enisa

THE EU CYBER SECURITY AGENCY

PRINCIPLES AND OPPORTUNITIES FOR A RENEWED EU CYBERSECURITY STRATEGY

ENISA's contribution to the Strategy review

VERSION B I JULY 2017

Foreword by the Executive Director

We are in 2017, 10 years after the cyber attack targeting Estonia[1] and 4 years after the Snowden[2] revelations of 2013. The scandal of the just recently revealed hacked emails before the French election has shown that our core values, our democracy is at risk.

Are we prepared to address the challenges arising from new threats and the new hybrid threat landscape in cyber space?

In 2009, the European Commission published the Communication on Critical Information Infrastructure Protection (CIIP)[3]. In the following years, COM launched several strategic level documents[4]: the EU Cybersecurity strategy in 2013, the European Agenda on Security in 2015, and the Digital Market Strategy; furthermore, in 2016, a Joint Framework on countering hybrid threats was published and the cPPP initiative was launched. The European Parliament and Council adopted in 2016[5] the General Data Protection Regulation (GDPR), Law Enforcement Authorities (LEA) data protection Directive, the Passenger Name Records Directive and the NIS directive. These initiatives demonstrate that political awareness results in political action.

On the implementation side, ENISA was established in 2004 to support the security of network and information systems across the EU, and its mandate was renewed in 2009 and 2013. Even with its limited resources, of about €11 million/year, ENISA has published and covered nearly every upcoming topic relevant for cybersecurity and cyber space. Examples of published reports include[6] the ENISA Threat Landscape, activities on cybersecurity exercises, reports on Smart Airports, Smart cities, eHealth, to name a few.

However, this is not enough!

New topics such as Industry 4.0, Robotics, growth in Artificial Intelligence, the Internet of Things, the Internet of People are now beginning to be deployed and are changing manufacturing and the lives of EU citizens. These technologies will have a significant societal impact. Europe and its digital single market needs to be ready to adopt, explore and apply the benefits from these technologies in a safe and secure cyber environment.

EU cybersecurity market grows slower than possible. In 2016, the EU cybersecurity market was estimated at €20.1bn and compares favourably with the cybersecurity market of other global regions. The Compound Annual Growth Rate (CAGR) of the EU market however is 6%, whereas the average growth rate is around 8%, and is growing slower than all other major regions.[7]

---

[1] 2007 cyberattacks on Estonia, available at: https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[2] Edward Snowden, American whistleblower and former National Security Agency contractor, available at: https://en.m.wikipedia.org/wiki/Edward_Snowden
[3] COM(2009) 149 final
[4] JOIN(2013) 1 final, COM(2015) 185 final, COM(2015) 192 final, JOIN/2016/018 final, COM/2016/0410 final
[5] Regulation (EU) 2016/679, Directive (EU) 2016/680, Directive (EU) 2016/681, Directive (EU) 2016/1148
[6] ENISA website: https://www.enisa.europa.eu/publications
[7] Cybersecurity as an economic enabler, ENISA, 2016, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler, p1

We see an increase in monetisation of cyber crime, crime as a service and of targeted attacks. Targeted attacks, like ransomware, entered the top ENISA 2016 cyber threats. According to the ENISA Threat landscape[8], in 2016, ransomware was the primary element for the manifestation of monetization of the activities of cyber-criminals, with an estimated loss of one billion US $ for the entire year 2016. More recently, the WannaCry ransomware campaign caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 230,000 systems[9]. Next to ransomware, information theft is the main area of 'malware innovation' in 2016. Targets affected included political organisations and democratic institutions[10].

We become more aware that our rights online and even our democracy are at risk. The scandal of hacked emails[11] in the US election in 2016 and the measures taken in Europe to prevent interferences in elections[12, 13, 14] cannot be ignored and are other examples that show us that there is more to be done to address the continuous changing landscape of threats and challenges in cyber space.

Small devices, which we sometimes forget are connected to Internet, are used to build very large cyber attacks affecting targeted businesses and infrastructures. In October 2016, the Mirai botnet[15] compromised IoT devices and household routers, where cases are documented that life was at risk because normal emergency telephone calls were not accessible. This raises the question of who is liable in such events.

Cyber space can be used for sabotage, espionage and warfare. Hybrid warfare (adding cyberwarfare to conventional and unconventional warfare tools) is evolving without necessarily using the word 'war' in describing the attacks. Some countries are already taking steps to combat these threats[16].

We see specialized institutions and bodies investing in activities related to cybersecurity. I would say that at this time, at least at the institutional level there is a relatively good understanding of the need for strong cybersecurity. However, given the limited resources and budgets a coordinated approach is required to make sure we do not fail in our mission. Now it is a good moment to ask ourselves some questions, and based on the replies to see how we can improve the context and go to the next stage/level of preparedness and readiness to address the emerging challenges.

I would like to list here some of the questions where I believe that the answers are not fully addressed:

---

[8] ENISA Threat Landscape Report 2016, ENISA publications covering threat landscape are available at: https://www.enisa.europa.eu/topics/threat-risk-management?tab=publications

[9] ENISA, WannaCry Ransomware Outburst, May 2017, available at: https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

[10] German parliament foiled cyber attack by hackers via Israeli website, 29/03/2017, available at: http://www.reuters.com/article/us-germany-cyber-idUSKBN1701V3

[11] Hillary Clinton Email Archive on WikiLeaks, available at: https://wikileaks.org/clinton-emails/emailid/30373

[12] Russian cyber-attacks could influence German election, says Merkel, The Guardian, available at: https://www.theguardian.com/world/2016/nov/08/russian-cyber-attacks-could-influence-german-election-says-merkel

[13] France's Hollande seeks 'specific measures' against election hacking, Politico, 15/02/2017, available at: http://www.politico.eu/article/frances-hollande-seeks-specific-measures-against-election-hacking-russia-putin/

[14] Dutch will count all election ballots by hand to thwart hacking, The Guardian, available at: https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking

[15] Dyn Analysis Summary Of Friday October 21 Attack, October 26th, 2016, available at: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[16] European Centre of Excellence for Countering Hybrid Threats established in Helsinki, Finnish government site, Government Communications Department, on 11.4.2017, available at: http://valtioneuvosto.fi/en/article/-/asset_publisher/10616/eurooppalainen-hybridiuhkien-osaamiskeskus-perustettiin-helsinkiin

- How do we adapt current security approaches to deal with the timescales and scale of deployment of new technologies such as IoT?
- Are we addressing all the needs for cybersecurity of all communities and, in particular, EU citizens? Are our human rights respected online? Are we as citizens protected enough?
- Are our critical infrastructures well prepared for the threats in cyber space?
- Do we have enough human and financial capacity to address the threats to the digital single market?
- How can we create and implement trust models that will enable us to take full advantage of the benefits of digital single market?
- How can we ensure that the EU has access to the cybersecurity skills and experience needed to thrive in a rapidly evolving threat environment?
- Do the roles and responsibilities currently defined across the EU enable us to prepare for and respond to cyber sabotage, cyber espionage, cyber warfare?

As already mentioned at the beginning of this section there are several policies, actions, and institutions already addressing the challenges. ENISA is one of them. In our position as the EU cybersecurity agency, we see this time as a good opportunity to present our vision, to contribute to the discussion on how to make more efficient and more effective use of the resources to address the cyber challenge.

The EU cybersecurity strategy is now under review; this paper identifies some principles, and opportunities that ENISA considers should be addressed in the new version.

The key issues addressed in this paper include:

- Programs should be put in place, at the earliest opportunity, to prepare and assess the likely impact of new disruptive technologies. Specific assessments need to be made in respect of each technology from a technical, political and societal perspective. Following these assessments, the need for new policies and legislative initiatives needs to be addressed.
- European industry, governments and citizens should have access to competitive secure and trustworthy products and services that allow data and service portability and do not depend on single (monopolistic) service providers.
- Member States should further invest in security awareness training and cyber hygiene. This includes promoting cybersecurity as a career choice in schools and universities, encouraging industry to develop cybersecurity training schemes that are aligned with established career paths and encouraging the retraining of adults and long life learning programs in this area.
- The EU, supported by institutions like ENISA, should be proactive in addressing the challenges of existing and emerging technologies by assessing the risks and providing mitigation solutions and policies to secure EU growth and compliance to EU values and norms.
- Europe should seek to be the early adopter of standards so that Europe is driving the marketplace rather than being pushed by vested interests.
- The EU should foster research, innovation and education for the delivery and operation of a digital space and a single market economy with trusted digital products and services.
- The EU should mandate a lead agency in the area of cybersecurity to work closely with all relevant stakeholders at EU level.
- The EU and its MS should maintain a high level of autonomy and sovereignty while having an open market with reliable and trustworthy products and services.

Please take this paper as our contribution to the discussion for the review of EU cybersecurity strategy.

Udo Helmbrecht, Executive Director ENISA

Table of Contents

1. Introduction

The EU Cybersecurity Strategy (2013)[17] is already 4 years old. Given the speed of developments in the cyber world during the last few years it is a good time to review the 2013 strategy.

In the last few years, there have been many new developments in the cyber world. We continue to witness the digitalisation of our daily lives, the development of new technologies, new threats and new stakeholders. The words cybersecurity, cyber warfare, cyber espionage, cyber terrorism and cyber defence are increasingly referred to in daily conversation by our citizens and politicians. Some new concepts that have emerged in the last few years include fake news, cyber ethics, cyber diplomacy and digital sovereignty.

From a technical perspective, we have new technologies changing the cyber landscape. The Internet of Things/ Internet of people is now being deployed with an estimated 20 Billion devices expected to be operational before 2020. Robots, Artificial Intelligence and Block Chain technologies are emerging as disruptive technologies and are beginning to affect our daily lives. Traditional approaches to security will have to be adapted in order to cope with issues of scalability and modified timelines.

The ENISA Threat Landscape Report of 2016 highlighted the growth in the traditional cyber challenges where we have witnessed the increased complexity of cyber incidents, the monetisation of cybercrime such as growth in ransomware, cyber espionage, advanced persistent threats and attacks on critical infrastructure.

ENISA has prepared this paper with the aim of stimulating the discussions and development of a new EU cybersecurity strategy which will serve the needs of the Digital Single Market, deliver economic growth and mitigate the cyber challenges of the future.

The reader is also referred to another recently published paper[18] by ENISA where the vision of the Agency for its role in securing cyber space is presented.

This paper is divided into two major parts.

The first part of this paper proposes a set of principles to be included in the reviewed EU cybersecurity strategy, with an emphasis on a comprehensive approach to addressing cybersecurity challenges, at all levels, from addressing the citizens/consumers' needs to the societal needs.

The second part presents a list of opportunities and recommendations for consideration in the revised strategy, that reflects the maturing of the cyber landscape in Europe in the last few years and proposes new structures and approaches to serve better the EU cyber challenge in a more efficient way.

[17] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber space, JOIN(2013) 1 final, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

[18] ENISA, ENISA's input to the mandate renewal discussion, version B, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-input-to-the-mandate-renewal-discussion

2. Cybersecurity and layers of protection

Cybersecurity operates on many different levels and one of the functions of the strategy should be to address coherently all the different levels of cybersecurity needs.

The following image draws on the Maslow's Pyramid of needs approach to categorising cyber space and cybersecurity needs in a hierarchical way. Any EU strategy must cover all aspects of the cybersecurity to ensure a comprehensive approach to addressing the cyber challenges of tomorrow.

Figure 1. Layers of cybersecurity needs.

Figure 1 presents ENISA's perspective on cybersecurity needs, starting with EU core values at the top, and, working the way down, to the basic citizens' needs.

The following paragraphs provide a short description of the pyramid and the layers as cybersecurity requirements.

Layer 1. Basic security protection. Safety and security of citizens in cyber space is not a matter of debate. Under no circumstances, the safety of users should be at risk due to actions in cyber space. Furthermore, preventive measures should be applied; education, awareness and cyber hygiene are very important. As you wash your hands to protect your health, or lock the door of you home to protect your properties, in the cyber space, you also have to be aware of the risks. Thus, every user should be aware and should be using minimum-security protection actions: firewalls, malware detection, apply updates and patches to safeguard devices and IT systems.

Layer 2. Critical asset protection. The Network and Information Security (NIS) directive brings new security requirements for protecting essential services and digital services in the EU. These requirements are the most recent ones; since past decade, several communications addressed the need for Critical Information Infrastructure Protection (CIIP)[19]. The implementation of NIS directive is an important step in protecting EU CIIP, the cooperation of CSIRTs via the CSIRTs network, the improvement of EU collaboration via the Cooperation Group, etc. Secure infrastructures in sectors like energy, transport, banking etc. provide bases for the society to function and for economy to grow.

Layer 3. Digital single market protection. The cyber space and technology evolution provide many opportunities for business development. Besides critical infrastructures, all business needs to be protected as their reliance on cyber space is increasing. The exposure to cyber space related threats like cyber attacks, cyber crime, cyber sabotage and/or cyber espionage becomes more visible every day and is visible in media almost daily. Security measures should be deployed and an EU approach is needed to address and support business in general and SMEs in particular in their cybersecurity needs.

Layer 4. Global stability protection. Espionage and war have millenniums of history. Cyber space associated terms are already in place; several actions during the past decade were assessed as cyber war, cyber espionage etc. There are several discussions on the need for cyber norms and cyber diplomacy. Cyber defence activities are funded and developed across the globe. Given the nature of cyber space, adequate measures and international agreements need to be in place to guarantee global stability in front of risks. The EEAS activities, the Tallinn manual, etc. are good examples of activities at this level that need to be supported and extended.

Layer 5. Democracy and human rights protection. Safety vs security balance is changing in the global physical world. Some emerging technologies (autonomous vehicles, etc.) – require new discussions on the ethical aspects. Human rights protection online is not an easy objective to achieve. Protection of the core EU values online needs to be guaranteed in the cyber space. Impact of new technologies, products and services needs to be assessed and adequate measures should be in place – i.e. any new technology should preserve rights, liberties and democracy.

There are interdependencies between the layers described above. Protection of the critical assets, i.e. critical information infrastructures provides a good base for other businesses, part of the digital single market, to flourish while supporting citizens' needs as well. Cybersecurity for citizens, infrastructures and business, in current context, cannot be achieved without addressing the challenges associated with globalisation. In the globalized context, cyber diplomacy needs to be in place, as well as the means to prevent, defend and protect the EU, its citizens, infrastructures and businesses. Furthermore, it should be noted that core EU values and norms, ethics, need to be applied to all levels in the cyber space: to all products and services available for EU customers, independent of their place of production/development in the world.

The principles listed in this paper apply to all the level of needs in the cybersecurity (pyramid). Some of the opportunities listed in the next sections apply to one or more layers of security requirements presented in figure 1.

[19] COM(2009) 149 final, COM(2011) 163 final

3. Guiding principles

The guiding principles listed in this section are meant to support development of a comprehensive strategy.

3.1 The same EU core values apply in the digital world as in the real world

The Treaty on the European Union (aka the Lisbon Treaty) sets the legal framework that reflects our core values and principles in Europe. There is a clear need to protect our fundamental rights, which include freedom of expression, personal data and privacy. Emerging / disruptive technologies are now raising new challenges and there is a need to interpret existing legislation in the context of these new technologies.

The basic principles of security by design, privacy by design and ethics by design need to be addressed in the cyber world of tomorrow. Similarly, at the implementation level, industrial processes for producing hardware and software need to be adapted to respond to new challenges, such as supply chain security and ensuring quality in software systems deploying hundreds of millions of lines of code (Industry 4.0). Where and how far the duty of care principle will extend to protect our core values will continue to be reviewed by the courts. Recent discussions in relation to data privacy and the proposed Privacy Shield to address differences between US and EU approaches to privacy remain to be tested and validated by the courts.

Imminent commercialization of autonomous systems (i.e. robots) and Artificial Intelligence are competing to deliver many functions previously reserved for humans. Software now needs to address and be programmed to make the same decisions as humans have done for centuries. Where humans are held responsible for their decisions and actions in a court of law, the next generation of robotics and autonomous machines, which will be executing the actions of tomorrow, will have to be examined in a different way. An example of a possible difficult decision is how an autonomous driving vehicle would be programmed to react to a potential head on collision with another vehicle. Will the vehicle maintain its path or will it swerve to avoid a collision but potentially putting other road users at risk? These technology developments raise questions about software liability and how liability will be addressed in this type of situation or when software is compromised by malware, which is subject to exploiting a vulnerability or a deliberate sabotage of the software.

The new EU cybersecurity strategy needs to address these types of challenges and foster policies to ensure that our economy is ready to embrace these emerging technologies and benefit from the economic and social opportunities that will arise from their deployment.

3.2 Being inclusive

The success of the EU single digital market hinges on the principle of inclusiveness whereby all 510 million citizens are confident in the digital environment. In addition, the approach towards cybersecurity in the EU needs to ensure that citizens are protected *in the different roles that they assume in society*. In other words, the EU approach to cybersecurity should ensure that the different stakeholder communities are all adequately catered for.

Confidence is built on the assumption that users can do their daily business in a safe and secure manner. Goods and services that make use of the virtual world need to be designed to be easy to use and to be user friendly. Security by design and privacy by design need to be fundamental principles adopted by manufacturers and digital service providers.

End users need to be confident not only that encryption algorithms are sufficiently strong but also that they can conduct their digital business without fear of unlawful interception, that their data is being stored in a manner that is secure and that access to this data is regulated and controlled in a safe manner. European manufacturers need to consider developing products and services that are secure and to brand them in this manner.

3.3 Making cybersecurity a competitive advantage for the EU

The value of the cybersecurity market in Europe was estimated to be 20 billion Euro in 2014 and is expected to grow at a rate of 6% per annum[20]. New disruptive technologies are facilitating the introduction of new products and services. Traditional machines are now being transformed by the use of software to deliver increased functionality, including robotics and self-driving vehicles. Europe has an opportunity to put policies in place to ensure that minimum-security requirements are met in digital products and services, to ensure real safety and security of the users and their data. Europe should capitalise on its engineering and manufacturing competences and combine this with state of the art cybersecurity to give Europe a competitive advantage.

ENISA is of the belief that end users across the world will pay a premium for goods and services if they believe that they are safe. Cybersecurity is now seen as a differentiator and an added value component. Where EU manufacturers and service providers can easily demonstrate conformity to security standards, they will have a competitive advantage where users will pay a premium for their products and services. European manufacturers should recognise the value of this approach and bring to market products and services that benefit from conformity with the appropriate security standards.

3.4 Fostering EU independency and autonomy

The EU is critically dependent on ICT in both the public and private sectors. In the public sector, ICT underpins not only key societal services, such as the provision of energy and emergency services but is also used to support core government processes. More recently, technology has played an increasingly important role in the interface between government and the citizen with many Member States offering governmental services online.

Where the private sector is concerned, it is worth noting that the internal single market of the EU is the biggest single market place in the world and in 2016 was reported[21] as representing nearly 15% of global trade with a GDP value of almost € 15 Trillion. The value of the ICT industry continues to grow and cybersecurity is a key component of this market.

Currently however, countries outside the EU dominate the supply of hardware and software in Europe. Recent revelations in respect of state sponsored surveillance and espionage have opened a debate about protecting core EU values such as privacy, security and data protection. Without trust, users will lose confidence in the digital market, and, economic growth will be affected.

---

[20] Cybersecurity as an economic enabler, ENISA, 2016, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler

[21] For reference, EUROSTAT data on international trade for 2016, here: http://ec.europa.eu/eurostat/statistics-explained/index.php/International_trade_in_goods and on GDP:
http://ec.europa.eu/eurostat/statistics-explained/index.php/National_accounts_and_GDP
http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=naida_10_gdp&lang=en

In order to protect the European ICT industry therefore, it is important to recognise the different threats with which it is faced and to ensure that the response provides adequate protection for all these threats. In this context, the concept of digital sovereignty – the ability of the EU to maintain a high level of control and security over the systems that it is using – is paramount. By ensuring that digital products and services are fit for purpose and that users have confidence in their use, the EU will simultaneously lay the foundations for a more secure society and protect its markets.

3.5 Technology aware, but technology neutral

The principles set out in this document and in the revised EU cybersecurity strategy should address the upcoming challenges related to emerging technologies without unnecessarily referencing specific technological solutions.

The strategy should set down principles that capture EU norms and values independent of the technology.

4. Opportunities for forward thinking

In the context of the review of Cybersecurity Strategy, one should not only focus on the challenges as a negative perspective, but also consider them as an opportunity and as an enabler, for solving the current and future cybersecurity issues. Investment in Cybersecurity has not only the potential to generate significant intellectual property to protect EU end users, but also to generate considerable export value. This is an opportunity for Europe, to lead and to generate the economic wealth and intellectual property, which will be used by the rest of the world.

4.1 Risk assessment using a multi-faceted approach.

The complexity of the cyber world is often underestimated. When the cyber aspect of new technologies is being assessed, boundaries are often created to simplify the risk assessment. An example includes the risk assessment associated with Artificial Intelligence, Robotics and automated transport where often-separate analysis is carried out to address cybersecurity and privacy. The absence of a comprehensive approach may result in weak conclusions and compartmentalised thinking that falls short of what is needed in the long run.

Currently, in some cases, cybersecurity challenges are examined from a threat landscape perspective. To ensure appropriate cybersecurity decisions, additional information and analysis should be taken into account. Such information and analysis should cover the entire life cycle of risks:

- Threat landscape (the analysis of current threats and new technologies and how they are being applied)
- Impact of cybersecurity incidents (impact area, impact on assets, impact scales, including impact on human rights, intellectual property, society)
- Relevance of cybersecurity on the asset landscape (what are the assets and how the assets can be compromised)
- Development and efficiency of the protection landscape (security measures and controls to protect the assets)

It is noted that in the preparation of cybersecurity strategies and policy both at EU and Member State level the multi-faceted approach is recommended where all of the above aspects are analysed.

ENISA recommends that when cyber incidents are being analysed and reported at EU and Member State level a more comprehensive approach is taken so that the level of analysis takes into account the multi-faceted aspect of cybersecurity. Any conclusion reached should be based on a comprehensive review rather than a limited analysis. It is believed that this approach will support better decision-making and preparedness for similar incidents.

It is suggested that in the definition of mandatory reporting the above approach is delivered.

4.2 Emerging technology monitoring and impact assessment from technical, political and societal perspective

Experience to date clearly shows that technology is developing at a faster and faster rate. It is believed that the societal impact of new technology deployment in the next few years will be unprecedented.

Examples of emerging disruptive technologies include Quantum Computing, Big Data, Artificial Intelligence, Virtual Reality, and the Internet of People. Europe needs to embrace these technologies. In order to achieve this, as early as possible. Europe needs to understand the impact of these technologies so that the necessary technical/ political/ societal policies are in place to address the challenges before these technologies are fully deployed. The impact of these technologies span from ethical considerations to human rights to the fundamentals of our democratic society.

ENISA recommends that programs are put in place at the earliest opportunity to prepare and assess the likely impact of these new disruptive technologies. Specific assessments need to be made in respect of each technology from a technical, political and societal perspective. In that respect, co-operation with the private sector should be reinforced.

Following these assessments, the need for new policies and legislative initiatives needs to be addressed. ENISA is of the opinion that cybersecurity will be a key aspect throughout this analysis from the perspective of the security of information including intellectual property and personal data so that citizens will be able to embrace these technologies believing that they are safe and secure.

4.3 Awareness and trustworthy digital environment for citizens

With the development of digital services and the shift to providing, more services using online tools new business models are being develop. Such online tools and models sometimes create a dependency context for the user i.e. the user is required to log in to one application to be able to use services of another application.

The right to be forgotten both in life and after in respect of personal data needs to be clarified and communicated to digital users.

In the Eurostat surveys, it should be noted that citizens would use more online services and products if they would trust them more.

ENISA recommends that lock in / dependency between various online applications (where to access the services of a provider login details and cross references to other applications are mandatory) should be avoided and the trustworthiness of digital environment should be a constant objective for all parties responsible in cyber space.

4.4 Invest in cyber hygiene, cybersecurity education and training

There is a pressing need to train more people in the area of cybersecurity. The commercial marketplace is reporting that there are not enough skilled graduates and that they have to be paid a premium to keep

them. The demand for cyber skilled personnel extends to both the public and private sectors. Recently the German military indicated that they needed to recruit more than 10,000 IT skilled personnel[22].

In addition, Member States should actively promote the idea of cyber hygiene as a first mechanism for reducing cyber risk. ENISA can support this process by helping Member States learn from each other and spreading good practice. In that respect the engagement of the private sector is crucial to the adoption good practices.

ENISA recommends:
- Promote cybersecurity as a career choice in schools and universities and encourage industry to develop cybersecurity training schemes that are aligned with established career paths.
- Encourage the retraining of adults and long life learning programs in this area.
- Develop cybersecurity culture in educational establishments and vocational training.
- Cybersecurity awareness campaigns should be continued to all citizens, that are not targeted by education or training, to support safe and secure interactions online.

4.5 Harmonisation of cyber products, services and skills

The value of the EU cybersecurity market in the EU will be in 2018 of about 25 billion Euro[23]. It is expected that this market can grow at a significant rate over the next five years.

A key element of a harmonised European cybersecurity market is having the ability to develop products, services and skills. Given that cyber-security is an enabler, having aligned policies and technical requirements across member states for products, services and skills, Europe will be better placed to capitalise on the EU single market. The existence of EU cybersecurity related standards presents good opportunities for EU manufacturers and service providers to serve the pan EU marketplace as opposed to addressing individual member state or company specific requirements. Where EU manufacturers and service providers can easily demonstrate conformity to security standards, they will have a competitive advantage where users will pay a premium for their products and services.

Europe should seek to be the early adopter of standards so that Europe is driving the marketplace rather than being pushed by vested interests. If Europe were to lead in setting cyber-security standards, it would have the opportunity to encompass the EU norms and core values defined in EU legislation such as privacy and data protection and generate competitive advantage in cybersecurity and trust. At present standards are being set by International bodies (such as ITU, ISO, IEEE), EU standards bodies (i.e. ETSI, CEN/CENLEC), National Bodies (i.e. DIN, BSI, AFNOR) and Industry groups.

Europe needs to assess the standards that are being set by these organisations to ensure that the most appropriate standards are adopted as EU standards. It is also necessary that future standardisation activities are coordinated at EU level to ensure that the best standards are developed and maintained to serve the EU market and EU citizens.

[22] More than 10k jobs requiring some IT skills in military and civil positions in army. Info here: www.bundeswehrkarriere.de/it/ and here: phys.org/news/2017-04-germany-military-combat-cyberattacks.html

[23] The cybersecurity market size in Europe in 2014 was estimated to grow from EUR 20.1 billion (out of EUR 71.7 billion worldwide estimation for 2015) with 6 % Compound Annual Growth Rate (CAGR) to EUR 24.4 billion in 2018, maintaining a share above one quarter of the worldwide cybersecurity market.

The existence of cybersecurity standards allows for the putting in place of certification processes that give confidence to the manufacturers, service providers and end users alike.

ENISA recommends:
- to set up a cybersecurity standards coordination body to ensure a coherent approach to the development of cybersecurity standards across Europe;
- Create a 'fast track' standards process for standardising technology areas that are evolving rapidly;
- Development of a pan EU Certification framework for cybersecurity products, services and skills. This framework should include different certification schemes appropriate to the level of application (from lightweight certification for a IoT devices to complex certification for high security applications such as are used for electronic banking identity).

4.6 Paradigm shift in liability and ownership of products controlled by software and the liability questions arising from the use of software.

The marketplace is being increasingly populated by hardware products that are controlled by software. Industry 4.0 is being deployed across the EU and greater seamless integration is taking place between the machine and the software controlling the performance of the machine.

Examples of products include mechanically propelled vehicles where the hardware is manufactured as a standard unit. However, the functionality of this unit is controlled by software which can alter the performance. Examples include engine power control software where the same standard engine can be set to deliver different levels of performance.

The ownership rights between the hardware (the engine) and the software are generally different. The purchaser may be of the opinion that they are the full owner and controller of the product. However, the software is generally covered by a licence from the manufacture to use the software for the life of the product and generally has a condition that by the use of this software the user agrees with terms and conditions that may limit the liability of the software manufacturer. In effect, no property rights transfer to the owner under this licence arrangement. This new approach raises new ownership and control issues for the purchaser.

There are also additional complexities about product liability between the hardware and software parts of the product. These products are increasingly gathering large amounts of personal data about the use of the product. Furthermore, the question of the security of the data generated and collected by the software needs to be addressed. Generally, the service of such products require periodic software updates where there may be an opportunity to transfer the personal data to the software manufacturer.

Similar issues also arise for example with the use of mobile phones e.g. location information, where large amounts of personal data are being collected and transferred electronically. This level of data being transferred to third parties is often supplemented by agreeing to the terms and conditions of many applications that are in everyday use.

The issue is that, increasingly the end user is left with no option but to accept the terms and conditions set unilaterally by the software developers. Experience to date has clearly demonstrated that there is no such thing as perfect software. We are living in a world where regular software updates to address security vulnerabilities are a daily occurrence.

The concept of the zero day vulnerability and its exploitation is becoming an increasing concern. Some manufacturers have offered bounties to encourage disclosure of these vulnerabilities. Other manufacturers while aware of the risk to the users have not addressed the problem and, have in some occasions, ceased to support the ongoing use of the software without providing a viable alternative.

Recognising the increasing importance of the security of software in products that affect our daily lives, further analysis needs to be carried out to address the protection of end users from the lack of security in the software.

ENISA proposes that at an EU level, an examination is carried out to address the increasing importance of the security of software, software liability, responsible disclosure of identified risks and their mitigation, the possible mandatory obligation to disclose security vulnerabilities in software and the management of personal data be carried out as soon as possible. This approach should address the unilateral power of the software manufacturers to impose their terms and conditions on the end user/consumer of the products.

4.7 Focused research and development based on EU needs to secure economic advantage

The EU is currently in the middle of its H2020 research program. While this program is delivering useful research the program may not be successful in transferring the research knowledge acquired into commercial opportunities.

ENISA should work together closely with Member States and the private sector to identify mechanisms that will support the transition of successful research ideas into commercial services and products. The main challenge will be to establish a framework linking researchers to operational communities that deploy their results so that new requirements and problems can be resolved after the research project has completed.

ENISA recommends that:

- more research funds are channelled into cybersecurity research to ensure the delivery of security by design.
- research funds are used to encourage the commercialisation of research. A closer collaboration between cyber experts in the public and private sectors be fostered to maximise the opportunity to do the most relevant research and to speed up the uptake of the intellectual property generated from the H2020 research program into the commercial world, the establishment of a framework (funding mechanisms, innovation hubs, mentoring, etc.)
- to support SMEs whose core business is cybersecurity, market studies are conducted to identify mechanisms to ensure that the EU market for cybersecurity products and services operates in an efficient market.

4.8 Updated EU governance structures with clear roles and responsibilities to address global cyber challenges

The EU cybersecurity governance framework

There are many EU institutions and bodies involved in cybersecurity, each with its own specific mandate and responsibilities (examples include Commission DGs, CERT EU, EUROPOL (EC3), EDA).

This situation has the advantage of being able to offer cybersecurity services that are targeted to particular communities, but could result in separate pools of incomplete information and incoherent methods across communities (including incompatible standards and methodologies).

In the image below, an update is proposed to address the EU cybersecurity governance, indicating the role of ENISA and the cooperation on cybersecurity topics with other parties.

The new EU Cybersecurity Strategy should embrace this challenge and mandate a lead agency to work closely with all relevant stakeholders at EU level. The risk of a fragmented approach potentially loses efficiencies from a human resource and an economic perspective.

The cyber challenge has many common aspects and duplication of expertise, capability and cost across the different stakeholders should be minimised. This is not to take away from the specialist roles that different stakeholders possess in their respective areas. The real challenge is to bring together, correctly inform and coordinate the relevant experts from different stakeholders to address common aspects of the security life cycle. For example, during the preventative stage of the security life cycle common skillsets should be located in one organisation rather than having malware analysis being duplicated in different organisations.

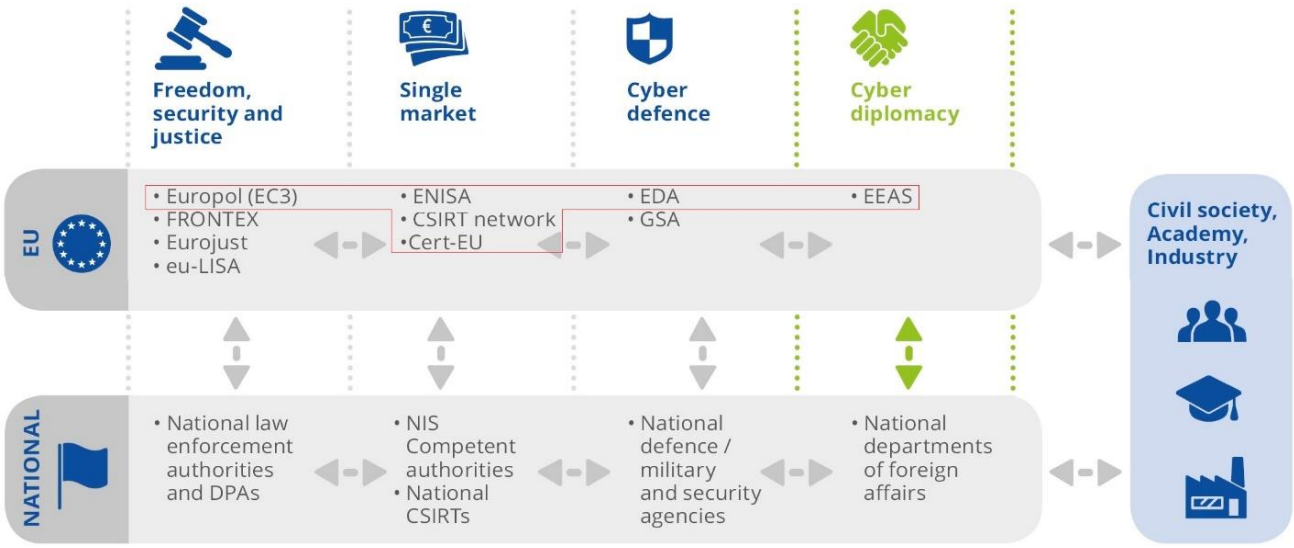

Figure 2. Role and responsibilities in the EU cybersecurity governance. Cooperation for cybersecurity.

To meet the cybersecurity challenge, Europe has a strong need for the best cyber experts available. The global war of talent requires Europe to set-up a strategy for recruiting and developing the cyber workforce.

ENISA as Europe's centre of excellence should improve its efforts to recruit the best talent and to provide up-to-date expertise to European institutions and member states.

ENISA, acting as a **cybersecurity coordination hub**, should support these different bodies by offering a number of 'cross-community support services' such as threat analysis, *cross-community trends analysis, trusted information exchange, advice on standards and certification practices, standard risk analysis techniques and taxonomies*. This will help to avoid fragmentation and duplication of resources.

Interplay of law enforcement and IT security cooperation in cyber space

The 2016 ENISA Threat Landscape Report describes the increasing level of monetisation of cyber crime. The lack of IT security in many environments is becoming an increasing important element contributing to the increase of crime, which needs to be addressed at a policy and operational level. At a policy level, the issue of encryption has become a subject of political debate[24] in recent times.

ENISA should work with Law Enforcement Stakeholders to address supporting law enforcement from an operational perspective and in the development of policy where for example the challenge of balancing the right to privacy and security in cyber space and physical safety in our society is addressed.

Interplay of civil and military cooperation in cyber space

In the last few years, Europe has witnessed increased and more sophisticated cyber attacks. Some of these cyber attacks are allegedly motivated by state actors seeking to carry out espionage or attacks on critical infrastructure. How these events are classified by the affected member states is a sovereign issue. However, when the risk of these attacks has the potential to effect more than one member state, it becomes a multijurisdictional issue and a matter, which can potentially become an EU competency issue.

While each Member State takes the lead on its own defence, the effect on other member States cannot be ignored. In the last few years, the role of the military in addressing cyber issues has increased in a number of member states. Depending on how cyber incidents are classified, the Military may have a role in both defensive and offensive activities. In addition, whereas the focus of the original Tallinn Manual was on the most severe cyber operations, the Tallinn Manual 2.0 'adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis and that fall below the thresholds of the use of force or armed conflict'[25].

There should be an enhanced level of cooperation between civil and military cyber authorities and this cooperation should aim to optimise skill sets that have already been built up in the two communities. The fact that ENISA is already supporting the European Defence Agency (EDA) in the area of cyber exercises is an example of this approach.

[24] On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

[25] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, more info at NATO CCDCOE: https://ccdcoe.org/research.html

Global aspect of cybersecurity

Given the true international dimension of the Internet and the responsibility of each sovereign nation to manage the use of the internet in their own jurisdictions, there is a need for the EU to engage in the appropriate international fora to promote the EU values and norms in respect of cybersecurity.

Cyber-crime knows no borders. There is increasing evidence that the criminals are jurisdiction shopping when they are choosing their illegal cyber activities. To address this challenge Europe has to work in the international arena with both political and technical organisations. Activities that could be supported is the adoption of the Budapest Convention, the training of computer emergency responders and the supporting of the legal system to prosecute cyber criminals in third countries.

ENISA should play a more proactive role in collaborating with international organisations having a role in cybersecurity (such as the OECD, ICANN, IETF) and should also be tasked with supporting cyber dialogues led notably by the EEAS when cybersecurity is an issue.

4.9 Protecting Cyber sovereignty in Europe

The definition of Sovereignty in the context of cyber space is under discussion. Notwithstanding this debate, there is a need to try to capture the principles involved and to attempt to address the challenges emerging. For the purposes of this paper, it is understood that cyber sovereignty describes the ability to control the confidentiality, integrity and availability of data and the reliability and integrity of the associated physical hardware and software.

The degree to which the EU can obtain cyber sovereignty can therefore be seen as a measure of our society's digital self-determination. Currently, the European cybersecurity market is dependent on a number of infrastructures that include software and hardware that is produced and maintained either partly or entirely outside its borders. Not only is Europe not leading in either of these markets, it is also faced with complex supply chains for many of the systems on which it depends. Furthermore, the cybersecurity market in the EU could be described as a 'supply push' market where suppliers have more influence in deciding on the security functionality of products than users. A consequence of this situation is that Europe is effectively dependent on third countries for the manufacturing and supply of cyber services and systems. Faced with such complex threat scenarios, the EU should develop core products and competencies that minimise critical external dependencies.

Digital sovereignty can also be considered in terms of the deployment and operation (configuration) of mass-market digital infrastructure. Here, the EU needs to be able to ensure that the norms and values enshrined in EU law, such as privacy and data protection, are protected in the operation of European digital infrastructure.

ENISA recommends that critical infrastructure operators address the above challenges by way of procedures that define clear security requirements for the entire life cycle of the products and services (e.g. from purchase to obsolescence). These requirements should take account of the need to verify security functionality in supply chains and result in a move away from a 'supply push' market by strengthening the demand side.

To assist purchasers, the Commission, assisted by ENISA, should work with Member States to develop and publish guidelines on what security aspects should be included in procurement tenders. These guidelines could be called "EU Trustworthy ICT Procurement Guidelines". These guidelines should be supported with recommendations that illustrate how purchasers should evaluate their cybersecurity requirements and should encourage a 'fair playing field'.

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

enisa.europa.eu