

CYSPA

PROTECTING EUROPEAN ORGANISATIONS
AGAINST CYBER THREATS



The Cyber challenge

Adjacent Digital Politics Ltd gives an overview of the EU Commission's Cyber Security Strategy and Commissioner Ashton's priorities to increase cyber security in Europe...

The internet and digital technologies play an integral part in society and the economy across Europe. However, network and information systems can be affected on a daily basis by incidents and malicious attacks. To help keep the online economy running and ensure consumer confidence, a high level of network and information across the EU is essential.

But, across Europe, cyber security incidents are on the increase and are becoming more complex. There are an estimated 150,000 computer viruses in circulation every day and 148,000 computers are compromised daily.

Cyber crime causes the majority of cyber security incidents and victims worldwide lose around €290bn each year. Figures show that by January 2012, only 26% of enterprises in the EU had a formally defined ICT security policy. ⁽¹⁾

Efforts by the European Commission to prevent such a loss have been growing, and the challenge to tackle cyber security is now at the forefront. In February 2013 the EU's Cyber Security Strategy – 'An Open, Safe and Secure Cyberspace', was launched, with a vision to prevent the growing problem of cyber attacks and crime.

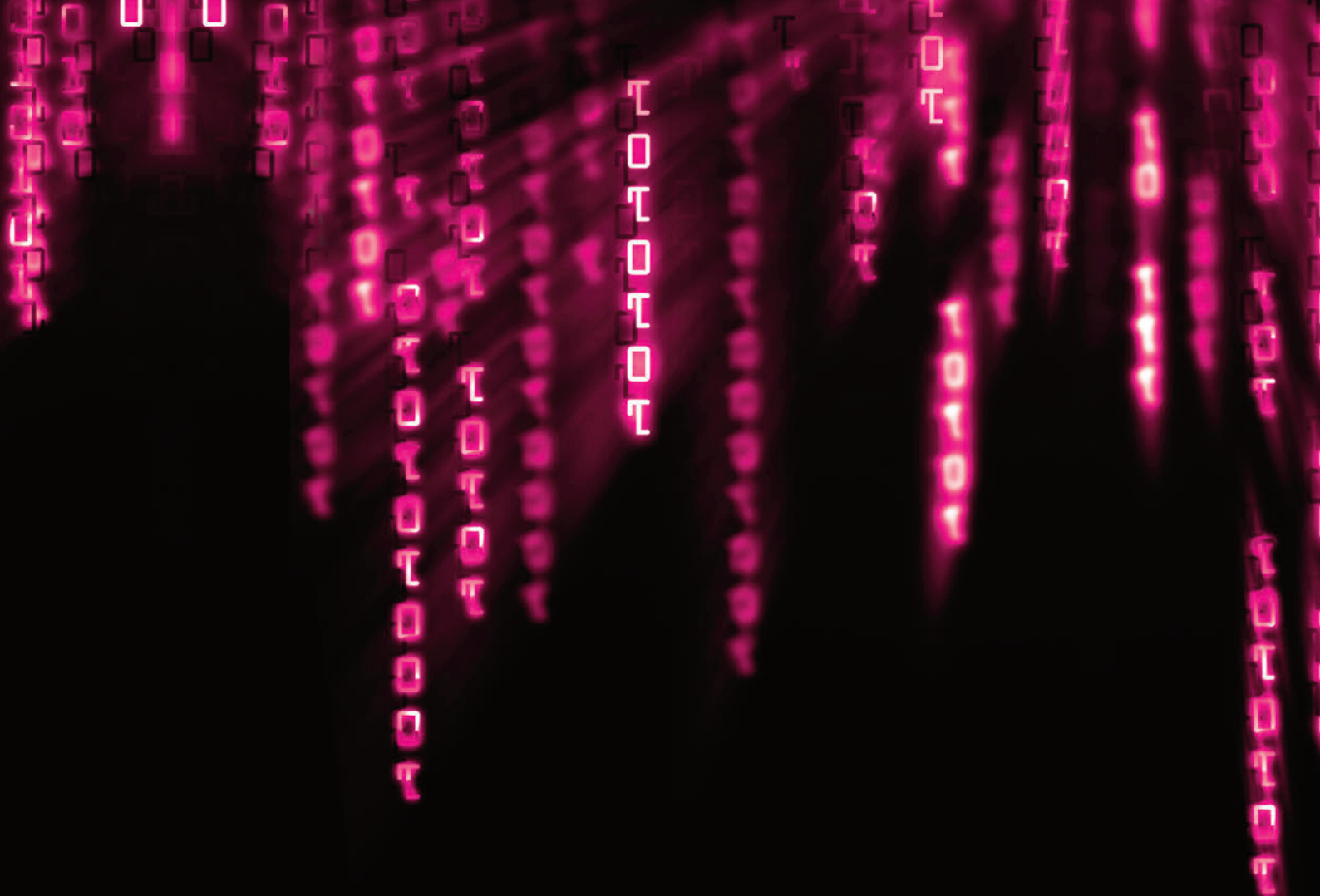
The strategy represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions, and communicates the EU's vision on cyber security with 5 priorities;

- Achieving cyber resilience;
- Drastically reducing cyber crime;
- Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
- Developing the industrial and technological resources for cyber-security;
- Establishing a coherent international cyberspace for the European Union and promoting core EU values.

Vice President of the European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Catherine Ashton, spoke at the launch of the strategy in February 2013, and said: "Cyber attacks on major international organisations and governments have become a daily reality. I would like to point particularly to the need to protect our children from those who would threaten or abuse them.

"This is unacceptable in any walk of life, and it is unacceptable in cyberspace too." ⁽²⁾

At the heart of the Commission's strategy is the firm belief that the protection of fundamental rights is as important in the virtual world as it is in the real world.



“For cyberspace to remain open and free, the same norms, principles and values that we uphold offline must also apply online. The European Union is determined to promote and defend its values online,” added Commissioner Ashton.

“For everyone to enjoy the benefits of cyberspace it has to remain free and open. It is a guiding principle of EU Cyber diplomacy. But we also have to recognise our responsibilities. We need to agree the norms of behaviour in cyberspace between countries.”⁽³⁾

As well as the strategy the EU has made key advances in better protecting citizens from online crimes, including establishing a European Cybercrime Centre; proposing legislation on attacks against information systems; and the launch of a Global Alliance to fight child sexual abuse online.

Commissioner Ashton commented that “Some important initiatives have already been launched to build trust and confidence between countries. There is a need to establish crisis communication lines and to enhance dialogues on cyber issues.

“Trust and confidence should be improved not only between states, but also between private and public sector. The Strategy we have launched sets out a number of priorities to improve IT systems, reduce cyber crime, and establish an international cyberspace policy for the EU.”⁽⁴⁾

Improving cooperation between different EU policy areas and working closely with international partners is key to ensure strategies such as this are successful. For example, the EU’s Digital Agenda sees internet trust and security as a vital element to a vibrant digital society.

“This means looking at how Member States can work better together and what the EU institutions and agencies can do to help them. It means improving cooperation between different EU policy areas, and promoting coordination between military and civilian sides,” explained the Commissioner.

“It means working closely with our international partners, the private sector and civil society. The expansion of the internet has been a success story. The new EU strategy is an important moment to work together for a safe, secure and free internet.”⁽⁵⁾

¹ http://europa.eu/rapid/press-release_IP-13-94_en.htm

²⁻⁵ http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/135287.pdf

CYSPA

The European Cyber Security Protection Alliance is a results oriented initiative set up by 17 organisations active in ICT.

Operating as a European project from October 2012 to March 2015, CYSPA is using this opportunity as the seed funding to launch an Alliance with a goal of self-sustainability beyond the end of the CYSPA project. The aim of the Alliance is to enable EU stakeholders to work together to articulate, embody and deliver the concrete actions needed to reduce cyber disruption, thereby increasing their capability to become a key actor in protecting their organisation against cyber risks.

A sector-based approach in e-government, energy, finance, telecommunications, and transport

CYSPA focuses on qualifying and quantifying cyber risks on a per-sector basis, helping organisations to understand their exposure and improve risk mitigation.

To support this, CYSPA delivers:

- An analysis of cyber threats impact across five sectors: e-government, energy, finance, telecommunications, and transport
- A technology and solutions observatory, enabling users to obtain up-to-date information about which approaches can be applied to the protection from specific cyber threats
- An integrated European strategy for the protection of cyberspace, consolidating the input and practical expertise built up by industrial and research communities in protecting from cyber threats

To deliver these concrete outcomes and enable the sharing and evolution of results, CYSPA members will benefit from a dedicated online platform (deployed during the first semester of

2014) allowing them to access CYSPA outputs, engage with other members of the CYSPA community, enrich the information, and share best practices to support secure operations in cyberspace.

CYSPA also directly addresses key challenges of Horizon 2020, in terms of:

- Increasing and consolidating the European industrial presence in the cyber security domain, a domain that is currently using a large number of non-EU solutions;
- Contributing to the societal challenge of an inclusive and secure society, by a better understanding of the impact of cyber disruptions;
- Providing solutions to better manage the risks and ultimately decrease the cost of cybercrime.

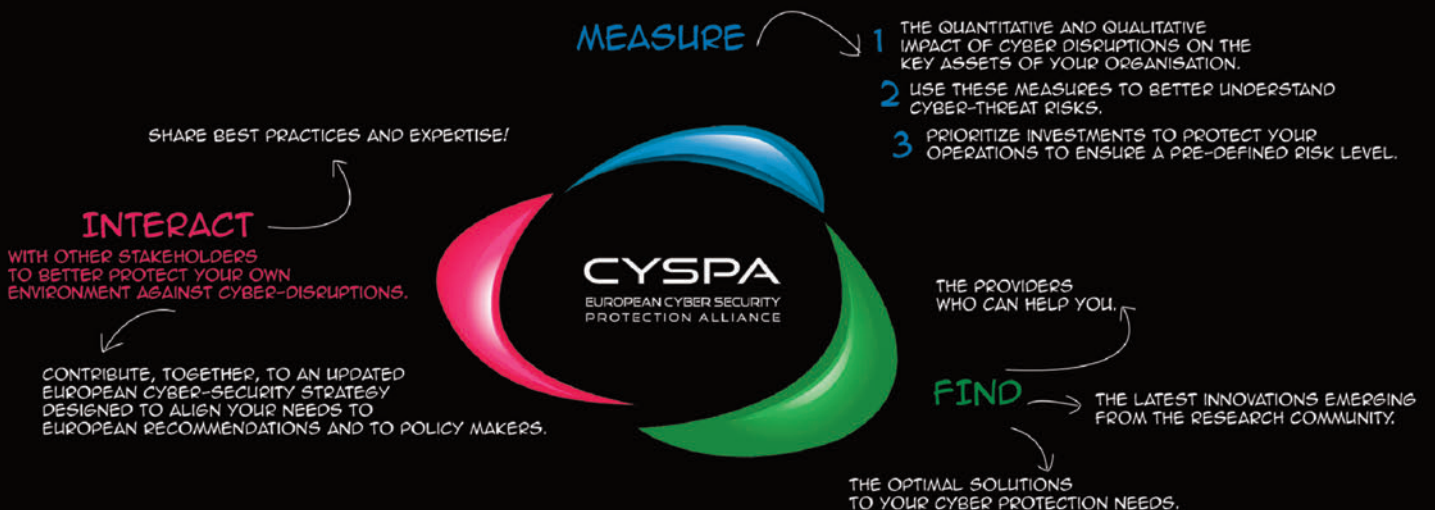
Delivering added value


CYSPA addresses a wide range of stakeholders, from public authorities to cyber security providers and users. The aim of the CYSPA Alliance is to create a community which enables industry, researchers, and operators across different economic sectors and public authorities to collaborate to protect themselves in cyberspace. By linking users and providers, CYSPA creates a unique network in which fighting cyber threats becomes a shared responsibility.

There are several benefits for each of these stakeholder groups in joining the CYSPA Alliance. In supporting the dialogue between users, providers and research institutions CYSPA can foster the collaboration needed to reduce the impact of cyber-attacks in each sector. CYSPA also provides the gateway for key stakeholder groups to communicate their needs at EU level and to provide input to European policy and initiatives.

For users, applying the Cyspa cyber risks evaluation methodology delivers an increased understanding of the impact of cyber threats within their own operating environment. The impact reports created in Cyspa on a per-sector basis using this methodology as well as the involvement of Alliance members operating in the same or similar contexts allows for an exchange of experiences thereby speeding up the process and improving protection against and mitigation of the effects of cyber disruptions.

For providers, the increased involvement of users as key actors in defining their desired level of cyber security protection is expected to create better defined and prioritised needs, thereby increasing the cyber security market and decreasing time to market for innovative cyber security capabilities. Through this increased user awareness and understanding, Cyspa will also give providers the opportunity to acquire a more in-depth understanding of users' key assets and, when feasible, involve users in testing innovations and pre-production solutions in industrial environments. Moving from market to policy contexts, Cyspa also benefits providers by operating as a single channel through which to convey messages and realities at European and national level.





Public authorities can benefit from an increased understanding of cyber risk posed to users across EU and a clearly articulated set of needs defined by users and providers and conveyed to the public authorities, thereby providing the authorities with direct access to needs validated by real users in operational contexts. As an Alliance, CYSPA can also bring in field-based expertise to validate proposed policies and directives, and more importantly, the feasibility of their implementation. Public authorities can also benefit from CYSPA as a means of sharing research needs across Member States.

A set of concrete activities open to members

The Alliance has created a dual level membership approach, with full and associate members.

Full members of the Alliance are expected to actively contribute to CYSPA objectives and, in that sense, each of the stakeholder groups can provide their own unique value and perspective within the Alliance. Users can make their application sector more visible through CYSPA and bring their needs to the European level, ensuring that these needs are part of the European cyber security strategy. Users can also bring in new sectors, in addition to the five sectors currently defined as the focus of CYSPA activities. Providers can create integrated solutions by interfacing with other providers and channel the latest innovations through CYSPA users. Public authorities can provide visibility to policies under elaboration through the CYSPA community and validate adoption paths for existing policies by showing their relevance to the different sectors.

What makes CYSPA unique?

Today, a staggering amount of information about incidents and threats, as well as the economic impact of those threats, is

disseminated. Thus, there is a lot of awareness regarding the dangers – but where information is much more scarce is on what to do about these dangers. This was the guiding line of creating CYSPA, the need to deliver a more personalised and solutions-oriented approach to organisations – and this is also what makes CYSPA unique in the current context.

CYSPA is working to empower each organisation to become THE key actor in increasing their level of cyber security, meaning that organisations need not only be aware of the problems but need to fully understand from where those problems originate within their own environment. This top goal in turn defines the directions in which CYSPA wishes to have a concrete impact, as well as the target beneficiaries of its actions.

Involving members in the CYSPA implementation path

CYSPA is committed to embodying its recommendations first within full member organisations, using the experience to then inform the wider community of associate members and beyond. CYSPA's membership aims to cover a unique mix of cyber security providers, public authorities and a range of user sectors from across Europe. This allows the modelling of market behaviours and gives a unique insight into the impact of potential actions. Moreover, CYSPA is industry led and its actions are impact and benefits driven, ensuring that they deliver concrete results to its members. As a European Alliance, CYSPA links together users and providers on a per-sector basis in order to qualify and quantify cyber risks, take action to mitigate cyber risk, and provide knowledge about the cyber threats most critical to each sector. CYSPA will also provide its members with a dynamic online repository of technology & solutions, which will be available through the community portal.



Join the CYSPA Alliance in 2014!

In order to initiate and consolidate European leadership in the context of CYSPA, the CYSPA Alliance will open to full and associate members beyond the initial 17 consortium partners currently collaborating within the CYSPA project.

The CYSPA Alliance will start its operations in 2014. An official launch event will be held, and the final date will be announced online on the CYSPA web site.

The founding members of CYSPA are:

European Organisation for Security, Engineering Ingegneria Informatica, Atos, Cassidian, BAE Systems Detica, Visionware, Elmar Husmann Unternehmensberatung, SAP, Selex ES, STM, Thales, Fraunhofer, TNO, University of Trento, Universidad Politecnica de Madrid, Telecom Italia, and Corte.

Interested in becoming a full or associate member of CYSPA? Please contact Nina Olesen (nina.olesen@eos-eu.com). Check out online at www.cyspa.eu.

TESTIMONIALS

“From viruses to theft of customer data, threats have never been greater. Fighting cyber threats is a shared responsibility. CYSPA equips IT providers with a unique network to sift out cyber security at 360° and more specifically per industry sector”

Jean-Christophe Pazzaglia, SAP

“CYSPA supports the dialogue between critical user industries, technical solutions providers, and cyber security research. In this context, CYSPA first of all acts as a supply of user industry insights and needs especially for research organisations”

Andreas Jakoby, FRAUNHOFER

“CYSPA offers access to a European community of transport actors working together to reduce the impact of cyber attacks in transport. With CYSPA, transport users can build a role model of best practices, shared at national and EU level”

Rémy Russotto, CORTE

“Being a member of CYSPA allows us to strengthen our relationships with user organisations across Europe, collaborate with a broad range of stakeholders to influence European policy and initiatives, and help to raise awareness of the need for good cyber security”

Arabella Whiting, BAE SYSTEMS DETICA

