ENISA's Role in the European Digital Single Market (DSM)

European Digital Market

ENISA's founding regulation provides that ENISA is assigned with tasks for the purpose of "… contributing to the establishment and proper functioning of the internal market. "[1]This document describes how ENISA can influence the growth of the cyber security market in Europe and thus support the IT-security level in EUROPE.

- European market for IT security is €20bn growing at 6% CAGR
  - There are 900,000 IT security professionals in Europe, forecast to grow at 6% p.a.
  - 7 of the top 37 global IT security companies are domiciled in Europe, generating global IT security revenues of €6bn

There is the opportunity to grow the cyber security market in Europe by up to €7bn, and enable value creation in the EU economy of up to €640bn by 2020.

- Cyber attacks are increasing in complexity and severity, with reported incidents growing at 41% p.a.
  - Aligning with global benchmarks could grow the European IT security market by up to €7bn p.a.
  - Matching North American spend on cyber security as a proportion of GDP would grow the EU cyber security industry by €7bn
  - Growing at the global average for IT security spend would increase the European market by €1.0bn to 2018
  - Achieving the same growth in cyber spend as a share of GDP as North America would increase the European cyber market by €0.4bn
  - Reducing shortage of talent within organisations could grow the workforce by up to 0.3m jobs in 2018
  - Revenues of companies domiciled in Europe could be increased by €1bn
- It is estimated that up to €640bn of potential EU economic is at risk depending on future scenarios: EU currently lags behind North America for technology adoption.

ENISA can influence both growth of the IT security market in Europe and enable significant value in the wider economy:

- ENISA can influence the European IT security market by increasing demand, reducing workforce shortfall and increasing revenues for companies domiciled in Europe
- ENISA can bring influence and transparency to achieve the potential value enabled by mature IT security in Europe by reporting leading and lagging metrics that describe how security is influencing adoption of value-adding technologies

[1] REGULATION (EU) No 526/2013 SECTION 1, SCOPE OBJECTIVES AND TASKS, *Article 1,*Subject matter and Scope: This Regulation establishes a European Union Agency for Network and Information Security (ENISA, hereinafter 'the Agency') to undertake the tasks assigned to it for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the establishment and proper functioning of the internal market.

I Messages

- ICT is the backbone every modern society, thus the EU needs to become **the single market of preference** for governments and industry where trusted core NIS technologies and services for industry and citizens are concerned (i.e. Trust in EU products and services).

- The EU needs an industry policy approach to create a competitive EU based ICT industry. ENISA can promote and support such an approach in the area of cybersecurity:
  - Promote cooperation of EU SMEs to compete together in global tenders.
  - Use public procurement[2] to foster EU based ICT industry by e.g. enforcing the requirement of standards and technical guidelines[3].
  - Further strengthen the EU position in areas like software, smart cards, cryptography.
  - ENISA should be an advisor in the Commissioner's Industry Advisory Group.

- ENISA provides advice on developing legislation, but is unique in its ability to support the implementation of legislation.
  - ENISA is by regulation involved in the implementation of the 2009 telecommunication package and the 2014 *eIDAS* Regulation[4].
  - ENISA is well positioned to support the Commission in implementing the NIS Directive and the cybersecurity component of the Digital Single Market (DSM) approach.
  - The Agency could also play a valuable role in supporting the upcoming General Data Protection Regulation.

- ENISA to become **the platform** to bring together public and private sector
  - ENISA to drive the content of the NIS platform and ensure alignment with its strategy and work program. This would result in more direct impact.
  - ENISA should be given an advisory role in H2020 and could also be charged with setting up a framework to ensure that H2020 ideas in cybersecurity result in commercial services and products.
  - ENISA to become a key advisor to standardisation committees.
  - Obligation to call upon ENISA to advise in EU in legislative processes.

- ENISA aligns the objectives and strategies of the Member States and Commission (DG CNECT).
  - ENISA to be involved in Commissions' communication regarding the Mandate extension.

[2] The public procurement market in the EU is estimated to be worth around one-sixth of total GDP in the EU.
[3] By competition! Currently there is no real incentive for investment in e.g. *common criteria* certified products
[4] REGULATION (EU) No 910/2014

II Cyber Challenges

When talking about cyber threats, it is usual to distinguish different categories:

Cyber Trust	EU citizens and business need to have the trust to make the best use of ICT.
Cyber Privacy	EU citizens need to have the confidence that all their online activity is protected in line with the principles set down in the EU law.
Cyber Crime	Crime on the internet has a new dimension. Modern technology allows organized crime to scale their "business", especially outside the legal boundaries of states.
Cyber Espionage	Military/state/industrial espionage has existed for thousands of years. The only difference between traditional espionage and cyber espionage is the use of technology and as long as we have civil intelligence agencies it will not stop. Another aspect is espionage because of philosophical disagreement[5].
Cyber Sabotage	The disruption if IT based infrastructure (e.g. Stuxnet).
Cyber Warfare	A new type of asymmetric warfare with a new paradigm and no taxonomy.

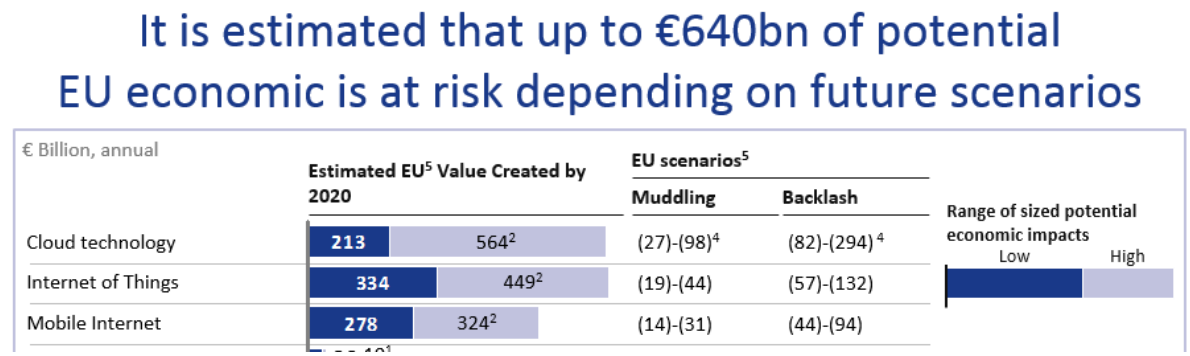
The challenge is that from a threat perspective the one who is attacked cannot on first sight analyse the origin of the threat. Also, the governments still are organized in silos: i.e. Ministry for Defense, Ministry for Economy, Ministry for Interior, etc.

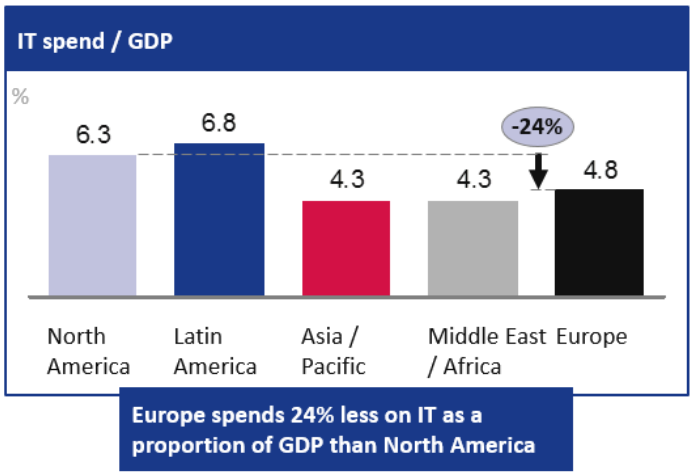
[5] e.g. some countries see industrial espionage as part of their social behaviour

III.EU and the Internet/ICT Industry

ICT is the backbone of every modern society, and here the EU needs to become the single market of choice for governments and industry, where trusted core NIS technologies and services for industry and citizens are concerned (i.e. Trust in EU products and services). However, over the past 15 years Europe has lost its leading position in ICT technology. All the new global players, such as Amazon, Google, Facebook, Twitter, Cisco, etc. are from the United States. In addition, Chinese companies like Alibaba, Baidu, Tencent, Huawei, etc. have sprung up in the last 10 years with the same or similar business models as US companies. "Old" companies like IBM, Microsoft, HP, etc. still dominate the market. This leaves only a few big players from the EU such as SAP or Nokia, the latter owned and strongly influenced by Microsoft. This problem needs to be urgently addressed.

The EU should seek to achieve a reasonable balance between measures that are derived from strong ethical principles and measures reflecting current business practices that could more effectively stimulate economic growth throughout the EU.





IV. Issues & Proposed Solutions

#1

Current attempts to improve NIS throughout the EU often do not achieve an optimal balance between opportunity and risk. This reduces the effectiveness of the overall approach and increases costs for both the public and private sector.

ENISA produces Threat Landscape Reports and its working with relevant stakeholders

Explanation

- There is no EU strategy for developing pool of competence that would establish the EU as leaders in the field of cybersecurity.
- Current approaches to NIS throughout the EU concentrate on reducing risk rather than looking at what level of risk is compatible with the business opportunity.
- Companies often set very risk-averse security policies at the board level, but need to take risk in practice in order to benefit from market opportunities. This leads to a reactive approach where companies spend a lot of money to close audit points.
- Security is perceived as a cost and not as an enabler.

How ENISA can make a difference

- Assist the Commission and the Member States in ensuring that EU cybersecurity strategy and EU industrial policy are strongly aligned. Identify areas where the EU is well positioned to be a global leader and assist in defining long-term plans for building up these competencies.
- Promote industry to reason in terms of the balance between opportunities and risks and not just to concentrate on risk.
- Develop the ENISA Threat Landscape on a sectorial basis.
- Ensure that public policy can be implemented in an economically efficient way by promoting those good practices that are economically efficient.
- Place more emphasis on solutions for SMEs and small market players.
- Define and implement a wide-reaching programme of security evangelism to ensure that key messages spread between all sections of the community.

#2

The internal market for security products and services is not functioning correctly. The EU security market is dominated by US companies and functions on a 'supply push' principle rather than a 'demand pull' principle.

ENISA is working closely with the key stakeholders to support development of policy to address these challenges.

Explanation

- The EU market for security products and services is dominated by non-EU companies.
- Economically, in risk terms, if Europe cannot provide confidence to enterprise and citizens on security then €640b of economic value is at stake.
- The market is not an efficient market – it works by 'supply push' rather than by 'demand pull'.
- Security is seen more as a cost centre than a business requirement. Budgets are therefore kept to a minimum as they are not seen as contributing to the bottom line.
- EU NIS policy has traditionally concentrated on the telecommunications sector, whereas increasingly security issues are becoming associated with the applications and services that use this infrastructure. It would make more sense to talk about 'critical information services' than 'critical information infrastructure'.
- There is a gap in the market security needs to be more targeted for SMEs.

How ENISA can make a difference

- ENISA has developed a strong network of stakeholders in both the public and private sector and can call upon these at any time to support policy initiatives. The ENISA approach to working with its stakeholders greatly increases the scalability of its operations and results in a feeling of 'ownership' and a high level of buy-in.
- Update the Commission's 2009 study on the security market and provide targeted recommendations for improvement.
- Stimulate 'collective demand' by getting different industry sectors to define security requirements on a sector-by-sector basis. Use these requirements to drive procurement policies in these sectors.
- Assist the Commission in broadening the scope of current CIIP policy to other industry sectors. Produce a roadmap and assist in implementation.
- Work together with industry to define and disseminate approaches to security adapted to the needs of SMEs. Actively promote the uptake of such methods (e.g. by using the representative committee referred to above).

#3

The area of privacy and data protection is moving from a legal and principle-based debate to an implementation phase. The EU has a strong policy in this area but is very weak in terms of implemented solutions.

ENISA is engaging with the key stakeholders in this area identifying solutions and is supporting implementation

Explanation

- The revelations of Snowden have brought the issues of privacy and data protection into the public spotlight. The EU needs to deliver concrete results to back up its ambitious proposal for a new legal framework.
- Current processes and tools for managing privacy and data protection need to be greatly enhanced if we are to achieve the goals of this legislation. It would be a mistake to wait until the legislation has been adopted to start working on the processes and tools needed to implement the proposal.
- If the implementation details are not well thought out, there is a real danger that the EU will implement policies in a 'business unfriendly' manner, thereby potentially reducing the competitiveness of EU industry.
- This area could also be an opportunity for EU business, allowing it to develop an expertise that is underdeveloped in the global market place.

How ENISA can make a difference

- Identify existing methods and tools that could be used to implement the proposals of the regulation. Suggest which methods and tools could provide the best cost/benefit based on current operational experience.
- Identify 'gaps', where current methods and tools do not fulfil the requirements of the legal proposal. Identify the requirements that need to be met and provide them to industry and to R&D programmes (e.g. H2020).
- Help the Commission and Member States to move the privacy and data protection debate towards implementation strategies.
- Provide feedback to those working on the legislative framework as to what is feasible and what is not feasible from an operational perspective.

#4

Current EU research & development activities are not giving rise to successful services and products in the EU Network & Information Security.

ENISA can brings its expertise and knowledge to supporting initiatives such as H2020 and CEF

Explanation

- We are lagging behind the US in terms of security-related products – this is a fact.
- Whereas we developed a lead in certain areas in the past (e.g. EU cryptography) this has now been lost as the US has adapted its policy on cryptography to support its industry.
- EU research in security is of a high standard, but it does not result in products and services – there is a 'process gap' linking EU R&D in security to industry.
- H2020 now includes innovation as a goal, but it has a wide scope and will need to be actively supported by other EU mechanisms if it is to succeed.
- The funding models in the EU need to be adapted to the current economic environment. We need new models for venture capital (such as crowd funding).

How ENISA can make a difference:

- ENISA should implement a security 'Technology Watch' with the goal of identifying promising NIS technology developments before other global powers.
- Assist the EU in leveraging the position of 'trust' that the EU has developed over the last few years to support our security products (we are not weakened by Snowdon type revelations or human rights issues).
- Work together with universities and EU companies specialising in security to define and implement a framework for rapid implementation of EU research ideas in industry environments. Ensure a feedback mechanism to enable research to improve products together with industry.
- ENISA should be given a stronger role in participating H2020 projects in the area of NIS. In order to achieve scalability, the ENISA regulation should be changed so as to allow the Agency to receive funds for this.
- ENISA should promote ideas that support EU security products without naming them – this could be done on the basis of concepts where we have stronger implementation.
- Participate in important conferences outside the EU to influence the way in which NIS is perceived in favour of the EU approach.

#5

Standardisation and certification activities are not sufficiently aligned with modern needs of the industry.

ENISA can use the Cyber Security Coordination Group to ensure that standards are aligned with industry needs.

Explanation

- Proprietary standards increase the cost for the consumer and can result in 'lock in' to particular products.
- Standards are the basis of interoperability. If the EU does not develop the right standards it will not benefit from interoperable products.
- Currently, industry is not the major driving force behind new standards, which may reduce their level of buy-in to the final result.
- Technical guidelines developed with EU ICT companies give them a competitive advantage.
- Existing certification schemes are under-utilised:
    - for products e.g. "Common Criteria[6]"
    - for infrastructure e.g. "BSI Baseline Protection"
    - for Cloud computing e.g. ENISA's Cloud Certification Schemes List (CCSL).

How ENISA can make a difference

- ENISA should proactively foster the development of relevant standards by active participation in ISO, ETSI, CEN/CENELEC and other relevant standardisation groups.
- Use the Cyber Security Coordination Group to ensure that standards are aligned with industry needs. Use best practice as a precursor to standards in order to speed up implementation.
- Promote the development of technical guidelines for security in promising areas of innovation (e.g. Smart Cities, Internet of Things).
- Promote certification schemes by active contribution to initiatives such as the SOGIS[7] group and facilitate industry involvement.

[6] http://www.commoncriteriaportal.org
[7] http://www.sogisportal.eu

#6

Knowledge and skills related to network and information security are developed and maintained in a fragmented manner. There is no coherent approach for educating citizens, private sector and government.

ENISA will continue promote IT Security behaviour via national associations to outreach to citizens by building on initiatives such as the Cyber Security Month

Explanation

- Legislators need to understand the impact of their regulation. Technology impact assessments should become obligatory.
- Industry must understand threats and risks and must be capable of maintaining this knowledge in the long-term.
- Citizens must understand the consequences of their behaviour, surfing on the internet, buying in online shops, doing online banking.

How ENISA can make a difference

- Work together with schools, universities and professional associations to create a coherent framework for raising awareness and education in NIS. Assist industry in aligning skill sets with career paths.
- Organise events in Brussels where ENISA experts inform Politicians in legislative processes on security in the corresponding field (e.g. Cloud Computing, Data protection and privacy, etc.).
- Educate CISOs (e.g. ENISA risk methodology, ENISA Threat Landscape).
- Promote IT Security behaviour via national associations to outreach to citizens by building on initiatives such as the Cyber Security Month and the DsiN Cloud Scout[8] in Germany.

[8] https://www.sicher-im-netz.de/dsin-cloud-scout-der-cebit-2013

#7

The EU has Agencies in the area of ICT and security like EU Lisa, Frontex, Europol/EC3, CEPOL, Eurojust, EEAS, EDA, ENISA.

ENISA will work to ensure that all activities of these Agencies are complementary to one other to effective respond to the overall cyber challenges.

Explanation

ENISA is well integrated in the EU approach to Cybersecurity, but could take a more proactive role in ensuring effective and efficient information exchange between other EU agencies and bodies. The Agency could also act as coordinator for all activities in other agencies related to cybersecurity preparation.

How ENISA can make a difference

- ENISA to coordinate the NIS and cybersecurity activities of all EU agencies in line with existing policy statements in order to ensure a coherent approach across all communities.
- ENISA to advise the key Steering Committees and Advisory Boards for all Agencies and bodies involved in NIS as well as for all major NIS initiatives launched by the EU.
- ENISA to advise the key Steering Committees and Advisory Boards of Industrial Consortia that have a role in improving NIS.
- ENISA to influence policy development and implementation by being recognized as the focal point for NIS and cybersecurity for both the public and private sector.
- ENISA can strengthen the role and coordination of the CSIRT across Member States and EU institutions.

Support from the Commission

- The Commission should ensure that future EU policies, legislation and programmes recognize the central coordination role of ENISA in ensuring a coherent approach to cybersecurity across the EU, both in terms of Member States and in terms of communities.
- The Commission should actively support ENISA in its effort to be present on the key Steering Committees and Advisory Boards for all Agencies involved in NIS as well as for all major NIS initiatives launched by the EU.
- The Commission should promote ENISA as the focal point of NIS and cybersecurity.

IV Summary

The Agency has a number of 'flagships', which can be used as a platform for launching new, more ambitious services to support the Commission, Member States, EU Institutions and EU Citizens. Examples include the Pan-European Cybersecurity Exercises, the ENISA Threat Landscape, support for implementation of Security & Data Breach Notification obligations, the EU Cybersecurity Month and the work that ENISA has done in supporting the CSIRT community in the Member States and EU Institutions.

ENISA is ready, willing and able to:

- Assist the Commission and the Member States in ensuring that EU cybersecurity strategy and EU industrial policy are strongly aligned.

- Identify areas where the EU is well positioned to be a global leader in NIS and assist in defining long-term plans for building up these competencies.

- Stimulate 'collective demand' for NIS services and products by getting different industry sectors to define security requirements and drive procurement on a sector-by-sector basis.

- Encourage industry to balance opportunities and risks and not just to concentrate on risk, enabling businesses to improve business models (scalability, flexibility, agility).

- Promote approaches to security adapted to the needs of SMEs. Establish a representative group of SMEs to act as a communication channel for security issues dedicated to the SMEs in the EU.

- Actively promote implementation activities to support the new proposed privacy and data protection legislation so as to avoid an 'implementation gap' once the legislation is passed.

- Work together with universities and industry to define and implement a framework for rapid implementation of EU security research ideas in industry environments. Ensure a feedback mechanism to enable research to improve products together with industry.

- Use the Cyber Security Coordination Group to ensure that standards are aligned with industry needs. Foster the development of relevant standards by active participation in relevant standardisation groups.

- Work together with schools, universities and professional associations to create a coherent framework for raising awareness and education in NIS. Assist industry in aligning skill sets with career paths.