Framework of Trust in the Data Economy Strengthening IT security in Europe

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht - GDV Annual Congress

BONN, GERMANY
NOVEMBER 2017

It is both a great pleasure and an honour to be here today to talk about strengthening trust and cybersecurity in Europe and ENISA's pivotal role in this direction.

In our daily experience, we are all witnesses of major technological and scientific developments.

On a personal basis, we live in the era where the heating in your house can be remotely controlled, when personal files and digital information can be accessed from any place around the globe, when autonomous vehicles are ready to be deployed on the street and where my doctor can remotely conduct remote diagnosis and check my health in real-time.

However, we also live in the era where critical infrastructure such as the energy infrastructure of entire nations can be compromised, where telecommunications networks can be disrupted and manipulated, when smart connected devices can be exploited to attack large corporations to a level that their businesses begin to fail.

Cybersecurity has moved from being the content of hypothetical scenarios and of sci-fi films to the real world. Crime, espionage, sabotage and even international conflicts have moved from the so-called real world into the virtual cyber world, Hybrid warfare methods are now seen alongside conventional and unconventional warfare where cyberwarfare is being deployed more often. These threats call for cyber norms and cyber diplomacy responses at the EU, national, and international level.[1]

In the past where one needed a gun to rob a bank, today an equivalent amount of damage can be achieved from the action of a fingertip on a keyboard from any location with an internet connection in the world. Not so long ago, the words cyber and cybersecurity were reserved for the IT professionals and hackers. But as the years passed, and as the number of highly publicised cyber attacks increased and as the numbers of affected citizens grew, these words have now become mainstream.

Cybersecurity is not an option; it is a necessity.

[1] ENISA, *ENISA Overview of Cyber Security and Related Terminology,* October 2017, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

Cybersecurity impacts every sector, every citizen and most activities of our daily lives.

Let me describe a few real-life stories from the last 12 months.

Friday October 21, 2016. If you typed the URL of some well-known US internet service providers into your browser there was no response[2], and no online services were available. The reason - the Mirai botnet[3] had hacked millions of mainly Linux-based Internet-Of-Things devices and collectively performed a Denial-Of-Service attack on the Domain-Name-Service provider DYN with the result that the IP-addresses of hundreds of company services could not be accessed anymore. It was like removing the telephone number of these organisations in a way that customers could not contact them and the affected companies could not deliver service.

Sunday November 26, 2016. A friend of mine here in Germany, fell off the stairs at his home and injured his leg. He was home alone and in pain. He crawled to his VoIP based fix phone in his house. He tried to call emergency services but the phone did not work. His mobile was outside, in the car, and beyond reach. He had to wait several hours until the phone was operational again. This telephone outage was due to an attack targeting Deutsche Telekom Routers[4] where almost one million landline subscribers in Germany lost telephone service and access to the emergency services on their land lines.

Friday May 12, 2017. Getting ready for the weekend, employees of many organizations across the globe were faced with an unwelcome image on their screens stating that their files had been encrypted and demanding a ransom to unlock their files. This incident became known as the WannaCry attacks, a ransomware campaign targeting a vulnerability of the Windows OS that caused chaos due to its massive distribution. It is estimated that it affected more than 150 countries and over 230,000 systems[5]. Several of the systems affected by WannaCry were in hospitals, where many computer-operated machines such as scanners and patient record databases were affected. The end result was that operations and hospital services had to be postponed.

The last 15 years have generated a digital revolution where virtually all information and activity has been digitalised in some form. This new digital ecosystem is increasingly at risk from cyber attacks and the attacks described above have undermined our trust in this digital environment.

If we are to have trust in our digital ecosystem, we need to have more security, we need to have it faster and we need to maintain it.

[2] 2016 cyberattack, available at: https://en.m.wikipedia.org/wiki/2016_Dyn_cyberattack

[3] 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/

[4] Deutsche Telekom Probes Potential Hacking after Router Issues, Bloomberg, 28/11/2016, available at: https://www.bloomberg.com/news/articles/2016-11-28/deutsche-telekom-probes-potential-hacking-after-router-issues

[5] Wannacry Ransomware Outburst, ENISA, 17/05/2017, available at: https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

Cybersecurity is a shared responsibility.

A compromised computer is an effective weapon which can be used to attack real and personal property.

Users need to adopt basic cyber hygiene principles to establish the foundations of safety and security in the cyber space.

Critical asset operators need to establish baseline security measures and incident notification mechanisms to protect critical infrastructures.

Industry and businesses in Europe, need to take on board security measures in order to be protected themselves from cyber threats such as cyber-attacks, cybercrime, cyber sabotage and cyber espionage.

At a global level, given the pervasive nature of cyber space, adequate measures and international agreements need to be in place to guarantee global stability in the face of cyber risks that neither respect or acknowledge borders.

Computers and digital data go to the heart of our lives. The core EU values (human rights, liberties and democracy) enshrined in the Lisbon Treaty for the real world need also to be guaranteed in cyber space.

However, it is unrealistic to think that we are or will ever be 100% cyber secure.

Why is that the case?

There exist many reasons, the most indicative of which include:

The cybersecurity threat landscape is constantly changing;

Novel attack vectors and cybercrime techniques are emerging;

Increased connectivity leads to an increase in the attack surface;

Technological developments make it easier to mount advanced cyber attacks

Cybersecurity cannot depend on end users only.

So what are the solutions?

As with any complex problem the solution is multifaceted. The solutions include the delivery of a European cybersecurity strategy, enacting legislation to mandate increased activity in the cybersecurity areas including cyber security in critical infrastructures, certification of services and products, better training for end users, security and privacy by design, cyber insurance, mandatory notifications of cybersecurity breaches, increased research and development and most importantly the strengthening of the EU Cybersecurity Agency ENISA.

The most recent cybersecurity strategy[6] was launched by the EU Commission on the 13th September 2017 in President Juncker's State of the Union address[7]. The strategy proposes, inter alia, an emergency fund to assist in cross border cybersecurity incidents, as well as the introduction of a competence network and centre for research and development in cybersecurity, and is currently being given the political support by the adoption of Council Conclusions.

The Commission's draft Cybersecurity Act[8] is currently being debated by the co legislature and it proposes, inter alia, to introduce a pan European certification scheme for cybersecurity products and services, and a stronger and better resourced ENISA.

In relation to the current debate on introducing **a new certification scheme for Europe**, the draft EU Cybersecurity Act proposes to introduce a voluntary certification system for products and services that would represent an attempt to introduce a higher quality product and service that would have minimum security standards attached, thereby raising the security bar and protecting consumers and operators. It is envisaged that the introduction of the certification scheme will generate a new opportunity for EU manufacturers and service providers that will increase trust, protect our personal information and stimulate economic activity and wealth.

Additionally, the first piece of cybersecurity legislation in Europe called the Network and Information Security Directive (NISD) comes into effect in 2018. Other ancillary pieces of legislation have been introduced, such as the eIDAS Regulation giving legal effect to electronic identities and electronic trust services to secure cross border electronic transactions. With eIDAS, the EU has managed to lay down the right foundations and a predictable legal framework for people, companies (in particular SMEs) and public administrations to safely access to services and do transactions online and across border in just "one click". Indeed, rolling out eIDAS means higher security and more convenience for any online activity such as submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another Member State, authenticating for internet payments, bidding to on line call for tender, etc.

[6] European Commission, *Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN(2017) 450, available at: https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF

[7] European Commission, *State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks,* IP/17/3193, available at: http://europa.eu/rapid/press-release_IP-17-3193_en.htm

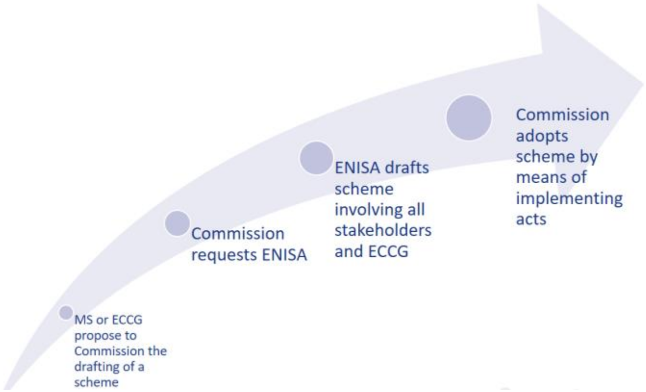
[8] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')*, COM(2017) 477, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN

Turning in more detail to the proposed EU-wide certification framework, in summary, the provisions on certification proposed in the draft Cybersecurity Act include:

1. making available a detailed specification of cybersecurity requirements against which ICT products will be evaluated
2. several assurance levels
3. specific evaluation criteria and methods to be used
4. outlining information to be supplied to Conformity Assessment Bodies (hereinafter, CABs)
5. laying out conditions to use marks and labels
6. setting out the mechanisms to demonstrate continual compliance as appropriate
7. providing for the conditions to grant maintenance and extension of a certificate
8. presenting the consequences of non-conformity
9. underscoring the voluntary nature of a European cybersecurity scheme, unless there is provision to the contrary in EU Law.

The various steps envisaged for the new European certification scheme are as follows:

1. The MS or the Group, propose the preparation of a candidate scheme to the Commission
2. The Commission issues a request to ENISA
    a. ENISA consults with all relevant stakeholders and it cooperates with the Commission and the Group
    b. ENISA proposes a scheme and transmits it to the Commission.
    c. The Commission may adopt implementing acts to adopt the scheme
3. ENISA thereafter maintains an informative web site on the scheme


MS or ECCG propose to Commission the drafting of a scheme
Commission requests ENISA
ENISA drafts scheme involving all stakeholders and ECCG
Commission adopts scheme by means of implementing acts

Thus, the proposal reserves a role for ENISA as the body that upon Commission request will draw up a scheme involving all relevant stakeholders.

The assurance levels foreseen are as follows:

1. Assurance level basic: a limited degree of confidence in the claimed or asserted cybersecurity qualities
2. Assurance level substantial: a higher degree of confidence in the claimed or asserted cybersecurity qualities
3. Assurance level high: a high degree of confidence in the claimed or asserted cybersecurity qualities

The EU framework should bring a clear benefit for producers and service providers in that their products and services will only need to be certified in one Member State to be made available in the entire EU market. This approach should increase speed to market, reduce the financial burdens of achieving national certification in each Member State and facilitate standardisation across the EU market.

The higher standard of security that such a certification framework entails is expected to require more EU-wide investments, boosting revenues and stimulating GDP growth across Europe.

In the 19th century, during the steam-driven industrial revolution, many steam engines exploded causing (fatal) accidents and leading to the creation of a steam boiler inspection association in Mannheim in 1866 – the forerunner of the TÜV. By analogy, today, we run the risk of IT blowing up around us due to lack of security. Therefore, we need to invest in the security and safety of IT products and services in order to build and maintain the trust of consumers and companies. This can be supported through certification, and building responsibility and liability mechanisms.

While the nature of a European cybersecurity scheme remains voluntary, unless there is provision to the contrary in EU Law, Certification Bodies (CABs) in the MS are authorised to issue the certificates. The duration of validity of certificates issued is limited to up to three years and they shall be recognised across all MS.

The issue of legal liability for defective products is well developed across the EU. However, there is increasing debate about the liability arising from products and services that fail to have adequate cybersecurity to protect their customers.

Liability of a notified CAB towards end users as a result of a conformity assessment procedure has been recently subjected to Court scrutiny in Case C-219/15 Elisabeth Schmitt v TÜV Rheinland LGA Products GmbH of 16 February 2017. The decision concerned a notified private body qualified in a MS (DE) for the conformity assessment of medical devices.

Pursuant to a competent authority in another MS (FR) notifying the non-compliance of a medical device with quality standards, the plaintiff claimed damages for non-material damages from that notified body, arguing that it did not carry out unannounced visits, final inspections of the products and that it did not control the delivery notes and invoices which evidenced that the manufacturer did not use an approved form of material.

The First Instance Court in the MS rejected the contractual and non-contractual liability of the notified body. The Court of Appeals of the MS referred the case to ECJ for a preliminary ruling on whether notified bodies have competence, under European law, to carry out unannounced inspections, examine the design of products as well as records.

The Court stated that the purpose of the Directive 93/42 is to protect the safety of natural persons.[9] Notified bodies within the scope of the market surveillance obligation must take appropriate measures if it becomes clear that a medical device may not comply with the requirements laid down in Law. Taking into account the purpose of the Directive, which does not cover liability of notified bodies, the Court did not exclude it, as an option governed under MS Law on grounds that the notified body did not fulfill its obligations *in toto* under the Directive, subject to the principles of equivalence and effectiveness.[10]

The considerations of the Court that the notified body should exert "due diligence" and "act on the face of the evidence" with respect to device compliance suggest that the notified body should be pro-active in seeking out evidence of the uptake of a certified product in the market. While circumstances determine the outcome of actions, notified bodies are assured that they bear no general obligation to do so at all times.

It is reasonable to assume that the jurisprudence in this area will continue to develop and it can easily be argued that providing adequate cybersecurity in electronic products and services to protect end users will be considered an essential aspect of the goods and services being fit for purpose. In the absence of the appropriate level of cybersecurity it is possible that the courts will impose liability on equipment suppliers.

Why are certification and liability issues becoming so important?

With increasing processing power of digital computers new domains such as robotics, artificial intelligence, automation and industry 4.0 are becoming a reality.

The market is now testing self-driving cars and legislatures in some countries are addressing the challenge of regulating their use.

Today's cars, which are driven by humans, have changed from being purely mechanically operated machines to being controlled by up to 100 million lines of software code. Periodic service visits to the garage not only involve an oil change but also a software upgrade to improve performance, address identified bugs and improve cybersecurity. And these cars do not yet have a permanent connection to the internet.

[9] The Court in its ruling referred to Case C-288/08 Kemikalieinspektionen v Nordiska Dental AB stating that the Directive on medical devices aims to protect "health stricto sensu" and the safety of third parties and other persons in general.

[10] While the Directive does not confer a general right to compensation the Court found that it should do so by reference to Case C-222/02 Peter Paul, Cornelia Sonnen-Lütte and Christel Mörkens v Bundesrepublik Deutschland of 12 October 2004, a case on MS liability for negligent supervision in the financial sector. In this Case the Court refused to apply a Francovich (Case C-6/90 Francovich v Italy, according to which failure by the MS to transpose a Directive into MS Law does not preclude individuals from seeking compensation and thus laying the ground for state liability for damaging an individual) type right to compensation by the MS on grounds that prudential supervision over credit institutions.

There have been many articles published describing how a remote internet connection to a self-driving car caused it to malfunction when it was subject to a cyber-attack. Media reports cite that the US Federal government is poised to create its first law for autonomous vehicles.[11] The state of Arizona's insurance regulator is stated be considering the question of liability when an accident occurs with a car not being driven by a human. In March of 2017 it is reported that in Arizona the first car crash took place between a self-driving car and a car driven by a human. In this case the police did not attribute fault to the self-driving car. However, the question arises as to what level of checking was done to check the quality of the software of the self-driving car and if there was a possible malfunction in the software.

It is not too difficult to imagine similar incidents involving a robot performing its tasks and injuring a human in the process.

The question of attributing liability will reach a new level of complexity as lawyers begin to argue in court the cybersecurity aspects of the software and hardware, the certification of the products and how fit the robot is not to injure a human.

While the lawyers will undoubtedly rise to this challenge, the role of the insurance industry cannot be ignored. I believe that cybersecurity will open up a new chapter of risk analysis that will be somewhat mitigated by the risk assessors of the insurance industry making detailed mathematical calculations and hopefully for them a healthy profit from this new world.

The data protection aspects and the risk of data leaks should not be forgotten. These digital machines will be gathering information continuously and many of the activities of these machines will have a close association with personal information. For example, the possession of a remotely controlled insulin pump is a good indication of a diabetes problem and the data associated with the activity of the pump in administering insulin could be an indication a poor state of health. Such information in the wrong hands could easily have an adverse effect on the wearer of the pump and give rise to a breach of the data protection regulations, material damage to the victim and an entitlement to compensation. Once again the cybersecurity aspects of this scenario need to addressed. In the absence of security by design and privacy by design a liability risk needs to be considered by the manufacturer. I can only imagine that the insurance industry will have a role to play in mitigating the risk for manufacturers.

Cyber Insurance plays an important role not only for the risk of being sued successfully for negligence but also for the residual risk. Cyber insurance can address the residual cyber risk, namely the risk that cannot be reasonably mitigated by cybersecurity measures.

While there is always a risk in being innovative and bringing new services and products to the market, cyber insurance has an important role to play in assisting manufacturers to develop the next generation of products and services.

[11] New York Times 14th November 2017

Cyber insurance can increase trust in the Digital Single Market.

Cyber risk is nowadays considered a Top-5 global risk[12], a factor that is expected to contribute to the growth potential of the cyber insurance market. Furthermore, the Digital Single Market and all assorted policy initiatives are expected to increase demand for cyber risk transfer options. The relevant lack of a sufficient "insurance market for cybersecurity" has been identified as a factor limiting people's participation in the digital market[13].

A recent example that demonstrates the need for cyber insurance is the NotPetya attack of June 27, 2017 that originated in Ukraine and is expected to result in large insurance pay-outs to U.S.-based pharmaceuticals giant Merck.[14]

The cyber insurance market currently generates about $3bn-$4bn[15] in premiums annually, but according to some industrial forecasts it is expected to reach $20bn by 2025, making it one of the fastest growing segments of the industry[16].

Still, the EU market is considered to be at its early development stages and lagging behind the US. The expected growth for the European market is anticipated to be further accelerated by the adoption of the GDPR and NIS directive, where the incident reporting costs and regulatory fines are expected to be the main drivers for market adoption.

Both the GDPR and the NISD constitute an exceptional opportunity for the cyber insurance market. The envisaged mandatory incident reporting schemes should be leveraged to produce meaningful data to be used by the cyber insurance industry.

ENISA has been working on the topic of cyber insurance for several years. We have been engaging with stakeholders spanning from industry to policy-makers and in this respect we encourage you to reach out to us to listen to what we have done and to help us do more!

[12] AON, *2017 Global Cyber Risk Transfer Comparison Report*, April 2017, available at: http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp

[13] European Commission, *Cybersecurity in the European Digital Single Market,* March 2017, available at: https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf

[14] Merck cyber attack may cost insurers $275 million: Verisk's PCS, Reuters, 19/10/2017, available at: https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP

[15] These figures refer to standalone coverage and exclude cyber cover bundled in traditional policies ("silent wording")

[16] Cyber insurance market expected to grow after WannaCry attack, Financial Times, 16/05/2017, available at: https://www.ft.com/content/25bf97e8-3a27-11e7-821a-6027b8a20f23

Solid cybersecurity is based on solid foundations of trust.

For the digital economy and the digital single market to succeed, trust needs to be established among all involved actors.

Trust is needed for citizens to use online services and to participate in the digital economy. Citizens need to be assured that their data and transactions are safe and secure, that their personal data is protected, that they will have uninterrupted access to the digital highway, that they will be compensated for any losses or problems.

Trust is also needed for the industry to provide its services and products for the digital economy. Industry needs to be assured that the same rules are applied for all, that there exist fair information sharing mechanisms, that their suppliers and other actors in the supply chain respect certain security principles, that any exchanged information remains private and confidential.

The European Union has two fundamental pieces of legislation to assist in the direction of establishing trust. The Network and Information Security Directive (NISD) and the General Data Protection Regulation (GDPR).

The Network and Information Security Directive is the first piece of EU legislation specifically aimed at improving cybersecurity throughout the Union. The Directive focuses on protection for Critical Information Infrastructures or namely national essential services through setting baseline security measures and implementing cyber incident notification. Full implementation of the Directive by all Member States by May 2018 is imperative for ensuring resilience in the Union. The adoption of baseline measures across operators of essential services promotes homogeneity and ensures transparency in terms of adopted cybersecurity measures. This leads to more trustworthy services.

The General Data Protection Regulation **sets EU wide rules on the protection of data** addressing in a uniform manner the management of personal information in all member states. The uniformity of rules across EU serves as a stimulus for the industry when providing services within the EU, since there is only needs to be one point of reference in terms of data protection. Moreover, the GDPR hands the power to the data subjects, the users, when their personal data is concerned. Such empowerment is clearly an enabler of trust and a puts Europe in a lead position in respect of protecting personal information.

Building strong cybersecurity requires actions on many fronts.

The EU is already working towards this direction in many ways. However, now is the time to streamline and synchronize all efforts. In 2013, the EU set out a Cybersecurity strategy launching numerous work streams to improve cyber resilience. The main goals of this strategy were to foster a reliable, safe and open cyber ecosystem for all. These goals that still remain valid. But the continuously evolving cyber threat landscape calls for more effective measures.

Earlier this year, the EU announced a Communication on resilience, deterrence and defence for building a strong cybersecurity for the EU. Within the EU, Member States have tools and policies required to address cybersecurity at a national level. However recent cyber incidents demonstrate a new scale of incident and a cross border nature to these incidents such as WannaCry. The nature of these attacks demonstrate that cyber incidents are no longer confined to one administration but that cross border cooperation is needed.

All actors - the EU, the Member States, industry and individuals – need to work together to give cybersecurity the priority it needs to deliver a better EU response to cyber-attacks.

However, to improve coordination between these actors, cyber exercises have been designed that not only bring together different sectors in a Member State but also all the EU Member States. These exercises bring together the relevant stakeholders at the technical, operational, political and media levels. It is only when there is trust between the actors that communications work and real cooperation begins to have its positive effect. To enhance cooperation and trust building ENISA has delivered biannual cyber exercises where all Member States participate. Standard operating procedures to respond to cyber incidents have been developed and tested by all the actors. Communications infrastructures have been built to facilitate the exchange of information in a confidential and trusted environment. ENISA has played a pivotal role in the building of this trust

In the EU cybersecurity landscape, ENISA has become the facilitator that brings the cyber security actors together.

The vision in the new draft Cybersecurity Act reinforces this position. By strengthening the European Union Agency for network and Information Security (ENISA), the proposal from the Commission which is now being considered by the Council and the Parliament proposes to increase the financial and human resources of the Agency. This will enable the Agency to be in a stronger position to support Member States, EU institutions, businesses and citizens in achieving a higher level of cyber security.

It is proposed that ENISA with its greater resources will be better positioned to have a stronger role in policy development and implementation including helping the Member States meet the requirements of the Network and Information Security Directive. It is also proposed that ENISA will act as a focal point for information and knowledge sharing and play an important role in both operational and crisis management across the EU. In addition, the proposal to organize annual cyber exercises should enhance the European preparedness to manage cyber incidents.

Cybersecurity is indeed a shared responsibility and ENISA is stepping forward and is already assuming its share of this responsibility. Accordingly, ENISA is working towards making collaboration and information and knowledge sharing stronger and more reliable. The multi-faceted efforts of ENISA across the cybersecurity spectrum are supporting and empowering a more cyber secure and safer Europe.

Your industry also has an important role to play in the digital ecosystem.

Insurance is not just about minimising risk and maximising profit. The insurance industry has a key strategic role in supporting the cyber manufacturing and the service industry by working with them to encourage industry to innovate, while minimising risk and avoiding industry being always fearful of bankruptcy due to an error in some digital product or service.

Manufacturers and service providers need the help of the insurance industry to push the digital boundaries forward and develop innovative cyber products and services. It is these digital products and services that will drive the next generation of wealth in Europe and the success of the digital single market.

I hope that I have presented some of the complex aspects and interactions that make up our digital ecosystem. I hope you will work with ENISA to address these challenges and that together we will make Europe a better place.

Thank you for your attention.

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
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu