2) a set of Best Available

	Techniques (BATs) pinpointing potential cybersecurity risks inherent to the common minimal functional requirements for Smart Metering Systems as in Recommendation 2012/148. This Expert Group will also provide recommendations to the Member States on minimum cyber security requirements for Smart Grids in Q2 2014, building on ENISA's work in this domain.
• **Launch an EU-funded pilot project 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 European Commission launched in 2013 a call for a pilot project, the **Advanced Cyber Defence Centre** (ACDC), to fight botnets and malware through the collaboration of a European-wide coalition of public and private stakeholders. By the end of the project in 2015, high uptake by participants and wider market actors is expected.
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**	• On 30 January 2014, ENISA has adopted on 30 January 2014 the report "Smart Grid Threat Landscape and Good Practice Guide" and will organize a workshop on 2 April 2014 to disseminate the findings of the report.
• **Examine in 2013 the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs) for the EU**	• In December 2013, ENISA released a Good practice guide for CERTs in the area of Industrial Control Systems, building on current best practices of those CERTs that have responsibilities for ICS networks, and on the work carried out by ENISA on baseline capabilities for national/ governmental (n/g) CERTs. The guide is structured on four categories of baseline capabilities: mandate, service portfolio and operations. It also addresses cooperation with relevant ICS stakeholders.

The Commission will: • **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**	• ENISA is currently planning with the EU Member States and EFTA countries the third pan European Exercise, **Cyber Europe 2014**. 29 European countries (EU+EFTA) and the EU institutions (coordinated by CERT-EU) will participate to CyberEurope 2014, that will aim to: o Test the European alert, cooperation and information exchange procedures between relevant national authorities o Provide an opportunity for the Member States to test internally their national NIS contingency plans and capabilities o Explore the effect of multiple and parallel information exchanges between private-public and private-private o Explore the NIS incident response escalation and de-escalation processes (technical-operational-political) o Explore the public affairs handling of large-scale cyber incidents. Upon lessons learnt from previous exercises, CyberEurope2014 will be carried out in three different phases to test EU coordination and cooperation capabilities at Technical, Operational and Strategic level.
The Commission invites the EP 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**	• This Commission proposal for a Directive (COM(2013) 48 final) is currently being discussed with the Council and European Parliament.
The Commission asks industry to:	• The **Trust in Digital Life** public-private partnership, with the support of DG CNECT, launched the annual event "Trust in Digital Life" (2013 in

• **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 particular through public-private partnerships like EP3R and Trust in Digital Life (TDL)**	Brussels, 2014 in Vienna) to foster the exchange of best practices on disruptive cybersecurity technologies.

1.2 Raising awareness

Actions proposed in the Cybersecurity Strategy	**Progress to date and outlook**
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 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.	• ENISA has launched an open call for experts and organisations to guide the development of a roadmap for a "**Network and Information Security driving licence**", the identification of relevant players and the specification of NIS skills being targeted. This process will entail a mapping of existing courses and certification schemes and assessing to what extent the offer matches the increasing need for NIS skills. The results will be released by the end of 2014. • ENISA is organising a workshop, to be held in Brussels on 29 April 2014, to discuss and share ideas on a **Cybersecurity championship.** • The **European Cybersecurity Awareness Month held in October 2013** was the first fully-fledged European campaign with 23 Member States + some EEA countries participating with the involvement of some 40 stakeholders and more than 50 NIS activities being carried out across Europe. It built upon a pilot month held in 2012n in which 8 Member

• **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 the interface with customers. In particular, industry should reflect on ways to make CEOs and Boards more accountable for ensuring cybersecurity.	States participated. The goal for the 2014 European Cybersecurity Awareness Month is to have the participation of all the Member States and to further develop the international outreach, particularly in cooperation with the United States. In October 2013, the International Mobile Safety Tips were released, coincing with the European Cybersecurity Awareness Month 2013, the 10th year of National Cyber Security Awareness Month in the US and the 4th annual Asia Pacific Economic Cooperation Telecommunications and Information Working Group (APEC-TEL) Cyber Security Awareness Day.

2. Drastically reducing cybercrime

2.1 Strong and effective legislation

Actions proposed in the Cybersecurity Strategy	**Progress to date and outlook**
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.	• The EU co-legislators have adopted two Directives related to cybercrime to date: o Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, and o Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. For the first Directive, the Commission hosted two meetings of experts from Member States ("Contact Committee") to allow for exchanges of experience in implementing the Directive into national law and to strive to

	solve open questions. The meetings took place on 13 December 2012 and 7 June 2013 and were well attended. The Commission also dealt with several implementation issues by means of bilateral exchanges with the relevant Member States. On 18 December 2013, the deadline for the implementation of the provisions of the Directive into national law expired. The Commission is currently in the process of assessing compliance of Member States' national laws with the directive, on the basis of the notifications submitted, with a view to determining whether the launch of infringement proceedings will be necessary, and has launched proceedings for non-notification of transposition measures where necessary. For the second Directive, on attacks against information systems, which was adopted more recently, the deadline for implementation of the provisions into national law is set for 4 September 2015. The Commission plans to create a Contact Committee, as described above for the Directive on fighting child sexual abuse, to facilitate the implementation process and to provide assistance where necessary to resolve open questions. The first meeting of the Committee is planned to take place in early summer 2014. • For the promotion of the Budapest Convention, the Commission, in cooperation with the EEAS, ensures that it is consistently presented as the instrument of choice and a model for national cybercrime legislation in all relevant fora. The Commission also urges ratification in bilateral meetings with relevant Member States. The Commission welcomes the recent ratification of the Budapest Convention by the Czech Republic (entry into force on 1 December 2013) and the Swedish legislative initiative to ratify the Convention still in 2014. At present, 23 Member States have ratified the Convention. Besides Sweden, Greece, Ireland, Luxembourg and Poland still have not ratified the Convention.

2.2 Enhanced operational capability to combat cybercrime

Actions proposed in the Cybersecurity Strategy	Progress to date and outlook
The Commission will: • Through its funding programmes, 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 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).	• The European Commission has been supporting Member States' efforts to exchange expertise on training and jointly develop training materials. One such means of support is the European Cybercrime Training and Education Group (ECTEG), which brings together participants from law enforcement, academia and the private sector from across Member States to jointly identify training needs and develop training materials, funded by the EU. Since 2009, over €5 million of ISEC funding has been provided to this initiative to build the capacity of European Law Enforcement Agencies to combat cybercrime. This has resulted in the development of a complete training pack that has been used already (at no cost) to train over 1,500 cybercrime investigators in the field of computer forensics and evidence collection. A revised agreement has recently been established between the European Cybercrime Centre (EC3), the European Police Training College (CEPOL) and ECTEG with a view to ensuring that necessary updates to training curricula are carried out. • In 2013, the Commission also adopted a Communication on Establishing a European Law Enforcement Training Scheme to equip law enforcement officers with the knowledge and skills needed to prevent and combat cross-border crime effectively through efficient cooperation with EU colleagues. The Training Scheme aims to make the EU's response to common security challenges more effective, to raise the standard of policing across the EU and to stimulate the development of a common law

	enforcement culture as a means of enhancing mutual trust and cooperation. • Furthermore, the EU funding administered by DG HOME (the former "ISEC Fund", now named "ISF Police" from 2014 onwards) is currently used to fund 10 Cybercrime Centres of Excellence in Research and Training in Greece, France, Estonia, Czech Republic, Bulgaria, Belgium, Romania, UK, Spain, Poland and Bulgaria. The Centres of Excellence are engaged in the development of forensic tools, the creation of a range of cybercrime training programmes and practical research into issues affecting European citizens, such as online financial crime, telecoms fraud and cybersecurity of critical national infrastructure. • The EU also provides funding to the European Academy of Law (ERA) for a project consisting of eight basic training courses on the legal and technical aspects of cybercrime that take place in Trier at the ERA premises between 2012 and 2015. The project will provide approximately 500 judges and prosecutors with the essential skills necessary to cope with internet-related offences. • Other initiatives by the Member States to identify and remedy gaps in capabilities, in particular where they relate to cooperation across national borders and communities, have also benefited from the support available under ISEC. A targeted call was launched under the 2013 ISEC programme, with €5 million committed to projects on cybercrime, sexual exploitation of children, and illegal use of the internet. This call aims to support, among others: co-operation between experts and law enforcement authorities on understanding and combating cybercrimes; actions establishing standard forms for law enforcement requests to the private sector and vice versa; actions against illegal online content; prevention of and fighting sexual exploitation of children online including through identification of offenders via credit cards and promoting cooperation with the European Cybercrime Centre at Europol. Successful projects are due to be announced in April 2014.

	• Future targeted and general calls under the new ISF Police funding scheme are also planned to include the support for bodies that make the link between research/academia, law enforcement practitioners and the private sector as a key priority. • The Commission's Joint Research Centre (JRC) has embarked on a fruitful cooperation with the European Cybercrime Centre since its inception in January 2013. The first joint research topic selected has focused on a video and image database search tool for forensic purposes. The aim is to develop and integrate smart tools for the identification of victims and perpetrators of online child abuse in very large media (video and picture) databases through enhanced automated categorisation of these media. The JRC furthermore has developed tools for open source intelligence analysis that are made available free of charge to law enforcement agencies of the Member States and have already been deployed in a number of Member States. • The Commission also plans to support the Member States' mutual assessment on cybercrime under the auspices of the Council Working Party on General Matters including Evaluations (GENVAL), scheduled to begin in late 2014, which includes possibilities for sharing best practices and identifying weaknesses.
• 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.	• The Commission and the EC³ are in constant contact to ensure alignment of operational activities with existing EU policy, on the one side, and effective support to operational activities by the policy process, on the other side. The alignment is strengthened through the EMPACT Policy Cycle process. The Policy Cycle was created by the Council of the European Union to tackle the most important criminal threats in a coherent and methodological manner through optimum cooperation between the relevant services of the Member States, EU Institutions and EU Agencies as well as relevant third countries and organisations. In identifying these most important criminal threats, the Europol Serious and Organised Crime Threat Assessment (SOCTA) provides key information.

	In summer 2013, on the basis of the SOCTA, three of the top criminal threats were identified in the realm of cybercrime, namely on-line and payment card fraud, cybercrimes which cause serious harm to their victims such as online child sexual exploitation, and cyber-attacks which affect critical infrastructure and information systems in the EU. Experts from all participating Member States and the EC³ then worked together with the Commission and Eurojust to identify strategic goals for the next four years of close cooperation on these priorities, and are currently implementing the first year's operational action plan. The priorities set by the EC³ in its work correspond to those priorities and operational actions. • To ensure continued support and policy alignment, the European Commission organized a Conference on 10 February 2014 on the occasion of the first anniversary of the EC³ to assess the achievements of the EC³ to date, identify emerging threats and propose priorities for the future work of the EC³, in close cooperation with stakeholders, including Member States' law enforcement authorities, the private sector and academia.

2.3 Improved coordination at EU level

Actions proposed in the Cybersecurity Strategy	**Progress to date and outlook**
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	• The Commission supports the work of the EC³ on an ongoing basis and holds weekly calls to ensure coordination, besides actively participating in the Programme Board, the Advisory Groups, and conferences and events, where the Commission regularly presents EU policy relevant to the subject matter and seeks to gather input for future policy priorities, to ensure that policies are put into place that address the problems at hand

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[1].	and facilitate cooperation between law enforcement agencies. • The Commission plans to delegate funding from the Internal Security Fund "Police" to Europol to support the work of the EMPACT Policy Cycle and finance operational cooperation. • The Commission furthermore proposed delegating funding for research purposes from the Horizon2020 budget to Europol in order to allow for more targeted research addressing the needs of law enforcement agencies. This funding, to be administered by Europol directly, would have allowed for a closer control by the end user (law enforcement) over the research and development output, to ensure that the projects funded result in deliverables that are useful to law enforcement agencies across the Member States. Unfortunately, this was rejected by the Member States in the Horizon2020 Committee for the current work programme. The Commission intends to resolve the concerns and to further pursue such a delegation, which should be beneficial for law enforcement across EU Member States.
• 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.	• The Commission has worked in close cooperation with international partners to promote law enforcement recommendations enabling a limited degree of accountability on the internet, by asking website owners to identify themselves when purchasing the domain name (currently it is possible to register a domain name to "Mickey Mouse", residing in Disneyland). Where websites are used for criminal activities, this makes investigations very difficult if not impossible. The law enforcement recommendations seek to implement minimum standards to allow for identification of a website owner by the registrar administering the domain names, in line with data protection rules. These recommendations have now been reflected to a certain extent in a new version of the Registrar Accreditation Agreement (RAA), in such a way as to fully respect the EU data protection acquis and at the same time not to grant

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

	complete impunity to cybercriminals. The implementation of this agreement now has to be followed closely to ensure that it also stays in line with the acquis.
• 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[2] and has, together with EU and non-EU countries, launched a **Global Alliance against Child Sexual Abuse Online**[3]. The Alliance is a vehicle for further actions from the Member States supported by the Commission and the EC3.	• The Global Alliance against Child Sexual Abuse Online, launched in December 2012, brought together 48 countries dedicated to improve victim identification, to more successfully prosecute perpetrators, to increase awareness and to reduce the amount of child sexual abuse images available online. It has since been able to expand its membership to 52 countries from around the globe and actively seeks to foster global cooperation in the fight against these crimes, inter alia by following up with participating countries on the commitments they have undertaken. In 2013, participating countries reported on their commitments to reach the high-level policy targets of the Alliance, and the Commission published a report summarizing these commitments in December 2013. In the near future, the US will take over the rotating presidency and secretariat of the Global Alliance from the European Commission. A threat assessment and a report on the implementation of participants' commitments are scheduled to be drafted this year, under the lead of the US, and a second conference at Ministerial level is to be held in the fall of 2014 to assess implementation and to jointly decide on the next steps for the Global Alliance. • The Member States' mutual assessment on cybercrime under the auspices of the Council Working Party on General Matters including Evaluations (GENVAL), scheduled to begin in late 2014, which was already mentioned above, will also contain questions relevant to the fight against child sexual abuse and will therefore provide further opportunities for strengthening the efforts to tackle this phenomenon. • The JRC is supporting the EU cybersecurity strategy in the fight against

[2] COM(2012) 196 final

[3] 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)

	on-line Child Sexual Abuse (CSA), with new and improved techniques related to biometric matching system, computer vision for the identification of victims and perpetrators of such crimes, as needed by enforcers. This work is done in close cooperation with the EU Cybercrime Centre and national enforcement authorities.
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 **EC³**, true to its mandate, has focused on assisting Member States' law enforcement agencies to dismantle and disrupt cybercrime networks primarily in the areas of child sexual abuse, payment fraud, botnets and intrusion. Its first year of operations was quite successful. • In the area of fighting **botnets, intrusions and other cyber attacks** it has, for example, assisted in the coordination of two major international investigations on ransomware, a type of malware that locks computers and effectively holds them hostage until a ransom is paid. Criminals had infected tens of thousands of computers worldwide and had realised over one million euros of profit per year before being shut down. EC³ also supported several international initiatives in the areas of botnet takedowns, disruption and investigation of criminal forums and malware attacks against financial institutions. • Significant efforts – jointly with many Member States and non-EU cooperation partners – were dedicated to **fighting online sexual abuse and exploitation of children**. This resulted in the disruption of the covert internet communication of over 25,000 paedophiles engaged in the dissemination of around 2 million harrowing pictures of child sexual abuse, leading to the arrest of hundreds of suspects within the European Union and beyond. • Last but not least, in the field of **payment fraud**, the EC3 supported investigations resulting in three different international networks of credit card fraudsters being dismantled, with tens of suspects being arrested and illegal workshops for producing devices and software to manipulate Point-of-Sale terminals being discovered and put out of operation.

	• Beyond this central task of assisting in and coordinating cross-border investigations, the EC3 has published **strategic analysis** and delivered **specialised reports on new trends and threats**. • The EC³ prepared a **report** on the activities during its first year, on current threats and trends and possible future priorities for the fight against cybercrime, which was published on 10 February 2014.[4]
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.	• CEPOL, in close cooperation with Europol and the European Cybercrime Training and Education Group (ECTEG), is currently conducting an assessment of training needs in two of the three priority areas identified under the EMPACT Policy Cycle, namely cyber attacks and payment card fraud. It will then organise additional courses addressing those areas. • In 2013, CEPOL organised 3 residential trainings on 'Child Abuses in Cyberspace', 'Member States' and Union capacities to detect, investigate and prosecute cybercrime', and 'Cybercrime Vs Cyber-Security', one Webinar on Cybercrime, and updated the e-Learning module on Cybercrime. In 2014, CEPOL will: o continue to foster coordination in cyber-crime areas following the EMPACT priorities and in line with the European Commission Communication on the Law Enforcement Training Scheme (LETS); o draft a training needs assessments for child sexual abuse, cyber-attacks and credit card frauds, in conjunction with Europol (EC3); o organise 4 residential courses, namely 'Child Abuses in Cyberspace', 'Member States' and Union capacities to detect, investigate and prosecute cybercrime', 'Cybercrime Vs Cyber-Security', and 'Cyber-Forensics and Digital Evidences'; o and hold 5 webinars on 'Internet Frauds (Credit Cards)', 'Disclosure',

[4] https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report.

	Investigation and Prosecution of Cybercrime', 'Forensic and Digital Evidences', 'Sexual Exploitation of Children on-line', 'Cooperation between Law Enforcement and Judicial Authorities within Child Sexual Exploitation'.
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.	Work on-going
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.	• Eurojust and Europol have been cooperating closely in the context of the three focal points related to cybercrime, i.e. cyber attacks, child sexual abuse and payment card fraud. Eurojust has been associated with all three focal points since 2010, and also participates in the EMPACT Policy Cycle 2014-2017 for all three cyber-related priorities. In order to ensure that Member States benefit most from both agencies, Europol and Eurojust are currently engaged in a process to avoid overlaps and duplication of work between themselves and to ensure the best possible level of coordination.

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

Actions proposed in the Cybersecurity Strategy	Progress to date and outlook
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;	Work on-going
• 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;	• Cyber Defence was discussed at the European Council in December 2013. Following the Council work is taking place in the following five areas: o to promote the development of EU cyber defence capabilities, research and technologies within EDA Cyber Defence Roadmap; o to protect networks supporting CSDP institutions, missions and operations; o to improve Cyber Defence Training, Education & Exercise opportunities for the Member States in the European and multinational context; o to strengthen cooperation with NATO, and other international organisations, private sector and academia to ensure effective defence capabilities; o to develop early warning and response mechanisms and to seek synergies between different actors in Europe in responding to cyber threats.

• 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	Work on-going
• 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.	• EU-NATO informal staff-to staff cyber security meetings have taken place regularly since 2010. Common areas for further cooperation have been identified, such as the need to raise cyber security awareness, training and capability development in terms of cyber resilience.

2.4 Develop industrial and technological resources for cybersecurity

Promoting a Single Market for cybersecurity products

Actions proposed in the Cybersecurity Strategy	**Progress to date and outlook**
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.	• The NIS Platform follows a bottom-up approach, drawing from the working practices of the public and private participants. The first meeting of the NIS Platform took place on 17 June 2013, following a call for expression of interest organised between April and May 2013.

	• At present, around 230 public and private organisations are taking part in the Platform, including organisations from: o 18 MS and Norway, including representatives from ministries, NIS agencies, NRAs and national CERTs, o Research and academia, o Various industry sectors: ICT, finance, post, transport, healthcare, defence, energy, water. o Colleagues from DG ENER, MOVE, HOME, MARKT, ENTR, JRC, as well as from the European Parliament are participating or following the work of the Platform. • Following the first plenary meeting, the NIS Platform has been divided in 3 Working Groups (WG): o WG1 on cybersecurity risk management Chair: Mr. Carl Colwill, Head of Security Risk Management, BT Co-chair: Mr. Miguel A. Sánchez Fornié, Director Control Systems and Telecoms, Iberdrola o WG2 on information exchange and incident notification Chair: Mr. Waldemar Grudzien, Director, Association of German Banks Co-chair: Mr. Will Semple, Head of Threat and Vulnerability Management Team, NYSE Euronext o WG3 on secure ICT Research and Innovation Chair: Mr. Fabio Martinelli, Security Group Istituto di Informatica e

	Telematica, CNR Co-chair: Mr. Raúl Riesco Granadino, Cybersecurity Excellence Program Manager, Inteco The WGs are organised in smaller groups, as follows: o WG1 – Risk management ➢ SG1: existing risk management methods and gap analysis ➢ SG2: existing risk metrics and the need to research new measures ➢ SG3: existing approaches to the application of frameworks and maturity models ➢ SG4: awareness o WG2 – Information sharing and incident notification ➢ SG1: existing information sharing platforms ➢ SG2: information sharing, including incident notification ➢ SG3: information sharing protocols o WG3 – Secure ICT Research and Innovation ➢ Steering Committee ➢ Secure ICT research landscape ➢ Business cases and innovation paths

	➢ Strategic Research Agenda ➢ Snapshot of education and training The bulk of the work of the Platform takes place in the WGs, which meet on a regular basis to conduct technical discussions and provide draft consensus papers, which are discussed and validated by the Plenary. The Commission hosted the kick-off meetings of the WGs on 25, 26 and 27 September 2013. A second plenary meeting was organised on 11 December 2013 to take stock of the progress of the 3 WGs and get feedback from the Plenary. The NIS Platform will issue the following **deliverables**: o Guidance on risk management and information sharing (WG1 and 2): June 2014 o Secure ICT research landscape (WG3): June 2014 o Business cases and innovation (WG3): December 2014 o Strategic Research Agenda (WG3): March 2015 o Snapshot of education and training (WG3): December 2015
• Propose in 2014 recommendations to ensure cybersecurity across the ICT value chain, drawing on the work of this platform	• In Q2 2014 the NIS Platform will issue guidance on risk management, information sharing and incident notification. This will be the first output of the Platform and an important one, as it will serve as a basis for the Commission to develop its own recommendations on cybersecurity. The main objective of the next plenary meeting of the Platform on 30 April

	2014 will be to discuss the first draft deliverables of WG1 and WG2.
• Examine how major providers of ICT hardware and software could inform national competent authorities on detected vulnerabilities that could have significant security-implications.	To be developed in the near future
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.	ENISA supports the activities of the NIS Platform and has published guidance and reports in various areas, amongst others: - Guidelines for trust service providers to mitigate the impact of security incidents and conduct risk assessment - Recommendations for a methodology of the assessment of severity of personal data breaches - Analysis on power supply dependencies in the electronic communications sectors - Good practice guide for CERTs on the Directive on attacks against information systems - Report on national roaming for resilience - Good practice guide on Alerts-Warnings-Announcements for CERTs - National level risk assessment: An Analysis report - Good Practice guide for securely deploying Governmental clouds - Schemes for auditing security measures - Technical guidelines on incident reporting in the electronic communications

	sector
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.	• In Horizon 2020, there are calls in 2014 for research and innovation in security-by-design and privacy-by-design. • Under the EU Cloud Computing Strategy, work has been carried out to cut through the jungle of existing standards so that users enjoy interoperability, data portability and reversibility. The Commission will work with the support of ENISA and other relevant bodies to assist the development of EU-wide voluntary certification schemes and establish a list of such schemes by 2014.

Fostering R&D investments and innovation

Actions proposed in the Cybersecurity Strategy	**Progress to date and outlook**
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	• The European Framework Programme for Research, H2020, has entered into force on 1st January 2014. The Work Programmes and the Calls for proposals for 2014 and 2015 have now been published. They cover ICT research, development and innovation actions addressing privacy, cybersecurity, trust and cybercrime.

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.	• (WG3) of the NIS Platform addresses issues related to Cybersecurity research and innovation. • Taking into account the variety of the challenges and the diversity of the players involved in Cyber Security, privacy and trust research, WG3 will also serve as a facilitator for the coordination of, and collaboration between, research agendas across Europe, including industry research roadmaps and national research and innovation programmes of the Member States. • In 2014, WG3 of the NIS Platform will present a map of the research landscape (including identifying, national R&I programmes in Cyber Security, trustworthy ICT and privacy), that will serve as a basis to engage with the national research agencies on a better coordination of research programs and resources.
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;	• Good practices to use the purchasing power of public administrations will be developed in the near future • The WG3 of the NIS Platform, promotes the engagement of industry and academia on future Research and Innovation.

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.	• In 2013, ENISA has adopted its annual Report on the Threat Landscape
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**.**	• The Commission is working on analysing the EU Cybersecurity insurance market and considering various options to leverage cyber insurance to foster cybersecurity and resilience

2.4 Establish a coherent international cyberspace policy for the European Union and promote EU core values

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

Actions proposed in the Cybersecurity Strategy	**Progress to date and outlook**
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;	• The EEAS is regularly contacted by third countries who intend to establish high level cyber dialogues with the EU. The EEAS coordinates these dialogues, with support of the European Commission. • A structured cyber dialogue currently exists with the US in the form of the EU-US Working Group on Cyber Security and Cybercrime. It is divided into four expert sub-groups that work on (i) cyber incident management, (ii) public-private partnerships, (iii) awareness raising, and (iv) cybercrime.

	• The Working Group has brought a meaningful contribution to EU-US cooperation on cybersecurity, particularly in fostering expert-level discussions on operational matters. Among other concrete deliverables, it is worth mentioning the 2011 EU-U.S. Cyber-incident table-top exercise, public-private workshops on botnets and smart grids, and the 2012 joint declaration on making the Internet safer for children. • The second meeting of the EU-China Task Force hosted by EEAS with support from COM took place in October 2013, with participation of Member States. The meeting provided a good opportunity to deepen cooperation but highlighted inevitable differences between our approaches to cyberspace. The next Task Force is scheduled for Autumn 2014. • A structured dialogue with India has been set up and last met in October 2012. Topics discussed included preparation of cyber security strategies, standardisation and regulatory questions, cybercrime issues and international cyber issues. • In 2014 potential cooperation with Japan, South Korea, Brazil and Taiwan is being examined.
• 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;	• Like-minded countries are working actively to build global consensus on norms for responsible behaviour in cyberspace and support the continued application of current international law over the introduction of new ones, which could serve to introduce further unwanted government control. The London Process aims to develop a common understanding among stakeholders on how to preserve positive aspects of cyberspace and is working towards defining universal norms. EEAS played an active part in the organisation of last October's Seoul Conference on Cyberspace. 1600 participants took part from 87 countries with attendance form

	governments, civil society, the private sector, academia, and international organisations. Eight ministerial level speakers were present from EU Member States. Themes of discussions focused on the economic opportunities of cyberspace, capacity building, cybercrime, international security, trust and resilience issues in cyberspace. The Conference confirmed two parallel processes in cyberspace: the growing divide on Internet governance issues and growing consensus on the need to invest more in cyber capacity building. • Confidence Building Measures (CBMs) are designed to address misunderstandings and misperception of cyber events to reduce the risk of conflict between states in cyberspace. In November 2013 the OSCE agreed to an initial set of CBMs, the first set of its kind to be agreed in a multilateral context. EEAS and EU member states support initiatives on development of CBMs within the ARF format.
• 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 us communication technology to promote fundamental rights;	• The EEAS, in accordance with the Action Plan, held informal discussions with the Commission and Member States in preparation for the draft guidelines on freedom of expression online and offline, to be adopted in 2014. The aim of the guidelines is to address unjustified restrictions on freedom of expression. Consultations were held with civil society on how to better engage and protect journalist and bloggers and in June 2013, the EEAS launched a public consultation through the Internet.
• 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,	• The EU is striving to devise a role in steering cyber capacity building efforts globally. EEAS is working with the EU Institute for Security Studies to take forward this work. Conferences are being organised for this year to agree on the regional and functional focus of

cybercrime and cyber terrorism, and to develop donor coordination for steering capacity-building efforts;	cybersecurity capacity building efforts, develop international coordination in capacity building and develop appropriate models that work.
• 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	• Cyber security capacity building in third countries is a priority both in the Strategy and globally. It requires focus on improving governance, protecting infrastructure, endorsing the rule of law and the provision of training. Cyber capacity building pilot projects have started within the Instrument for Stability with further Instrument for Stability funding available from 2015. To achieve tangible results and to promote EU core values in this domain capacity building needs to become a central feature in EU international cyber policy.
• 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.	• The European Forum for Member States continues to address policy cooperation among national authorities competent for NIS matters.