الجمهورية الجزائرية الدّيمقراطية الشّعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Direction de la Coopération et des
Échanges Interuniversitaires
Sous-Direction de
la Coopération Multilatérale
N° : 412 /D.C.E.I.U/S.D.C.M/2016

Alger, le 25 JUIL. 2016

3509 /Bec/16

2016 [illegible] 28

Monsieur le Président
de la Conférence Régionale des Universités
de l'Est

Objet : Cyber-sécurité/ Plan d'action public-privé de l'Union européenne.
P.J: Trois (03).

J'ai l'honneur de vous informer que la Commission européenne a lancé un nouveau partenariat public-privé sur la cyber-sécurité qui vise à coordonner les efforts de ses Etats membres et des acteurs du marché de la cyber-sécurité pour faire face aux cyber-attaques.

Ce partenariat public-privé s'inscrit dans le cadre du Programme « Horizon 2020 pour la recherche et l'innovation ». Il fera l'objet d'une série initiale d'appels d'offres au 1er trimestre 2017.

Veuillez trouver ci-joint le document relatif à ce sujet.

Je vous saurais gré des dispositions que vous voudrez bien prendre en vue d'assurer une large diffusion auprès des établissements universitaires de la région Est.

Cordialement

عن الوزير و بتفويض منه
مدير التعاون و [illegible] الجامعات
إمضاء سعيد [illegible] رزقي

La Commission signe un accord avec le secteur de la cybersécurité et redouble d'efforts pour lutter contre les cybermenaces

Bruxelles, le 5 juillet 2016

La Commission lance aujourd'hui un nouveau partenariat public-privé sur la cybersécurité qui devrait générer 1,8 milliard d'euros d'investissements d'ici à 2020. Ce partenariat fait partie d'un ensemble d'initiatives pour mieux armer l'Europe contre les cyberattaques et renforcer la compétitivité du secteur de la cybersécurité.

D'après un récent sondage, au moins 80 % des entreprises européennes ont connu au minimum un incident lié à la cybersécurité au cours de l'a nnée écoulée et le nombre d'incidents de sécurité tous secteurs confondus dans le monde a augmenté de 38 % en 2015.Ces incidents nuisent aux entreprises européennes, qu'elles soient grandes ou petites, et risquent d'ébranler la confiance dans l'é conomie numérique. Dans le cadre de sa stratégie pour le marché unique numérique, la Commission veut renforcer la coopération par-delà les frontières et entre tous les acteurs et secteurs œuvrant dans le domaine de la cybersécurité, et contribuer au développement de technologies, de produits et de services sûrs et innovants, *dans l'ensemble* de l'UE.

Andrus **Ansip**, vice-président pour le marché unique numérique, a déclaré: *«Sans confiance et sans sécurité, il n'y a pas de marché unique numérique. L'Europe doit être prête à faire face aux cybermenaces qui sont de plus en plus sophistiquées et ne connaissent pas de frontières. Aujourd'hui, nous proposons des mesures concrètes pour renforcer la résilience de l'Europe contre ces attaques et nous doter des capacités nécessaires pour la construction et le développement de notre économie numérique.»*

Günther H. **Oettinger**, commissaire européen pour l'économie et la société numériques, a ajouté: *«L'Europe a besoin de produits et de services de qualité, abordables et interopérables dans le domaine de la cybersécurité. C'est une opportunité majeure pour notre secteur de la cybersécurité d'être compétitifs sur un marché mondial en pleine expansion. Nous exhortons les États membres et tous les organismes de cybersécurité à renforcer leur coopération et à mettre en commun leurs connaissances, leurs informations et leur expertise afin d'améliorer la cyber-résilience de l'Europe. Le partenariat historique en matière de cybersécurité signé aujourd'hui constitue une étape cruciale.»*

Le plan d'action présenté aujourd'hui comprend le lancement du premier **partenariat public-privé européen sur la cybersécurité**. L'UE investira 450 millions d'euros dans ce partenariat dans le cadre de son programme pour la recherche et l'innovation Horizon 2020. Les acteurs du marché de la cybersécurité, représentés par l'organisation européenne pour la cybersécurité (ECSO), devraient investir trois fois plus. Ce partenariat regroupera également des membres d'administrations publiques nationales, régionales et locales, de centres de recherche et d'universités. L'o bjectif du partenariat est de stimuler la coopération à un stade précoce du processus de recherche et d'innovation et de forger des solutions de cybersécurité applicables à différents secteurs, tels que l'énergie, la santé, les transports et la finance. Le commissaire Oettinger signe aujourd'hui le partenariat avec l'ECSO à Strasbourg (les photos et les vidéos seront disponibles vers 12h00 CET).

Par ailleurs, la Commission présente différentes mesures pour remédier à la fragmentation du marché européen de la cybersécurité. Actuellement, une entreprise du secteur des technologies de l'information doit parfois se soumettre à différentes procédures de certification pour vendre ses produits et services dans plusieurs États membres. La Commission va donc se pencher sur la possibilité de mettre en place un **cadre européen de certification** pour les produits de sécurité des TIC.

Une myriade de PME européennes innovantes ont fait leur apparition sur des marchés de niches (par exemple, la cryptographie) et sur d'autres bien établis avec de nouveaux modèles d'entreprise (par exemple, logiciels antivirus), mais elles sont souvent incapables de développer leur activité. La Commission souhaite **faciliter l'accès au financement pour les petites entreprises** actives dans le domaine de la cybersécurité et elle explorera différentes options prévues par le plan d'investissement de l'Union.

La **directive sur la sécurité des réseaux et de l'i nformation**, qui devrait être adoptée par le Parlement européen demain, met déjà en place un réseau d'équipes de réaction aux incidents touchant la sécurité informatique dans l'ensemble de l'UE afin de réagir rapidement aux cybermenaces et

cyberincidents. Elle établit également un «groupe de coopération» entre États membres afin de favoriser et de faciliter une coopération stratégique ainsi que l'échange d'informations, et de renforcer la confiance. Aujourd'hui, la Commission invite les États membres à tirer le meilleur parti de ces nouveaux mécanismes et à accroître la coordination lorsque c'est possible. Elle proposera des moyens pour **améliorer la coopération transfrontière en cas de cyberincident majeur**. Étant donné la rapidité avec laquelle évolue la cybersécurité, la Commission présentera également son évaluation de l'**Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA)**.Cette évaluation permettra de déterminer si le mandat de l'ENISA et ses capacités sont toujours adéquats pour assurer sa mission d'assistance aux États membres de l'UE aux fins de renforcer leur propre cyber-résilience. La Commission étudie également comment renforcer et rationaliser la coopération dans le domaine de la cybersécurité à travers les différents secteurs économiques, notamment dans la formation et l'enseignement en matière de cybersécurité.

Contexte

Le plan d'action présenté aujourd'hui se fonde essentiellement sur la stratégie pour le marché unique numérique de 2015, la stratégie de cybersécurité de l'UE de 2013 et la future directive sur la sécurité des réseaux et de l'information (SRI). Il s'a ppuie sur les récentes communications concernant le programme européen en matière de sécurité et la lutte contre les menaces hybrides.

Pour en savoir plus

Questions et réponses

Cybersécurité

Le secteur de la cybersécurité

ENISA

Résultats de la consultation publique sur le PPPc et les mesures d'a ccompagnement

Documents adoptés aujourd'hui (en ligne vers 10h00 CET):

- Communication: Renforcer le système européen de cyber-résilience et favoriser la compétitivité et l'innovation dans le secteur de la cybersécurité

- Décision de la Commission relative à un accord contractuel concernant un partenariat public-privé contractuel sur la cybersécurité (PPPc)

- Document de travail des services de la Commission relatif au PPPc et aux mesures d'accompagnement

- Document de travail des services de la Commission relatif à l'évaluation de la cybersécurité dans le septième programme-cadre de l'UE pour la recherche et le développement technologique (7e PC) et le programme-cadre pour l'innovation et la compétitivité (CIP)

- Document de travail des services de la Commission relatif à la procédure de consultation

Médias sociaux

#DigitalSingleMarket (marché unique numérique); #cybersecurity (cybersécurité); #PPP; #**NIS** (directive SRI).

IP/16/2321

Personnes de contact pour la presse:

Nathalie VANDYSTADT (+32 2 296 70 83)
Marie FRENAY (+32 2 29 64532)

Renseignements au public: Europe Direct par téléphone au 00 800 67 89 10 11 ou par courriel

EUROPEAN CYBER SECURITY ORGANISATION

Contract between the public side (European Commission) and the private side (ECSO ASBL) has been signed at the European Parliament

Strasbourg, July 5, 2016

On July 5, 2016, contract between the public side (European Commission) and the private side (ECSO ASBL) has been signed at the European Parliament in Strasbourg, to stimulate the cybersecurity industry in Europe on strategic research and innovation.

The European Commission today signed the contract for a Public-Private Partnership (PPP) with the European Cyber Security Organisation (ECSO) ASBL for a strategic alliance in cybersecurity. The EU will invest €450 million in this partnership under its research and innovation (R&I) programme H2020. In return, each euro of public funding is expected to trigger additional investments of three or more Euro by the cybersecurity market players represented by ECSO. In total, this partnership on cybersecurity is expected to raise around €1.8 billion of investment by 2020 and with this, develop innovative and trusted cybersecurity solutions, products and services in Europe.

ECSO will work directly with the European Commission to improve Europe's industrial policy on cybersecurity, focusing on innovation and following a strategic R&I roadmap. This PPP will help build trust among Member States, industrial actors and end-users, by fostering bottom up

cooperation on strategic R&I and building a strong, harmonised and competitive cybersecurity market in Europe across various sectors such as energy, transport, health and finance.

The signature ceremony hosted by Vice President for Digital Single Market, Andrus Ansip and Commissioner for Digital Economy and Society, Gunther Oettinger, gathered high-level ECSO member representatives of 48 public and private organisations from 14 different countries. The signature was preceded by a short exchange of views between Commissioner Oettinger and participants.

Commissioner Gunther Oettinger signed the contract of the PPP on cybersecurity together with Luigi Rebuffi, CEO of the European Organisation for Security (EOS) and interim Chairman of ECSO.

Commissioner Oettinger said that "Europe needs high quality, affordable and interoperable cybersecurity products and services. There is a major opportunity for our cybersecurity industry to compete in a fast-growing global market. We call on Member States and all cybersecurity bodies to strengthen cooperation and pool their knowledge, information and expertise to increase Europe's cyber resilience. The milestone partnership on cybersecurity signed today with the industry is a major step".

Luigi Rebuffi said that "Signing this contractual partnership with the European Commission represents a pivotal step in public-private cooperation for the advancement of cybersecurity R&I and the growth of a competitive cybersecurity and ICT industry in Europe. ECSO is a fast growing organisation which has received, as of today, more than 120 membership applications. This shows the strong commitment from all cybersecurity players to develop a sustainable market in Europe ensuring digital autonomy and contributing to the goals of the Digital Single Market".

Background

The PPPs are based on roadmaps for research and innovation activities which are the result of an open consultation process, and which have been positively evaluated by the European Commission with the help of independent experts. The PPP on cybersecurity will build on the Strategic Research Agenda (SRA) in the area of secure information and communication technologies (ICT), developed by the NIS Platform and published in September 2015. In 20 January, 2016 a preparation workshop for the "Contractual Public-Private Partnership" between the European Commission, Member States and the cybersecurity industry took place in Brussels. The workshop aimed to brainstorm on the concept of a PPP. As the result of the workshop 5 working groups of industry representatives were formed led by EOS, CNR, ACN, Guardtime representing the Estonian ICT Association and TELETRUST to create ECSO. ECSO was legally established on 13 June 2016 as a fully self-financed non-for-profit association (ASBL) under Belgian law with the aim of representing the private sector in the contractual PPP. ECSO is a pan-European organisation which members include large companies, SMEs, start-ups,

research centers, academia, users and operators, associations, clusters and national, regional and local public administrations of Member States, EEA/EFTA countries and H2020 associated countries. ECSO will support all types of initiatives or projects that aim to develop, promote, encourage cybersecurity in Europe, and in particular to foster and protect the growth of the European Digital Single Market.

Back (http://www.ecs-org.eu/news)

About ECSO (http://www.ecs-org.eu/about)

News & Agenda (http://www.ecs-org.eu/news)

Membership (http://www.ecs-org.eu/membership)

FAQ (http://www.ecs-org.eu/faq)

Contact Us (http://www.ecs-org.eu/contact)

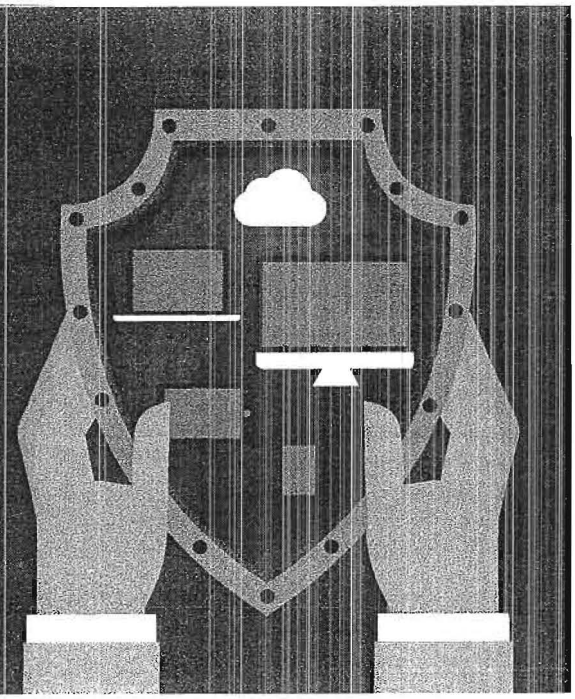
Follow us

(https://twitter.com/ecso_eu)

European Commission

EU cybersecurity initiatives

working towards a more secure online environment



5 July 2016

Since the adoption of the EU Cybersecurity Strategy in 2013, the European Commission has stepped up its efforts to better protect Europeans online. It has adopted a set of legislative proposals, in particular on network and information security, earmarked more than €600 million of EU investment for research and innovation in cybersecurity projects during the 2014-2020 period, and fostered cooperation within the EU and with partners on the global stage.

The Commission has further strengthened its approach in the past year by including cybersecurity at the heart of its political priorities: **trust and security** are at the core of the Digital Single Market Strategy presented in May 2015, while the **fight against cybercrime** is one of the three pillars of the European Agenda on Security adopted in April 2015.

Delivering on these strategies, the Commission today presented additional measures to boost the cybersecurity industry and to tackle cyber-threats.

The upcoming adoption of the **Network and Information Security (NIS) Directive** by the European Parliament expected tomorrow is another important milestone towards a more secure online environment

Why is cybersecurity so important?

Over the past years, digital technologies have become the backbone of our economy and are a critical resource all economic sectors rely on. They now underpin the complex systems which keep our economies running in, for example, finance, health, energy and transport. Many business models are built on the uninterrupted availability of the internet and the smooth functioning of information systems.

Cybersecurity incidents, be they intentional or accidental, could disrupt the supply of essential services we take for granted such as water or electricity. Threats can have different origins – including criminal, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

By completing the Digital Single Market, the EU could boost its economy by almost €415 billion per year and create hundreds of thousands of new jobs.

But for new connected technologies to take off – including e-payments, cloud computing or machine-to- machine communication – Europeans need trust and confidence.

The digital world should be protected from incidents, malicious activities and misuse. It is a priority for the Commission to help prevent these incidents, and in case they occur, provide the most efficient response.

Both governments and the private sector have a significant role to play - this is why the Commission works with all these actors to strengthen cybersecurity.

What are the key objectives of the Commission in the field of cybersecurity?

1. **Increasing cybersecurity capabilities and cooperation**

   The aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level.

2. **Making the EU a strong player in cybersecurity**

   Europe needs to be more ambitious in nurturing its competitive advantage in the field of cybersecurity to ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology, which is interoperable, competitive, trustworthy and respects fundamental rights including the right to privacy. This should also help take advantage of the booming global cybersecurity market. To achieve this Europe needs to overcome the current cybersecurity market fragmentation and foster European cybersecurity industry.

3. **Mainstreaming cybersecurity in EU policies**

   The objective is to embed cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids and the Internet of Things (IoT).

What is the Commission doing to strengthen cybersecurity?

The Commission has put forward several initiatives and is contributing to a series of key measures:

1. EU STRATEGIES

EU Cybersecurity Strategy (2013)

The Commission and the European External Action Service launched the EU Cybersecurity Strategy in 2013. The strategy outlines the principles that will guide the EU action in this domain – for example on the importance of access to the internet and of the protection of fundamental rights online. It sets five priorities:

1. increasing **cyber resilience**;
2. drastically reducing **cybercrime**;
3. developing EU **cyber defence policy** and capabilities related to the Common Security and Defence Policy (CSDP);
4. developing the **industrial and technological resources** for cybersecurity;
5. establishing a **coherent international cyberspace** policy for the EU and promote core EU values

European Agenda on Security (2015)

Fighting cybercrime more effectively is one of the three priorities under the new European Agenda on Security 2015-2020 which was adopted by the Commission in April 2015. Cybercrime requires a coordinated response at European level.

Therefore, the European Agenda on Security sets out the following actions:

- giving renewed emphasis to **implementation of existing policies on cybersecurity, attacks against information systems, and combating child sexual exploitation**;
- reviewing and possibly extending legislation on **combatting fraud and counterfeiting of non-cash means of payments** to take account of newer forms of crime and counterfeiting in financial instruments, with proposals in 2016;
- reviewing obstacles to **criminal investigations on cybercrime**, notably on issues of competent jurisdiction and rules on access to evidence and information;
- enhancing **cyber capacity building action** under external assistance instruments.

Digital Single Market Strategy (2015)

Trust and security are essential to reap the benefits of the digital economy. This is why the Digital Single Market Strategy presented in May 2015 includes a public-private partnership (PPP) on cybersecurity.

The goal of this partnership is to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, building trust between Member States and industrial actors as well as helping align the demand and supply sectors for cybersecurity products and solutions.

This partnership will be instrumental in structuring and coordinating digital security industrial resources in Europe. It will include a wide range of actors, from innovative SMEs to producers of components and equipment, critical infrastructure operators and research institutes. The initiative will leverage EU, national, regional and private efforts and resources - including research and innovation funds - to increase investments in cybersecurity.

Ultimately, the partnership will enable to:

- gather industrial and public resources to deliver innovation against a **jointly-agreed strategic research and innovation roadmap**;
- **focus on targeted technical priorities** defined jointly with industry;
- **maximize the impact of available funds**;
- provide visibility to **European research and innovation excellence** in cybersecurity.

The partnership will be supported by EU funds coming from the Horizon 2020 Research and Innovation Framework Programme (H2020) with a total investment of up to **€450 million** until 2020. The Commission aims at launching the first H2020 calls for proposals under the cybersecurity PPP in the first quarter of 2017.

Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016)

Delivering on the EU Cybersecurity Strategy and the Digital Single Market Strategy, the Commission adopted the Communication Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry on 5 July 2016.

It includes a set of measures aiming at:

- **Stepping up cooperation across Europe**: the Commission encourages Member States to make the most of the cooperation mechanisms under the forthcoming Network and Information Security (NIS) Directive and to improve the way in which they work together to prepare for a large-scale cyber incident. This includes more work on education, training and cybersecurity exercises.
- **Supporting the emerging single market for cybersecurity products and services in the EU**: for example, the Commission will explore the possibility of creating a framework for certification of relevant ICT products and services, complemented by a voluntary and light weight labelling scheme for the security of ICT products; the Commission suggests also possible measures to scale up cybersecurity investment in Europe and to support SMEs active in the market.
- **Establishing a contractual public-private partnership (PPP) with industry**, to nurture cybersecurity industrial capabilities and innovation in the EU (cf. above).

The Europol's Cybercrime Centre

The Europol's Cybercrime Centre (EC3) was set up in 2013 as integral part of Europol and has become a focal point in combatting and preventing cross-border cybercrime by:

- serving as the central hub for criminal information and intelligence;
- supporting Member States' operations and investigations by means of operational analysis, coordination and expertise;
- providing strategic analysis products;
- reaching out to cybercrime related law enforcement services, private sector, academia and other non-law enforcement partners (such as internet security companies, the financial sector, computer emergency response teams) to enhance cooperation amongst them;
- supporting training and capacity building in the Member States;
- providing highly specialised technical and digital forensic support capabilities to investigations and operations;
- representing the EU law enforcement community in areas of common interest (R&D requirements, internet governance, policy development).

4. EU FUNDING

Research and Innovation

During the 2007-2013 period, the EU invested **€334 million** in cybersecurity and online privacy projects. Topics such as trustworthy network and service infrastructures, cryptology and advanced biometrics were addressed under the 7th Framework Programme (FP7) and the Competitiveness and Innovation Programme (CIP). During the same period, the Security Research theme of FP7 invested **€50 million** in cybercrime projects addressing topics like the economy of cybercrime, risk analysis for infrastructure protection, money laundering and dedicated road mapping actions.

For the period 2014-2016, the EU has so far invested **€160 million** under the Horizon 2020 Research and Innovation Framework Programme (H2020) in cybersecurity research and innovation projects. The EU will also invest up to **€450 million** of H2020 funding to pursue cybersecurity research and innovation under the contractual public-private partnership on cybersecurity for the period 2017-2020.

Cybersecurity and privacy are part of two streams of the **Horizon 2020 programme**:

- Under the Societal Challenge **"Secure societies – Protecting freedom and security of Europe and its citizens"**.

  The **Digital Security** strand focuses on increasing the security of current applications, services and infrastructures by integrating state-of-the-art security solutions or processes, supporting the creation of lead markets and market incentives in Europe. Security is also a so-called "digital focus area" under other challenges (privacy and security in ehealth; energy; transport; innovative security solutions for public administrations). The aim is to ensure digital security integration in the application domains.

  The **Fighting Crime and Terrorism** strand focuses on increasing the knowledge of the cybercrime phenomenon - its specificities, its economy (including its unlawful markets and its use of virtual currencies) and the means for law enforcement authorities to fight it more efficiently and to prosecute offenders with more solid evidence from specialised forensic activities.

- Under **Leadership in enabling and industrial technologies** Projects on dedicated technology- driven digital security building blocks are funded (such as the 2014 calls on Cryptography and Security- by-Design). Security is also integrated as a functional requirement in specific technologies, such as the Internet of Things, 5G, Cloud, etc.