Looking into the crystal ball

A report on emerging technologies and security challenges

VERSION 1.0

JANUARY 2018

www.enisa.europa.eu

European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe’s critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use louis.marinos@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to acknowledge the contributions from experts involved in the brainstorming sessions. In particular:

From the University of German Federal Armed Forces: Thomas Diefenbach*, Peter Hillmann,* Prof. Dr. Ulrike Lechner, Prof. Dr. Axel Lehmann

From secunet AG: Dr. Rainer Baumgart, Thomas Pleines, Dr. Kai Martius, Johan Hasse

Legal notice
Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Table of Contents

Executive Summary

The time has come for ENISA to take a look at the crystal ball of technology; In particular looking at what are considered to be emerging technologies and what might be their prospective usage scenarios. Considering emerging technologies and applications is an important step in assessing future security needs.

ENISA has performed this effort in collaboration with external experts from academia and industry. Starting with a small number of individuals, it is planned to expand this assessment by engaging additional experts, both within and outside ENISA committees and bodies. For the time being, the initial sight to emerging technologies has shown that currently top technological challenges are:

- The Internet of Things,
- Autonomous systems,
- Next generation virtualized infrastructures (including SDN and 5G),
- Upcoming societal challenges,
- Virtual and Augmented reality,
- The Internet of Bio-Nano Things,
- AI and Robotics.

Knowing that the above list is not exhaustive, ENISA will continue the dialogue with experts to complement it. For the above emerging technology areas both technological and cyber-security challenges are presented in this report.

By taking into account the emerging security challenges, the most important cyber security areas have been identified by means of “emerging security related areas”. These are:

- Elaboration on Certification,
- Coordination of actions in cyber space,
- Development of trustworthiness,
- Coverage of complete lifecycle,
- The future of cryptography,
- Future Identification technologies,
- Use of Artificial Intelligence and Machine Learning in cyber security,
- Increasing end-user involvement.

ENISA believes that these cyber security areas will present challenges to the cyber security community in the years to come and hopes that they will be extensively discussed within its stakeholder communities.

Last but not least, in this work input that has been received by the ENISA Permanent Stakeholder Group (PSG) is being mentioned. In a similar manner, input will be integrated through an interaction with the new PSG that will have its kick-off end of October 2017. In this manner, both previous and new contributions from PSG will be put in the context of the areas presented in this report, widening thus significantly the number of contributors.

1. Introduction

This paper is the initial documentation of an attempt to assess upcoming technology and the associated security challenges. This will be achieved through interaction with security experts from various sectors such as industry, academia, public sector, etc.

This idea is not new: within ENISA, the consideration of future technological challenges is part of the internal planning and knowledge management process. It allows to develop proposals, channel knowledge development and set work priorities. In the realm of ENISA projects, various external experts participate in achieving this objective, for example by contributing to the corresponding activities (e.g. conclusions drawn in projects, providing advice, supporting studies, stock-takings, surveys, etc.). Finally, the Permanent Stakeholder Group[1] (PSG) is established in order to channel information and ideas on new developments into the ENISA planning process.

Yet, with this effort the prediction of future challenges is being brought on a broader and yet more focused basis: ENISA initiated a dedicated dialogue with representatives of stakeholder groups to brainstorm about emerging technological and security challenges and consolidates discussions/ideas/experiences in form of this paper. The time horizon covered by the covered technology areas varies and covers developments that are ca. 1 to 5 years ahead of our time. Aim of this approach is to create an initial nucleus of material with relatively low resource investment, by collecting input from various key stakeholders. At the initial phases of this report, a collection within technology oriented stakeholders in the area of Information/Cyber Security has been performed. After an assessment of the achieved results, this activity may be put on a wider basis, both regarding the involved skills and number of contributing stakeholders.

The process behind this work has a second objective: through the interaction with various stakeholders, ENISA gets an insight on complementary, mutually enforcing interests and ideas of those stakeholders. To this extent, ENISA will play the role of mediator to achieve mutual fertilization of ideas that might lead to advancement of security practices/products/operation among these stakeholders. At the same time, results from activities of these stakeholders may flow into the work of others, including ENISA’s deliverables and will be disseminated to the public.

[1] https://www.enisa.europa.eu/about-enisa/structure-organization/psg, accessed June 2017.

2. Process and Content

2.1 Process

In order to proceed with this work, the following process has been defined:

- An ongoing information collection is established within ENISA. This is based mainly on open source and covers various areas of security, technology and policy developments. Moreover, this information contains also input from interactions of ENISA management team with key stakeholders.
- Available material from previous stakeholder interactions (e.g. previous ENISA Permanent Stakeholder Group -PSG) has been taken into account.
- Within the ENISA annual work programme delivery process, open points, future requirements and gaps in the area of security and emerging technologies are being identified. This material is subject to discussions, both internally and with contributing stakeholders.
- Guidance and brainstorming is being performed within various ENISA bodies, particularly in the ENISA PSG. This information flows in prospective versions of work programmes and is being taken up within internal and external projects/activities.
- Interested key contacts of ENISA (e.g. PSG-experts, other experts engaged within ENISA projects, academic organisations working together with ENISA) are enrolled in a brainstorming dialogue relating to emerging technology and security issues.
- All this information is consolidated internally and has been used as input to this paper.
- This initial draft will be put to the attention of a wider group of stakeholders/experts for wider consultations. ENISA will ask for contributions the members of the newly appointed Permanent Stakeholder Group during its constitutional meeting end October 2017.

2.2 Content

The content of this paper is oriented towards groups of issues/topics/aspects that share some common characteristics. Examples are: same technology sector, same business area, same policy context and scope, etc. Knowing that it is impossible to be free of overlaps, the different topics presented may have commonalities both regarding technological but also security issues.

In the following we present different prevailing views on technological topics and – when appropriate – we draw possible consequences for cyber security.

In case actions have been identified that relate to some existing ENISA work programme topics, these will be indicatively mentioned. The same holds true in case identified topics map to non-confidential activities of the stakeholders involved in the brainstorming. Such topics are good candidates for the initiation of cross-stakeholder interactions based on topics of common interest.

Finally, for the sake of completeness, we provide a list with topics addressed in the performed brainstorming per organisation. This material serves as a reminder for the list of topics discussed and the sequence bellow does not indicate any prioritization.

3. Consolidation of collected ideas: Emerging Technology Areas

This chapter contains all evolving technology areas that are considered to bring cyber-security challenges. This assessment is based on discussions, presentations and information collection that has been performed over the previous year. It is taken as given, that these technology areas will present challenges to the cyber security community for the years to come.

3.1 Internet of Things

3.1.1 Technological Challenges

The Internet of Things (IoT) has been considered as an emerging technology area due to its potential in affecting human lives and to lead to digital transformation through new products. Even though this technology is available for some years now and as such not new, experts believe that its potential is by far not yet exhausted and brings a lot of technological challenges.

The challenges related to Internet of Things (IoT) are known and understood in the (security) community. IoT plays an important role in life, as it serves/manages various areas of consumer environments. Hence, from the market point of view IoT:

- Is the new context for delivering hardware, software and services to consumers;
- Creates a lot of re-usable data helping the development of new products;
- Allows for penetrating[2] – hence marketing - private life and private sphere of users;
- Allows for a flexible development of environments, while enabling customer binding;
- Constitutes the next level of convergence of various infrastructures, data and services.

These facts make clear why information about IoT deployment/usage will be a very desirable piece of information for a variety of market, government, national security, but also malicious actors.

Addressing security in IoT is difficult: cheap, mass production devices are launched with weak security due to cost issues. Moreover, as they are of generic purpose, it is difficult to foresee the area of application, thus take care of protection requirements during fabrication. Nonetheless, when bundled into bigger/constellations they might be part of a complex infrastructure processing significant amounts of data of that pose strong confidentiality, integrity and availability requirements.

Another challenge is the computing power that is inherently available in interconnected devices. This computing power can be misused when entire or parts of an IoT network is being taken over by malicious agents. The Mirai[4] botnet has demonstrated the intensity an orchestrated attack from large numbers of devices may have (see also next section).

It is interesting to see that in the Gartner Hype Cycle 2016[3], IoT is considered as being still in the innovation trigger phase (i.e. early phase). Hence, there is significant time for action in the IoT till market maturity/productivity.

[2] The penetration of IoT in every day's life becomes more and more evident, eventually with corresponding market growth.
[3] http://www.gartner.com/newsroom/id/3412017, accessed June 2017.

All in all, the challenge with IoT environments and devices alike will be to maintain the balance between low cost (i.e. the driver for IoT adoption), short time to market and security (i.e. the enabler of trustworthiness). If this balance is lost, there is a risk for market failure of IoT applications.

3.1.2 Security Challenges of IoT

IoT will be an opportunity for cyber-crime monetization activities. Equivalently, IoT will be in the focus of national security and espionage, both state and corporations sponsored. Moreover, data on user behaviour will be the future marketing instrument.

Having said that, one can easily assess the areas of misuse of this information and the corresponding threat exposure (list indicative, non-exhaustive):

- Data and available functions from IoT applications may be misused within cyber-threats such as phishing, ransomware, cyber-espionage, data breaches, identity theft, etc[4].
- Ill-secured devices can be hijacked and misused in various attack scenarios, e.g. Botnets, Denial of Service, spam, etc.
- Available ill-protected interfaces and processes owned by service providers may be misused to penetrate their systems. Moreover, the absence of product life-cycle functions (e.g. updates) makes the elimination of vulnerabilities impossible.
- Available functions, processes and data can be misused with the aim of illicit profit.
- Companies may be interested in data, practices and functions available to spy on their competitors.
- Home appliances of single households or group of those can be misused by activists, terrorists, cyber-warriors, etc. to cause harm to entire areas.

Given the intimate but also existential nature of IoT applications (media consumption, life habits, private environment, e-health, assisted living, etc.) confidentiality, integrity and availability requirements will be high. It will be necessary to develop products to protect such environments.

Instead of “micro” - protecting each element in an IoT environment, a focus on protecting architecture components may be more appropriate. The utilization of existing/well known/efficiently manageable security controls may provide a good protection if applied properly at the right level of the IoT architecture. Current discussion shows that IoT needs a lot of work to mature, both regarding architectures and services. The Mirai[4] botnet, for example, that is taken predominantly as THE example of an IoT misuse, was actually abusing internet routers. Nonetheless, such components have never been considered to be part of IoT infrastructures.

Estimated timescale for rollout[5]: 2 to 5 years

Takeaways IoT

- IoT platform is in early development phases.
- 5G and virtualization will enhance the device-to-device interactions (M2M).
- IoT protection as a whole will be difficult. Application/sector oriented solutions are more feasible.
- IoT will enlarge attack surface by means of novel abuse scenarios.
- Existing security protection controls will need to be considered for IoT scenarios.

[4] https://en.wikipedia.org/wiki/Mirai_(malware), accessed June 2017.
[5] http://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/, accessed September 2017.

- Although processed data may be volatile and of low value, data protection will be necessary in order to maintain privacy.

3.2 The interplay between Technology Use and Societal Challenges

3.2.1 Technological and Societal challenges

Though not a technology area per se, societal changes play an important role in technology adoption: firstly they affect the creation of new products. Secondly, they play an important role on how existing products are being used. In both cases, societal challenges affect technology deployment and security/privacy issues. As such, they have been considered in our brainstorming sessions as an area that is setting up context of technology use. This is the main reason for considering societal changes this chapter.

Societal changes with regard to digitization are undoubtedly a significant phenomenon in society. Understanding those changes helps identifying behaviour and habits of end users – that is - deriving various usage scenarios. This, in turn, provides important incentives for protection requirements of end-users.

A noticeable shift has happened in the way media are consumed: while the average age of traditional TV viewers is growing, younger generations go away from TV watching[6]. At the same time, use of video on demand is mostly used by younger users[7]. Similarly, technology has played and still plays an important role in changes of social behaviour of younger generations, in particular regarding their communication, interaction, media consumption and socialization habits.

Complex behaviour of users can also be assessed in the areas of socializing by using messaging services, social networks and sharing of life-logging information and qualified self[8]. Many of those trends are in partial contradiction with the use of well formulated human rights regarding the need of privacy. For example, some users may publicise information about themselves that the government treats as confidential personal data.

Moreover, modern considerations of the digital divide show that there is a difference in technology usage between (socially) advanced and disadvantaged individuals. These differences are reflected in the way they are using online services[9].

It is impossible to talk and act in the area of technology and technological platforms without fully understanding end-user behaviour. This will lead to failure of any technical measure, including cyber-security.

3.2.2 Security challenges emerging from Societal Changes

Challenges to cyber-security from societal changes in the user community are quite big. This is mainly due to the fact that there is a need to better understand the motives, habits and psychology of end-users, knowingly the weakest link in cyber-security.

Assessments show that a better security awareness from end-users may reduce over 50% of the current security incidents that are reportedly based on human error[39,40]. This is indicative for the importance of

[6] http://www.marketingcharts.com/television/are-young-people-watching-less-tv-24817/
[7] https://digiday.com/media/demographics-youtube-5-charts/
[8] http://aias.au.dk/events/the-quantified-self/
[9] https://www.linkedin.com/pulse/new-digital-divide-emilio-mordini?trk=prof-post

such measures, though their spread is far beyond average throughout all age categories. This has been well understood in the security community: important awareness campaigns currently launched take into account such facts.

From user behaviour, cyber-security may draw important conclusions regarding (list in indicative, non-exhaustive):

- Weaknesses caused by behavioural patterns;
- Weaknesses caused by usage scenarios;
- Threats exposure due to weaknesses;
- Misuse scenarios;
- Identification/assessment of important user assets;
- Elaboration on security controls that can be managed by non-experts;
- Awareness raising and training matters including differentiation according to age of target groups.
- Balance/orchestration of societal needs, educational methods and user behavioural patterns.
- Elaboration on potential courses of action to achieve this balance (including regulation, user liability etc.).

Estimated timescale for addressing: 2 to 5 years

Takeaways Societal Changes

- User behaviour needs to be better studied and understood
- User habits have to be taken into account in cyber-security
- With implementation of basic security controls, significant mitigation of risk can be achieved

3.3 Next Generation IT infrastructure

3.3.1 Technological Challenges

In many areas of IT we see currently the creation of next generation IT-Infrastructures. Main characteristics of this evolution is the increased deployment of virtualization, meshed environments/applications, multi-tenant capabilities, provision of customization and management capabilities, just to mention a few. In those systems, end-to-end offerings are being considered, where the operation can be managed remotely, without the need to maintain any own infrastructure locally.

These trends pose significant technological, operational and economic challenges. Based on these trends, for example, many end-to-end services will need to be re-defined and re-commissioned.

Though being positive from the user’s point of view, this trend will create a big re-shuffling of current market equilibria: big vendors will be in the position to displace or take over competitors whose offerings will become transparent for end-customers. By means of market competition, however, this trend may lead to concentration of market power to a few giants. Such an oligopoly may influence end-user flexibility regarding their needs, costs and security with regard to the offered services.

New generation IT Infrastructures implement multi-layer architectures that neutralise from the peculiarities of individual hardware and low level functional dependencies. While the configuration and management of these systems is being performed at the application level, inherent dependencies with the heterogeneous subsystems (hard- and software) pose technical, operational and security challenges.

3.3.2 Security challenges next gen IT

Multi-layered, virtualized architectures have the advantage of abstracting from peculiarities of sub-systems. Multiple systems may be independently defined on a common hard- and software platform and then be managed by means of a hypervisor. Next generation systems are delivering thus a more comprehensive and coherent view to the operators and to the end-users. The implementation of such functions, however, needs to support translation of user actions over various logical and system layers into the particular system-specifics of underlying components.

This kind of back-and-forward translation and execution bears security risks, in particular if the short innovation cycles of underlying (hardware) systems is taken into account. It is worth mentioning, that most popular next generation infrastructures in the context of this discussion are software defined networks and 5G.

These risks may be related to eventual weaknesses of sub-systems, errors in configuration, versioning, incompatibility, security gaps, etc. Moreover, the impact from materialization of such risks may be big, as it may affect operations of multiple tenants using the system.

The large number of users/tenants using the service is a motive for adversaries to target those platforms: if such a service can be compromised, access to a large amount of data can be obtained. Obviously, the manipulation options from such a breach may be quite broad. In general, next gen IT infrastructures will bring many security challenges, indicatively:

- Multiple options of weakness/vulnerability hunting due to big number of heterogeneous components;
- Efficient abuse of weaknesses/vulnerabilities due to multiple logical and physical layers;
- Multiple monetization opportunities through large number of services offered and users;
- Multiple attack scenarios due to various technical, procedural and business workflows implemented on these platforms;
- Multiple abuse cases due to various involved management/administrative roles involved (esp. insider abuse);
- Inefficient cross-layer implementation of security measures introducing protection gaps;
- Too many ways to circumvent existing security controls by abusing multi-layered architectures.

Estimated timescale for rollout[5]: 5 to 10 years

Takeaways next gen IT-infrastructures

- Traditionally, security abuse takes place between system layers. Next gen IT encompasses a lot of layers and components which increase abuse cases.
- Just as with cloud infrastructures, next gen IT will be an attractive target due to the large volume of information that can be breached.
- Flaws of components involved in virtualized infrastructures may affect confidentiality and integrity of data.
- New ways to understand the interplay and architectural requirements of new virtualized infrastructures; establishment of security protection in accordance.

3.4 Virtual and Augmented reality / Gamification

Generally speaking, virtual reality and gamification technologies are used when decoupling a process from its physical pedant is desirable. This technology allows simulation of catastrophic events without actually experiencing them. Simulation is very common in training when the trainee wants to obtain skills for professions which – when performed in real life – may bear significant risks. Examples can be found in medicine, aerospace, underwater, military, etc. As far as the decoupling between the cyber and physical spaces are maintained, the relevance of virtual reality and gamification to cyber security is rather low. This will change, when the virtual and physical words start getting connected. Nonetheless, virtual reality and gamification has significant relevance to privacy.

3.4.1 Technological Challenges

Virtual and augmented reality (VAR) is a technology area that has made significant improvements towards going to production phases[3,10]. Depending on the sector/domain in which virtual and augmented technology is being used, it may be quite intrusive and/or crucial for human activities, especially when used in sectors like medicine, military, aviation, space, etc.

Virtual and augmented reality is being used within gamification by means of games, both serious and for fun. As such, it is being utilized by a very wide user community in a wide spectrum of applications. Current challenges regarding this technology are related to the display and to the capture of user feedback through sensors.

Being a collection of highly interacting components, virtual and augmented reality bears the challenges of complex systems regarding robustness of architecture, as well as reliability of connected components (see also challenges in next gen IT infrastructures above).

3.4.2 Security Challenges

Security challenges in virtual and augmented reality resemble those of complex, highly interconnected multi-component environments. Moreover, VAR will offer an additional field to collect data about user habits. This information may be of intimate nature, and, depending the filed in which VAR is used, may be misused to affect human life.

As in other emerging technological areas, VAR is a challenge for cyber-security be means of:

- Security and privacy implication from VAR information misuse;
- Role of confidentiality, integrity and availability requirements for information processed and functions provided by such systems;
- Weaknesses from usage (i.e. addiction, confusion, etc.), operation, maintenance;
- Insider abuse scenarios;
- Threat exposure due to weak integration of components.

Estimated timescale for rollout[5]: 2 years (Virtual Reality) to 10 years (Augmented Reality)

Takeaways next gen IT-infrastructures

- Security requirements of this technology area need to be understood
- VAR will deliver new attack surfaces and weaknesses
- VAR misuse implications/impact still subject to assessments

[10] http://www.bbc.com/future/story/20160729-virtual-reality-the-hype-the-problems-and-the-promise

3.5 Autonomous systems (e.g. vehicles)

3.5.1 Technological challenges

Autonomous systems is one of the emerging technologies that finds currently a gradual implementation in the sector of autonomous vehicles. Though experiencing some successful show-cases[11] and providing positive predictions about product development, autonomous systems often deliver headlines related to failures[12].

For obvious reasons, testing is undoubtedly one of the most important, yet laborious tasks for the product deployment of autonomous systems[13]. Scientists see a number of challenges related to testing, in particular:

- Mastering the complexity of the environment of the autonomous system;
- Managing complex soft- and hardware, including integration and interfacing with a large number of situational parameters and eventually other complex systems;
- Mastering the maintenance of all these components, given the variety in the life-cycles of heterogeneous components.

Moreover, some additional technology challenges relate to fault tolerance, trust in functions and resiliency:

- Given the fact that configuration errors and device failures are frequent sources of system failures, there is a need for increasing of fault tolerance, fault avoidance and fault removal. This property turns to be inevitable in autonomous systems, especially with the ones that are relating to human life;
- Establishment of trust to the system functions and the operation of autonomous systems;
- Even in cases of failures, autonomous systems will need to be in the position to adjust their functional characteristics to the new situation and fall back to secure states for the entire ecosystem they operate in.

3.5.2 Security challenges

The security challenges in the area of autonomous systems emerge from the resiliency requirements, as well as from the trust and integrity requirements. It is worth mentioning that in autonomous systems the interplay between security and safety will need to be better understood: due to typical engineering legacies in the area of autonomous systems many (trust) requirements are based on safety. In elaborating security issues of such systems, one will need to understand the use of security controls to ensure safety, but also elaborate on the impact of security failures to safety. More specifically:

- Autonomous systems resilience is their ability to survive various classes of failures without falling into states that may cause personal injury, loss of life or severe damage or loss of assets. Such assets may be the ones controlled by the autonomous system or are directly/indirectly belong to the environment the autonomous system. In order to achieve this, continuity mechanisms, fail over and redundancy mechanisms need to be maintained. In addition, security mechanisms will be necessary to protect the run-time environment in all its phases, from development to its operation.

[11] https://www.wired.com/2017/04/detroit-stomping-silicon-valley-self-driving-car-race/, accessed April 2017.
[12] https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html?_r=0, accessed April 2017.
[13] https://www.researchgate.net/publication/305622163_Testing_of_Autonomous_Systems_-_Challenges_and_Current_State-of-the-Art, accessed April 2017.

- One of the most challenging requirements that needs to be covered by autonomous systems is trust. This trust relates to the establishment of trust functions among the various components of the system so that they cannot be faked/maliciously changed. Moreover, trust relationships need to be in place in order to guarantee authenticity in the interaction with other components/systems that are external to the autonomous system. This is particularly important for autonomous vehicles as they will probably be critically dependent in information exchanged with the outside world (e.g. GPS and traffic information). Finally, trust in the security of various critical functions of the autonomous system per se needs to be established (e.g. non-repudiation of processed information). The entire range of trust functions can be implemented by using security function, merely based on cyphers (e.g. block chain, authentication, data signatures, certificates, etc.).
- Besides the availability requirements posed by resilience (see bullet above), maintenance of integrity is another basic function needed by such systems. Besides the non-changeability of existing functions and processed information while on the flow and at rest, such systems need to maintain non-repudiation of performed activities. This will be required, given that such systems may affect human life (e.g. through accidents).
- Trust is particularly important in autonomous systems: the complexity of such systems and the severe impact (i.e. loss of life) of failure or malicious action opens the question on the trust among the involved components. Taking into account potential ad-hoc interconnections among such systems (i.e. via M2M), it becomes clear that models of trust for interacting systems will need to be developed.

Estimated timescale for rollout[5]: more than 10 years

Takeaways autonomous systems

- Autonomous systems need to interact with other components based on some trust models.
- Resilience of autonomous systems will reach new qualities, given their potential role in traffic and health.
- Autonomous systems will eventually require novel approaches in security mechanisms, especially in their interaction with less reliable devices such as sensors, eventually belonging to IoT environments.

3.6 The Internet of Bio-Nano Things (IoBNT)

3.6.1 Technological challenges

After the introduction of the Internet of Things[14], scientists elaborate on the possibility to combine Internet-enabled devices with miniaturization and biological processes. It is being envisaged that technology will provide “tools to control, reuse, modify, and reengineer the cells’ structure and function, and it is expected to enable engineers to effectively use the biological cells as programmable substrates”[15]. In this context an implementation of Bio-Nano Things as biological embedded computing devices is being considered as a main enabler.

[14] https://www.scientificamerican.com/article/the-internet-of-things-goes-nano/, accessed April 2017.

[15] https://bwn.ece.gatech.edu/papers/2015/j3.pdf, accessed April 2017.

If seen together with developments in DNA research, biocomputing[16,17] and advances in e-health and medicine, IoBNT opens up numerous avenues for technological breakthroughs where cyber becomes part of and controls vital human biological processes[18].

Such a development will bring massive challenges to technology, including ethical, social, legal economic and political aspects, to mention the most imminent ones. Though the effects of these developments are difficult to assess by now, technologist will need to be aware that a lot of work will be necessary in order to cope with such challenges.

3.6.2 Security challenges

Coverage of security issues in IoBNT will bring massive challenges for security and cyber-security: level of protection will be the highest possible, as the assets to be protected are the building blocks of life and health. Moreover, trust in the functions and in the communication between all involved components will be of great importance. Finally, requirements of identification, accountability, non-repudiation and integrity functions will be decisive for the development and deployment of IoBNT.

Estimated timescale for rollout[5]: more than 10 years

Takeaways IoBNT

- IoBNT will bring enormous challenges for information security / cyber-security. This is because of the interdisciplinary nature of assets involved in this sector.
- An initial risk assessment of these technologies will be absolutely vital to understand the implications of this technology.
- Due to the nature of the application area and the very nature of the involved components and their interaction, it will be necessary to expand existing security techniques in order to achieve the required protection needed.

3.7 AI and Robotics

3.7.1 Technological Challenges

Artificial intelligence (AI) in computer science AI refers to computer systems/services/applications that perceive their environment and use this potentially incomplete data from the environment to maximize the success rate of completing a certain task. AI techniques and methods can range from simple decision making algorithms, to pattern recognition and data mining, as well as to deep learning and other reinforcement learning techniques to name a few. Interesting showcase examples of AI include robotics, autonomous driving, drones, medical diagnostics, personal assistants, etc.

- Complex and large landscape: Robotics and AI build on a wealth of information that enable intelligent decision making. AI and robotics go hand-in-hand in facilitating the deployment of intelligent, adaptive, context-aware services and applications. It is therefore evident that the complexity of securing AI touches upon many areas and domains, hence security controls need to be adaptive and operate in

[16] https://singularityhub.com/2017/04/12/scientists-hacked-a-cells-dna-and-made-a-biocomputer-out-of-it/, accessed April 2017.
[17] http://www.nature.com/nbt/journal/vaop/ncurrent/full/nbt.3805.html, accessed April 2017.
[18] https://futurism-com.cdn.ampproject.org/c/s/futurism.com/kurzweil-by-2030-nanobots-will-flow-throughout-our-bodies/amp/, accessed April 2017.

these coordinated settings. This kind of security controls are novel and are still subject of new development.

- Financial costs: the wide penetration of AI in several critical sectors denotes the potential of significant financial costs associated to cyber security, compared with the ones needed for the replaced components/humans.
- Omnipresence: while AI is rightly heralded as one of the technologies that bring about both a societal and technological paradigm shift, it might be established as something that people rely on, without giving too much awareness to associated risks. As with most innovations, in its adoption phase it is more prevalent to consider the benefits of AI without much consideration to its shortcomings.
- Large supply chain: there is a great number of stakeholders involved in every AI solution, e.g. software developers, hardware manufacturers, network providers, software providers, service providers of big data/machine learning solutions, data exchange protocols, mathematicians, etc. to name a few.
- Algorithmic integrity: AI usually being a black box does not allow for algorithmic verification, whereas the dynamic and evolving nature of said algorithms hinders forensic efforts. The problem is exacerbated by the fact that algorithms are tightly linked to the data that was used to train and test them, which when modified can lead to whole different algorithm behaviours. Therefore, verification of the aforementioned algorithms to ensure they are not biased and are secure and trustworthy is of high importance.

3.7.2 Security Challenges

AI technologies facilitate intelligent and automated decision-making and are thus a prerequisite to the deployment of IoT and Industry 4.0 scenarios. The paramount need for security in such scenarios, therefore naturally extends to AI. By analysing existing material on AI and robotics, ENISA has identified a series of cybersecurity challenges. Though not exhaustive, the cyber-security risks and challenges below are indicative:

- Trust: given the particularity of AI that supports automated decision making often not considering human input at all, the notion of trust emerges as being of paramount importance. Robotics systems need to interact with other components based on some trust models. How this trust is built into such AI-based systems, how it is propagated in a chain of trust, how it can be used to promote user awareness and how it can be used to raise concern over security implications, are among the open challenges in the domain.
- Very large attack surface: the threats and risks related to robotics and AI are manifold and they evolve rapidly. With great impact on citizens' health, safety and privacy (data collection and processing may be unclear to the users), the threat landscape concerning AI is extremely wide.
- Complex landscape: security concerns are exacerbated since AI and its application on robotics should not be seen as a collection of standalone algorithms and solutions, but rather as a rich, diverse and wide ecosystem involving aspects such as software, hardware, data, devices, communications, interfaces, and people.
- Uncertainty: The very nature of autonomous robotics systems relies on a certain degree of uncertainty, given the lack of deterministic such systems. Security controls need to consider this aspect and provide appropriate solutions.
- Transparency: transparency of decision making implies the need for AI to be able to justify the cause of actions and the logical flow of decision making. Why a decision was taken is something to be made available to regulators and users alike, to increase trust and appropriate responsibilities if needed. Acceptance and hence adoption of robotics relies on such transparency.

- Widespread deployment: apart from commercial applications of AI (e.g. smart notifications regarding wearables), recent trends see Critical Infrastructures (CIs) migrating toward Smart ones by employing AI on top of legacy infrastructures, namely Industry 4.0 (e.g. robotics in manufacturing). Dynamic security controls to cater for the different context under which said systems will operate need to be considered.
- Safety and security process integration: this is a very challenging task since it involves possibly contradicting viewpoints and requirements from all involved stakeholders. Safety challenges are in their own extremely high in the agenda. Security for safety should be promoted since AI decisions and actions of robots can have serious and solid effects on the physical world.
- Repercussions for personal data and privacy: AI may lead to concentration of massive knowledge about user behaviour within few organisations/companies. It will be a challenge to guarantee compliance of this concentration with privacy regulation and information security practices. Moreover, the need for AI to collect and process data is likely to impact the behaviour of consumers as their personal data and privacy might risk to be disclosed to illegitimate parties. In this respect the way consent is provided, the way an application on AI operates, the way data is relayed from one algorithm to another, etc., need to be further analysed.

Estimated timescale for rollout[5]: 5 to 10 yeas

Takeaways AI and Robotics

- There is a need to understand the building blocks of AI and robotics technologies AND their interplay. Based on this (technological) information, security experts will be in the position to identify their risk exposure.
- Threats and weaknesses pertinent to the components of AI and robotics have to be assessed. Given the wide scope of use of these technologies, this assessment needs to include both technical and non-technical issues.
- Both social and technological issues identified need to be addressed by policy: the role of various stakeholders will need to be identified; the level of necessary guidance through governments; the interface to various existing regulation, etc.
- It is important to ensure security in all stages of the life cycle of products and services, especially in the design, development phase (testing, because of API reuse), and the usage and maintenance (security patch, especially when using third-party security functions/API).

4. Consolidation of collected ideas: Emerging Security Related Areas

4.1 Certification

Through mobile computing, smart devices and IoT, security protection is relevant for many families of devices and commodities. This increases the need for a seal regarding certifying existence and efficiency of security functions, in a similar manner to seals used for electric appliances[19].

Existing certification schemes, however, are too "*heavy*" (i.e. expensive, rigid, narrowly scoped and static). These properties are not "*compatible*" with the characteristics of IoT devices that are short-lived, inexpensive and may rapidly change their mode of operation. In many cases, the effort to obtain a certification of security functions may drastically lower the economic benefits emerging from the product marketing. This fact acts as a disincentive to security certificates.

Over time, various ideas for security certification have been developed in order to overcome the deficiencies mentioned.

One of those ideas is related to the creation of artificial exposure of devices via simulated cyber-threat landscapes. This would show the level of resistance/protection offered by various security products. Though not formal, such an approach could be a pragmatic, economically efficient way to check the security level offered by commercial products. A similar approach is followed by the commission in the area of research (H2020) by means of an open call[20].

Other existing ideas include trustworthiness models for vendors and/or components (both hard- and software). In such a scenario, evaluators are called upon to assess the effectiveness of security functions based on knowledge of the utilized architecture and exposure scenarios (see also discussion on trustworthiness below). Whereas the latter option is similar to the one mentioned in the paragraph above. Software liability may be an area that will impact the developments in innovative, short living components/technologies.

ENISA has a series of activities in the area of security certification of products[21] and supports the commission and Member States to establish a framework for mapping Europe-wide available certification standards. As an additional element hereto, both stakeholders and ENISA plan to elaborate on lightweight certification schemes to be applied to retail hard- and software components deployed in consumer-oriented environments and applications (e.g. IoT, eHelath, connected home, etc.).

It is worth mentioning, that in its proposal on a Regulation of the European Parliament and of the Council on the future of ENISA, the European Commission has delivered a draft of potential content for certification[22]. This draft is subject to negotiations with EU Member States and stakeholders.

[19] http://www.atbatt.com/laptop-chargers/adapter-safety-mark, accessed April 2017.
[20] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/ds-01-2016.html, accessed April 2017.
[21] https://www.enisa.europa.eu/events/ict-security-certification-for-industry/security-certification-of-ict-products-in-europe, accessed April 2017.
[22] https://www.enisa.europa.eu/news/enisa-news/european-commission-proposal-on-a-regulation-on-the-future-of-enisa, accessed September 2017.

Takeaways Certification

- Existing certification schemes are not appropriate for lightweight devices similar to the ones found in IoT.
- Novel approaches for the development of alternative methods to check the cyber-security functions will be necessary.
- ENISA supports the Commission in consolidating existing approaches.

4.2 One virtual terrain, many actors: civil, LE and military societies on cyber-space

The cyber-space is the virtual terrain on which various criminal/illegal/offensive acts are taking place. When notified upon the existence of such incidents/acts, various professional actors who own IT-components at stake will take some actions to protect their assets. Similarly, national security, law enforcement and military forces may intervene to take care of the effects of cyber-incidents.

Just as in a real space/territory, a serious security incident will attract the simultaneous attention of national security, law enforcement and eventually military forces. Due to lessons learned from this field, it is apparent that the deployment of forces acting in the terrain of the incidents reserves careful coordination. Otherwise the risk does exist to create more harm through the rescue forces than the incident itself.

The fact that the cyber-space is practically virtual and attribution is difficult makes the coordination of the acting organisations even more difficult, yet critical. If seen in combination with the fact that the regulatory frameworks for coordinated action of various forces is not yet in place, it becomes apparent how urgent this matter is, in particular in a cross-border, pan European manner[23].

This has been already understood by the relevant community. Cyber-crisis management cooperation is considered as one important matter that needs to be taken forward, both at the level of Commission[24] and ENISA[25]. Given the draft provided by the commission on the future of ENISA[22], it is expected that quite some developments will happen in this area in the coming period.

Takeaways coordination of actions

- Like in other areas of life (e.g. crises, catastrophic events, etc.) it will be necessary to coordinate activities of various players including defence, law enforcement, rescue forces.
- Cyber-crisis cooperation is an important area that needs to be addressed.

4.3 Trustworthiness

Trustworthiness, a collection of characteristics that make an entity trustful with regard to an interaction with others. The need to become trusted among various interacting parties is not a new security issue. This

[23] https://www.eu2017.ee/news/press-releases/estonia-conduct-first-cyber-defence-exercise-defence-ministers, accessed September 2017.
[24] http://europa.eu/rapid/press-release_MEMO-16-2322_en.htm, accessed April 2017.
[25] https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation, accessed April 2017.

need has emerged in e-commerce over the past decade. Various models have been developed, some based on strong authentication (e.g. PKI based) and others are based on reputation models[26].

While such models fulfil their purpose, e.g. within e-commerce platforms and transactions, they might not necessarily be applicable to various emerging technology areas as the ones mentioned in section 4. We expect that various new trust models will be developed, in particular for components establishing communication in ad-hoc manner via wireless protocols. Such models will be necessary in order to achieve the data protection / data privacy that is appropriate in order to obtain the necessary user trust.

A challenge that has to be addressed by authentication based systems is definitely scalability: given the number of devices/services and the large number of interactions, the performance of the authentication process (including the processing of involved credentials) may be a limiting factor for deployment.

Given multi-vendor and ad-hoc manner of interoperability of components, it is expected that existing trust infrastructures (e.g. ones based on PKI, encryption, etc.) will need to increase their interoperability in order to mutually recognise trusted components. This need will lead to new business models for trust infrastructure providers. Moreover, the necessary functions and infrastructure may be part of "all-inclusive" service portfolios of globally acting big players engaged in related fields. It can be expected tht trust and trustworthiness may cross-fertilize the area of certification.

Takeaways trustworthiness

- New trust models will be developed to accommodate the needs of ad-hoc components interactions.
- Existing and new trust infrastructures will need to fulfil necessary interoperability and performance requirements.
- Trust models will be important for the acceptance of the service offerings and can be thus seamlessly integrated in service portfolios.

4.4 Security coverage of complete lifecycle

Given the complexity and of current and future infrastructures, systems, applications and services, the coverage of security during the complete life cycle of all kinds of IT-products is inevitable. Including security in all phases of IT-products covers design, development, testing, procurement, operation, management and phase-out. IT-product liability is an issue that will require attention in the coming time[27,28,29]. Together with proper configuration and maintenance of the components from the user side, security coverage of the life-cycle is one of the conditions for the achievement of liability of IT-products. This service level will need to be kept during the entire life-cycle of products, often having lifespans up to few decades[30].

There is one more important reason for including security in the complete lifecycle, namely the possibility to implement a holistic security management or integrate the relevant component in an existing security management system.

[26] http://courses.cs.washington.edu/courses/cse522/05au/reputation-ebay.pdf, accessed April 2017.
[27] https://threatpost.com/software-liability-is-inevitable/114136/, accessed April 2017.
[28] https://devant.co.uk/software-companies-new-liability-under-the-commercial-agents-regulations-1993/, accessed April 2017.
[29] https://www.itnews.com.au/blogentry/software-liability-is-coming-447800, accessed April 2017.
[30] http://plcwhatisplcscada.blogspot.gr/, accessed June 2017.

The ability of a component to be integrated into an overall security management system is very important: in the emerging technology areas mentioned above, the availability of security management is an enabler for the achievement of acceptable security and protection levels. Moreover, one can make the assumption that most of the professionally used IT-Infrastructures will be part of a security management system.

A final point that can be made here is the need to encompass agility both in the ability of components to integrate to existing security management platforms, and the ability of security management platforms to adapt to the changing threat landscape.

Takeaways security lifecycle

- Inclusion of security in product development lifecycles is a precondition for the necessary improvement of security in infrastructures of all kinds.
- Inclusion of security in product development lifecycles increases agility with regard to changing threat environment.
- Security in product development lifecycle is the only way to incorporate IT-components into holistic security management schemes.

4.5 Upcoming issues in the area of Encryption

Currently, we see a race between those who want privacy, e.g. encryption, and those that want security through surveillance. In 2016, there is evidence that the privacy vs. national security battle is as uncertain as never before. Various states tend to develop own interpretations on how cyber-security and surveillance will be implemented in order to ensure national security[31].

Nonetheless, having different encryption and privacy regulations, new encryption “legislation geographies” are created. Citizens on the move within these areas may find their compliance status changing. This is a similar situation as older generations have experienced when strong encryption was restricted in the US by law[32]. Given that ca. half of the internet traffic is already encrypted[33], national security sees this as an increasing obstacle in gaining intelligence from data communications.

At the same time, states and industry work on censorship functions and on control of massive traffic streams/bandwidths. And political developments show a trend towards de-globalization. This may lead to control centres of big parts of the internet. Such entities may be in the position to exert their power to all nations and individuals who have caused this traffic[34]. The tension created by this diverging development will certainly bother the cyber-security community in the future.

As regards competition, it is considered meaningful to bundle existing EU-capabilities in cryptography. European competitive advances in areas such as key management, hardware crypto, identification methods, encryption and data protection belong to core of EU capabilities. Any relevant resources, skills and knowledge hereto should be consolidated and used within engagement and support frameworks (e.g. EU programmes, Member State supported development plans, etc.).

[31] https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper, accessed June 2017.
[32] https://en.wikipedia.org/wiki/Export_of_cryptography_from_the_United_States, accessed June 2017.
[33] https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/, accessed June 2017.
[34] http://www.iisp.gatech.edu/sites/default/files/documents/2017_threats_report_finalblu-web.pdf, accessed June 2017.

In particular, European advances in medical device certification standards and regulation may be considered in order to impose high European security requirements for such devices and implement competitive advantages for European vendors of that are engaged in this market.

Last but not least, new models for use of cryptography are being developed in an attempt to secure component interactions within IoT environments/applications. This trend is quite strong and is related to the implementation business processes on IoT infrastructures, such as e-payment options via digital currencies. It is expected that usage of encryption will be a key technology for securing such interactions both within IoT but also other technology areas.

Concluding this section one should mention the importance of technological advances: secure encryption schemes and protocols, for instance in the light of Quantum Computers, and possible other mathematical breakthroughs will be crucial. Both from the defenders and offenders sides. Such developments make a working crypto an indispensable component.

Takeaways security encryption

- At nation-state level encryption is seen as a barrier in lawful surveillance. Nation-states will invest resources in overcoming these barrier.
- Vendors/providers are interested in weak data protection that will allow them to have a better international presence with uniform security standards that will ease product development/integration efforts[35].
- EU should capitalize on existing advances of encryption technology and services in this area to implement global market leadership.
- New usage models for encryption functions are under development. This will boost the need to include encryption functions in soft- and hardware products.

4.6 Identification

Just as now, identification will be in the future THE function in all kinds of interconnected technologies, individuals, components and all other identifiable objects in cyber-space. Identification is a necessary prerequisite for trust, but also non-repudiation, that is, the non-debatable evidence that an action has happened between two or more identifiable subjects.

Currently, most forms of identification cover human subjects and are used mostly within authentication. Moreover, quite some identification/authentication methods have been developed for non-human subjects. In both cases, identities are one of the most desirable objects for cyber-criminals. For obvious reasons, personally Identifiable Information (PII) tops breached data.

Recent research shows the shortcomings in current implementation of cutting edge, widely deployed biometric authentication methods[36]. Would such an authentication mechanism implementation be used within e-health or financial applications? Obviously not; therefore it is necessary to (pre-) invest efforts in identification/authentication methods that are appropriate for emerging technologies in order to avoid sever incidents in critical IT systems.

[35] http://www.spiegel.de/wirtschaft/soziales/tisa-leaks-wie-das-dienstleistungsabkommen-den-datenschutz-gefaehrdet-a-1122844.html, accessed June 2017.
[36] https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html, accessed April 2017.

Two other equally important aspects in cyber-space that are subject to identification is anonymity and attribution. Though being two sides of the same coin, both anonymity and non-repudiation of actions are two functions/qualities that need to be supported by identification mechanisms. They bring an additional dimension in the complexity of the entire identification area.

Finally, due to the rich digital footprint of users (e.g. summary of all digital traces), the notion of identity in general needs to be reconsidered, as it goes far beyond typical identities as covered by today's functions, products and services. Moreover, identities of non-user components such as autonomous systems, will become increasingly important, as they are going to undertake important functions of human life.

Takeaways identification

- The interplay between identification and trust needs to be investigated.
- The notion of anonymity, identity and non-repudiation need to be put in common basis and considered in modern IT infrastructures, also with respect to privacy and security requirements.
- The notion of identity needs to be put to a wider basis, as multiple user data allow for the definition of exact profiles matching single users in the internet.

4.7 Artificial Intelligence (AI) and Machine Learning (ML) as cybersecurity tools

AI/ML and IoT seems to be an interesting combination that gains in speed: AI and ML can be used to semi-automatically or automatically supervise simple tasks within an IoT environment[37]. This can be achieved by leveraging on available knowledge/data (massively) created by interacting components/sensors. This can be a great advantage given that fact that the internet never forgets. Such information could be used to perform corrective actions of component interactions, thus increasing security and resilience.

Just as for many application areas, ML and AI are both interesting within cyber-security. They can be used to detect attacks by identifying anomalies in operational or communication patterns of components. Similarly, ML and AI can be used in the discovery of interrelationships required in the collection of cyber-threat intelligence, hence establishing context out of mass data. Similar activities are already reported in the area of big data and national security[38].

The use of ML and AI in security may also support the autonomous supervision of infrastructure and application areas with regard to security management policies. To this extend, ML and AI will contribute towards the revision of policy implementation and oversight that has been typically performed by humans to a great extent. In this way, ML and AI may achieve costs reduction and increase of efficiency towards secure operations.

Takeaways security AI and ML

- AI and ML are important tools in the area of cyber-security. The can be used for context discovery in the area of Threat Intelligence (TI).
- A second very promising area is the use of ML and AI in the identification of attack patterns (i.e. based on TI) and facilitation of security management/policy implementation supervision.

[37] http://telecoms.com/480122/ericssons-big-black-box-full-of-ai-goodness-intrigues-at-mwc-2017/, accessed June 2017.

[38] https://www.washingtonpost.com/news/monkey-cage/wp/2017/09/27/national-security-relies-more-and-more-on-big-data-heres-why/?utm_term=.4072fff3ca40, accessed September 2017.

- AI and ML will be target to attacks. They might open new avenues in manipulation and attack methods.

4.8 Getting end-user more involved

There is no doubt that cyber-security knowledge needs to be transferred to end-users. Numbers from incident analysis show that over 50% of the incidents are due to common/basic user errors[39,40]. This makes clear that user awareness, can become the most efficient security control by means of cost/benefit ratio.

Awareness actions for cyber-security do exist and education efforts are ongoing. Thought many initiatives cover end user training, there is still plenty of space for improvements. Some examples are: security and education, improvement of information awareness of decision makers, better enrolment of user in managing security of their devices/applications, target group oriented methods for communication of security information. The list and width/depth of this matter is quite wide. We believe that end-user security is an important area that is not growing in analogy to the digitalization of the society.

Last but not least, it is known that there is a significant shortage in cyber-security skills. This need will be further intensified in the future. New types of organisations from the area of military come to complete the picture of big white-hat cyber-players. Yet the question is how to fill the gap in cyber-security and cyber-threats skills. Is the enlargement of cyber-warfare going to affect other, commercial areas? This is a difficult question given that already today, a wide grey area does exist among cyber-crime, cyber-warfare, cyber-espionage, vendors, researches and other commercial organisations.

There is no question that the security community has to let people know more about it and decision makers need to create more capacities to better educate people at all levels of education.

Takeaways involving the end user

- Education and awareness on cyber-security needs to advance to include all levels and skills.
- Professional education needs to try covering the skill shortage in the market.
- Products need to take care of hiding complexity and supporting users to manage security parameters.

[39] http://www.cybersecuritytrend.com/topics/cyber-security/articles/421821-human-error-to-blame-most-breaches.htm, accessed June 2017.
[40] http://searchcompliance.techtarget.com/feature/Verizon-Human-error-still-among-the-top-data-security-threats, accessed June 2017.

5. List of topics University of Federal Armed Forces (Universität der Bundeswehr)

Participants of brainstorming session: Thomas Diefenbach, *Peter Hillmann,* Prof. Dr. Ulrike Lechner, Prof. Dr. Axel Lehmann

During our brainstorming session on 3rd March 2017, we have raised the following topics of mutual interest:

- Simulation of exposure to threats and materialization of risks is important, eventually by means of scenarios. E.g. based on those scenarios, serious games on cyber security can be generated.
- Organic computing as self-protective/adaptive system organisation. This paradigm might be useful in the context of resilience.
- Risk and perception of risks as a topic regarding own organisation. Perception of risks is an item that needs to be elaborated on.
- Prediction of botnet activity on the basis of system behaviour such as recognition of patterns, etc. seems to be an important element for research, simulation but also exercises.
- Threat analysis and threat landscaping, threat evolution, etc. is considered as an area of innovation. Seen in conjunction with novel tools for operations and risk management, this area is a challenge for the security community and the University in particular.
- Within a multi-project coordination effort, the University is involved in a project that covers IT-Security match-playing. The game is in German, however, any player from ENISA would be very welcome.
- Data sharing for surfacing emergencies is an area of activity covering the needs for military interventions in health matters. This experience is considered to be relevant for cyber-emergencies.
- Trace the operational pictures of security: consisting of measuring efficiency, social media aspects, mentioning in dark fora and in the web, evaluation of environmental parameters, etc.
- ENISA will consider the EUROSTARS call (part of H2020 framework) to assess the possibility of finding partners. This would enable the desired creation of synergies with the objective of product development.
- ENISA will establish contacts to its experts for future interactions in the areas of:
  - CIIP – Comprehensive and Integrated Infrastructure Program
  - Simulation (serious games)
  - E-health (ENISA provides access to available project/internal data)
  - Cyber exercises and emergency coordination
  - Networking (SDN – Software Defined Networks)

- On the basis of these interactions, the development of a yearly plan specifying delivery every 3 months will take place. These plans are subject to revisions based on the progress made.

6. List of topics received by Secunet

Participants of brainstorming session: Dr Rainer Baumgart, Thomas Pleines, Dr Kai Martius, Johan Hasse

IT topics
=========

AI
- what are the real improvements in threat detection with AI?
- can help AI for self-learning / self-improving systems?

# Augmented Reality / Virtual Reality
- influenced by security issues?
- just another (networked) application?

# Cloud
- will security concerns limit adoption and scalability?
(country-specific data centers already growing - re-localization)
- edge-cloud / smart dust concepts?

# Software Defined everything
- more standardization of hardware platforms
- fast config / software changes

security topics
===============

# Crypto
- (Post) Quantum Computer Crypto
- crypto agility at large
- Blockchain technology - hype or real innovator (making a simple technology broadly usable)

- Resource misuse 'and beyond' (DDoS..) -> resiliance

# Threat / attack detection
- currently fast growing;
- automation / integration (tools / products)
- authoritive CTI resources (business models vs. public need)

# identification / attribution
- stronger measures against identity theft
- stronger identification with anonymity option at the same time
- attribution problem in Cyber warfare

# trustworthyness of IT in general
- trust models / evaluation processes that scale with the innovation cycles

7. ENISA Permanent Stakeholder Group: Key Topics for Future Work Programmes

Below, a list of key topics for future work is presented. This list has been added after four years of interaction the ENISA PSG (2015-2017)[41]. Within this chapter we try to show the relevance of these points to the one mentioned in this report. This is being performed by means of a mapping between each identified top priority and the content of the crystal ball report.

Top priorities and challenges mentioned by PSG members in this respect include the following:

1. Implementation of the new cyber-security strategy
   Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

2. Cyber-security policy for the EU: Europeans dependence from external cyber security assets has been increasing rapidly. At the same time a large portion of European Cyber Security providers have been merged to foreign companies, or totally vanished. Only EU’s biggest countries still have governmental support to build competences and companies and tight governmental control for national security purposes. ENISA should support building European new cyber security policy, which would be reflecting the real situation. European current situation where EU MB's are having cyber security and policy defining assets, policy, hardware, standards etc. coming largely from one single non-European country, when in the same time fastest development, understanding European like dependency from external cyber security assets, is happening outside this one country. ENISA should either build policy which defends European only cyber-security assets and competences, or ENISA should make policy which should fully utilise international best practises and technologies which are coming countries having similar dependencies like EU and still build holistic Cybersecurity to protect digital sovereignty and citizen’s privacy.
   Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

3. GDPR and NIS guideline for European Industry: There are two major disturbances coming next year. GDPR and NIS directive. Both are changing cyber security rules fundamentally and are also for first time, entering the national cyber security policy space. Some national governmental stakeholders are facing the challenge not to be able to support and guide public, or private companies which will fall under one, or both directives. Now there is a clear need for clear communication and support even directly to these companies/Institutions.
   Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

4. Put the new ENISA mandate into effect
   Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

[41] https://www.enisa.europa.eu/about-enisa/structure-organization/psg/members/psg-2015-2017, accessed September 2017.

5. Focus on synergy of best implementation practices in Europe per security topic and community building i.e. become the hub of best practices made in Europe.
   Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

6. Focus on education by observing closely the NIS trends and assist in the creation of an NIS work force
   Relevance: See educational issues mentioned in section *Security challenges emerging from Societal Changes* and *Getting end-user more involved*

7. Provide flexible solutions on NIS matters and strengthen Europe as a security hub (economy and science – use and sell)
   Relevance: See European competitiveness mentioned in section *Upcoming issues in the area of Encryption*

8. Look into new technologies and new trends positioning
   Relevance: The entire crystal ball paper

9. Develop an EU Industrial policy for cyber security that is based on open solutions, innovation, and respect for privacy and fair competition
   Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

10. Community building around the development and support of open and innovative security technologies including cryptography, secure communications, distributed resilient systems
    Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

11. Examine the economic impact of NIS and develop standards
    Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

12. Coordination across different sectors
    Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

13. Joint Policy input- recommendations
    Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

14. IoT data flows: security assurances for users. With many sensors IoT devices are often (and often unexpected by users) collecting data. This holds not only for smartphones or hoovers and other robot-like devices, but also e.g. toys (puppets, toy tanks, etc.). It is important for users to know what data are collected and how, and where they may be flowing, so that users can make decisions about this. Given the often small user interfaces this is not easy. At the same time, it is important, that users get assurance, that the decisions on data flows are really respected and implemented by the IoT devices. So the security/privacy testing and evaluation of these devices is essential.
    Relevance: See challenges mentioned in section *Internet of Things.*

15. Privacy respecting identity management in eIDAS (electronic IDentification, Authentication and trust Services) context. Meanwhile the more and more eIDAS services are being established. Most of them deal with personal identities and identifiers. Often these identifiers are for assurance reasons spread through many entities (e.g. the “calling home effect” in in the STORK PEPS protocols), which is creating privacy issues, as too many entities are learning about the users’ interests and behaviour on the Internet. As now a number of real eIDAS services exist, it is time for a privacy analysis of these.
    Relevance: Privacy issues mentioned in security challenges of section *Trustworthiness* and *Identification* and *AI and Robotics*

16. Reacting to Cyberattacks: Cyberattacks are real existing threats, but it is still unclear what an appropriate response to these threats might be. Is it for example acceptable to start a counter-attack against the originator of a cyberattack, although it is known that the counterstrike has consequences for uninvolved nations, people, and infrastructures? For this reason it is important to establish useful rules and measures, which take into account the juridical status on the national / EU level as well as political, social and ethical requirements.
    Relevance: Coordination issues mentioned in section *One virtual terrain, many actors: civil, LE and military societies on cyber-space*

17. Industry 4.0: The digitalisation of the industry provides various challenges regarding IT security. To maintain and increase the competitiveness of products supplied by European manufacturers, it is important to raise the IT security level in the industry. Therefore, it is necessary to create common framework conditions and regulations for Industry 4.0 applications and infrastructures to establish a high IT security level within the EU.
    Reference: Security challenges mentioned in sections *Internet of Things, Next Generation IT infrastructure* and *AI and Robotics*

18. ENISA to define the roadmap for an integrated and robust NIS strategy
    Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

19. Influence and educate the MS through PSG’s support
    Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

20. Harmonisation in NIS practices
    Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

21. Take IoT and CIIP beyond national strategies
    Relevance: Technological and security challenges mentioned in Section *Internet of Things.*
22. Colonise new NIS areas and influence policy
    Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

23. Increase the activity of cyber- exercises: incidents like Wannacry, Petya, or Dyn Attack past october’16 have demonstrated we need more simulations or testing of crisis situations, national crisis and how to

coordinate at national level and European level these situations. There are too many actors to coordinate, Member States, Europol, CERT-EU, ENISA, etc. Enforcing and increasing the activities of cyber-exercises could give to the Industry (mainly Critical Operators) new capabilities and also improve current capabilities. Organising one Cyber-Europe exercise each two years could be poor, as there is a need to test, to train, to stress organizations, to prepare for next incidents and new situations. Make it possible for PSG members to participate as observers during the cyber-exercises. PSGs could be counsellors, proposing new topics and scenarios, studying and analysing the activities and also improving with more lessons learned the reports on results.
Relevance: Coordination aspects mentioned in section *One virtual terrain, many actors: civil, LE and military societies on cyber-space*

24. Assist in the creation of a cyber-security engineer official degree. ENISA and PSG Members could be an advisor, or counsellor in this matter.
Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

25. Data sovereignty and digital sovereignty at EU level.
Relevance: CONSIDERED AS NOT DIRECTLY RELEVANT TO EMERGING TECHNOLOGY AREAS

26. Network Functions Virtualization (NFV) helps service providers become more agile and reduce their costs. However, NFV's new architecture, operations, and openness create new security challenges. Those challenges must be overcome for service providers to scale NFV and earn its business benefits. The needs here are a risk identification methodology, followed by a careful review of the top security risks when migrating services to NFV. The intent is to provide security practitioners with a basis for developing a documented risk dashboard in order to bring down the overall security risk to an acceptable level when migrating to NFV.
Relevance: Virtualization issues mentioned in section *Next Generation IT infrastructure*

27. 5G: As observed by 3GPP today, 5G networks will require complex security requirements at different layers within the system. Moreover, with standardization at an early stage, innovative security solutions proportionate to the threats will have to be built into the network from the very start. This approach will protect subscribers, devices and their communications, as well as the integrity of the network itself-whatever the use case. Investing in 5G security now is also a wise insurance policy to avoid unexpected costs that might arise later from countering attacks or from suffering the consequences of insufficiently protected high-value data. The wrong decision about security today will only prove to be false economy in the future.
Relevance: security issues mentioned in section *Security challenges next gen IT*

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