European Commission

Scientific Advice Mechanism (SAM)

Cybersecurity

in the European Digital Single Market

High Level Group of Scientific Advisors

Scientific Opinion No. 2/2017

Research and Innovation

EUROPEAN COMMISSION

Directorate-General for Research and Innovation
Unit RTD.01 – Scientific Advice Mechanism (SAM)

E-mail: EC-SAM@ec.europa.eu
RTD-PUBLICATIONS@ec.europa.eu

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Scientific Advice Mechanism (SAM)
INDEPENDENT SCIENTIFIC ADVICE FOR POLICY MAKING

Cybersecurity
in the European Digital Single Market

High Level Group of Scientific Advisors
Scientific Opinion 02

Brussels, 24 March 2017

2017 Directorate-General for Research and Innovation

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

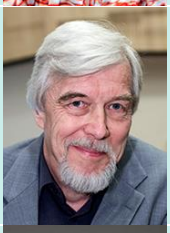
Luxembourg: Publications Office of the European Union, 2017

Print	ISBN 978-92-79-66218-8	doi:10.2777/978703	KI-01-17-149-EN-C
PDF	ISBN 978-92-79-66217-1	doi:10.2777/466885	KI-01-17-149-EN-N

Table of Contents

ANNEXES

High Level Group of Scientific Advisors

	**Janusz Bujnicki** **Professor, Head of the Laboratory of Bioinformatics and Protein Engineering, International Institute of Molecular and Cell Biology, Warsaw**
	**Pearl Dykstra** **Deputy Chair** **Professor of Sociology, Erasmus University Rotterdam**
	**Elvira Fortunato** **Professor, Materials Science Department of the Faculty of Science and Technology, NOVA University, Lisbon**
	**Rolf-Dieter Heuer** **Chair** **Former Director-General of the European Organization for Nuclear Research (CERN)**
	**Carina Keskitalo** **Professor of Political Science, Department of Geography and Economic History, Umeå University**
	**Cédric Villani** **Director, Henri Poincaré Institute, Paris**
	**Paul Nurse** **Director of the Francis Crick Institute**

ACKNOWLEDGEMENTS

This Scientific Opinion was delivered by the High Level Group of Scientific Advisors to the European Commission on 24 March 2017, following a request by the Commission which was accepted by the High Level Group on 29 January 2016.

The High Level Group Members Rolf-Dieter Heuer, Pearl Dykstra, Janusz Bujnicki and Cédric Villani were in charge of developing this Scientific Opinion which has been endorsed by the full Group.

The High Level Group wishes to thank the many contributors for the support they have provided to this Scientific Opinion:

The European Academy organisations – especially to Academia Europaea (AE), All European Academies (ALLEA), the European Academies Science Advisory Council (EASAC), the European Council of Academies of Applied Sciences, Technologies and Engineering (Euro-CASE) and the Federation of European Academies of Medicine (FEAM).- members of the consortium of the 'Scientific Advice for Policy by European Academies' (SAPEA) project supported under Horizon2020.

The many scientific experts and stakeholders from the science, policy, industry and civil society communities that have contributed to the development of this Opinion (list in annex 5).

The services of the European Commission, in particular DG CONNECT, DG HOME and DG JRC.

The scientific support team at the SAM Unit (DG RTD), especially Iphigenia Pottaki, James Gavigan, Frédéric Bastide, Stuart Kirk, Laura Contor and Jennifer Martins Branco Correia Lopes.

EXECUTIVE SUMMARY

Cybersecurity is – and has been for some time – a priority matter for business and political leaders around the world. As cyber threats also impact on individuals' many everyday digital transactions and interactions, cybersecurity is a prime concern for citizens too.

Discussions are beginning this year to revise the EU's 2013 cybersecurity strategy. This Scientific Opinion of the SAM HLG on cybersecurity, responding to a January 2016 request from the European Commission's Vice President for the Digital Single Market Andrus Ansip, is particularly timely to inform this process.

The amount of academic, expert practitioner and stakeholder literature on cybersecurity as well as in specialised and general published media is vast, revealing the intricate and multidisciplinary nature of the field. It is also clear from the literature that for scientific advice on cybersecurity policy to take account of the field's inherent complexities and fast-evolving challenges, it requires scientific expert views, analysis and evidence beyond that delivered by empirical work to date.

The specificity of this SAM HLG Scientific Opinion on cybersecurity compared to other reputable independent reports in the field, is that it presents a European view on cybersecurity in the Digital Single Market directed towards EU-level policy makers. Its ten recommendations aim to inform a revised cybersecurity policy which enables a strong and growing Digital Single Market where security, innovation, citizen participation and informed choice go hand in hand with protecting fundamental rights and European values.

The recommendations are:

CRYPTOGRAPHIC STANDARDS

Ensure that cryptographic standards in the EU reach and remain at state-of-the-art levels.

To maintain the trust of users/citizens as well as protecting their privacy and providing security, neither back doors nor other ways of weakening encryption should be introduced.

SYSTEMS APPROACH

Encourage the adoption of a systems engineering approach to the totality of on-line relevant Information and Communication Technologies (ICT) developments - starting from the design stage, and throughout connected systems, including the EU's Internet and Cloud infrastructure.

Pursue and enforce security and privacy by design and by default, covering both software and hardware, as recognised in the General Data Protection Regulation (GDPR).

TECHNICAL VULNERABILITIES

Europe should focus its efforts on reducing software vulnerabilities over the product life cycle, requiring "duty of care" from design to testing and verification, including formal verification where applicable, long term maintenance and fast repair. In parallel, emphasis should be placed on the timely fixing of hardware vulnerabilities, especially through supporting testing and verification of hardware.

Provide at EU level appropriate incentives (including economic and legal) to encourage responsible disclosure and repair of vulnerabilities.

CONTEXTUAL IDENTITY

To respect privacy, promote the development and context-tailored use of attribute-based digital identity management.

ENGAGING CITIZENS

Promote data-literacy education and build European citizens' awareness on cybersecurity. Promote citizens' engagement in shaping the future of the digital world, respecting fundamental values.

USER CHOICE

Support the deployment of the means - including technologies and processes - for user choice and control over their digital identities, footprints and personal data.

Support individual autonomy and privacy by giving users well informed options, including the opt-out right not to be profiled and the right to be forgotten.

CYBERSECURITY INDUSTRY

Support the development of an EU cybersecurity industry ("made in Europe"), including data transfer and network technologies, protection of meta data, and "cloud"-based data storage and processing, to enhance the security of digital systems and guarantee the fundamental rights of EU citizens, while also increasing job creation and European competitiveness in the global market.

TRAINING PROFESSIONALS

Promote cybersecurity education curricula and lifelong cybersecurity training to build talent and sustain the skills of professionals. Make cybersecurity education more attractive to students.

Educate system engineers to further develop a "security" skills base in Europe and to shift to a systems design model which incorporates security principles from the very beginning.

EVIDENCE COLLECTION AND SHARING

Support the development of evidence collection methods, including sharing of evidence and best practices, between EU member states of cybersecurity-related information.

Improve the mutual trust between national entities (e.g. Computer Emergency Response Teams - CERTs) such that intelligence information can be more freely disseminated between stakeholders.

Develop and monitor cybersecurity standards and practices, and provide sufficient authority and resources to do so, including adequate technical expertise in European bodies.

EU AND THE WORLD

Given the global and rapidly-evolving nature of cybersecurity challenges, Europe should be at the forefront of establishing worldwide and coherent cybersecurity governance for the digital economy. This should be consistent with and build upon a strong European cybersecurity governance framework, fully aligned with European values and the fundamental rights of EU citizens.

INTRODUCTION

1. INTRODUCTION

The internet revolution is giving rise to a digitally-connected world full of opportunities for innovation, creativity and new forms of social endeavour. Indeed, the ubiquity of digital technologies in economic and social life has the potential for huge progress in the form of increases in service and amenity value to citizens as well as economic efficiency gains. But this world is also characterised by growing clandestine intrusion into digital systems. This includes cybercrime and inappropriate or unsanctioned use of digital information which defy geographical and jurisdictional boundaries. The perpetrators seem undeterred by the cybersecurity counter measures and policies of businesses and public authorities.

The result is growing economic losses, many of which go unreported[1]. In addition, there are intangible costs to society – e.g. reputational damage to businesses and individuals, psychological trauma, general feelings of frustration and insecurity, etc. Beyond these costs, there are risks to national security, which is increasingly dependent on a safe and resilient cyberspace. The magnitude this state of affairs has reached is becoming a threat to safety and fundamental rights such as privacy. If the clandestine intrusion continues unabated, the costs to society will be substantial. It is therefore not surprising that cybersecurity is – and has been for some time – a priority matter for business and political leaders around the world.

Within the context of the European Single Market, the Digital Single Market (DSM) strategy includes regulatory and other measures addressing different aspects of digital transactions[2]. The strategy should enable citizens, businesses and governments to benefit from the digitalisation of markets

[1] Cyberattacks for data fraud or theft are 8th in the list of the 10 most likely global risks according to the World Economic Forum (The Global Risks Report, 2016)

[2] The Digital Single Market aims to address existing barriers online, which limit opportunities for growth and create costs because citizens miss out on goods and services, internet companies and start-ups have their horizons limited, and businesses and governments cannot fully benefit from digital tools. It is expected to contribute €415 billion per year to the Union's economy and create hundreds of thousands of new jobs. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A Digital Single Market Strategy for Europe (2015)

for goods and services, and thus foster growth and job creation. The DSM supports infrastructure development and aims to provide a seamless and level playing field for businesses. Within the DSM, the rights and responsibilities of stakeholders should be protected and enforced.

Secure network and information systems are essential to keep the online economy running and to promote prosperity. The EU adopted a cybersecurity strategy in 2013[3]. This strategy defines cybersecurity as "the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein". The cybersecurity strategy, together with the European Agenda on Security[4], describe the EU policies and initiatives on cybersecurity and cybercrime – from legislation and investment to raising Member State capabilities, promoting intra EU coordination and international cooperation. However, the cyber-world is fast evolving and so there is a persistent need to revisit measures and policies and take timely action in response to new threats and opportunities.

Scientific advice based on existing knowledge and evidence can provide valuable information and insights to EU policies on cybersecurity. However, providing science-to-policy advice is made difficult as cybersecurity is not a clearly demarcated field of academic study that lends itself readily to scientific investigation. Rather, cybersecurity combines a multiplicity of disciplines from the technical to behavioural and cultural. Scientific study is further complicated by the rapidly evolving nature of threats, the difficulty to undertake controlled experiments and the pace of technical change and innovation. In short, cybersecurity is much more than a science.

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOINT (2013)

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions The European Agenda on Security (2015)

Despite these difficulties, cybersecurity has been the subject of authoritative scientific reports, including *At the Nexus of Cybersecurity and Public Policy - Some Basic Concepts and Issues* (U.S. National Academy of Sciences, 2014), *Internet Privacy - Options for adequate realisation* (ACATECH, 2013) and *Progress and research in cybersecurity* (UK Royal Society, 2016).

The Scientific Opinion by the European Commission's Scientific Advice Mechanism's High Level Group (hereafter referred to simply as "the Opinion") is in keeping with the scientific and independent basis that academic bodies uphold. The Opinion presents a European view on cybersecurity in the DSM to inform policy development in the coming years.

AIM, SCOPE AND METHODOLOGICAL APPROACH

2. AIM, SCOPE AND METHODOLOGICAL APPROACH

The SAM High Level Group of Scientific Advisors (SAM HLG) began its work following a request from the Vice President of the European Commission, Andrus Ansip, in January 2016. The aim was to provide scientific advice that would inform the revision of the EU's cybersecurity strategy, as well as the further development of the Digital Single Market strategy. This was described in the cybersecurity scoping paper[5], which listed a number of questions falling in two broad categories:

1. Trust in transactions intermediated by ICT (e.g. backdoors, encryption, digital identities)

2. Cross cutting questions (e.g. evidence collection, risk management, science of cybersecurity)

Cybersecurity relies on a triad of people, processes and technology (hardware and software). This brings to cybersecurity a combination of technical, socio-economic, ethical and jurisdictional challenges. Furthermore, different broad cybersecurity discourses can be identified within academic and stakeholder communities depending on the primary preoccupation – e.g. privacy and the protection of fundamental rights; criminality and law enforcement; or defence, and national security – though with no clear-cut boundary between them. The Opinion had to draw on these different domains and could not address science and technology separately from the rest. The scope of the Opinion was thus refined in consultation with experts.

The first exploratory step in the development of the Opinion was a wide sampling of evidence and expert knowledge. This involved literature searches (scientific publications and grey literature), participation in

[5] See https://ec.europa.eu/research/sam/index.cfm?pg=cybersecurity

conferences and workshops, and discussions with experts selected primarily in consultation with the European Academies[6].

Throughout the development of the Opinion the SAM HLG sought to identify consensus views in the scientific communities. A key activity for this purpose was a large expert workshop entitled "Secure Digital Identities for the Digital Single Market in Europe" which took place on 25-26 October 2016 in Vilnius, Lithuania, that brought together around 50 experts from different disciplines[7]. Subsequently, additional information was collated and expert consultations held, on selected cybersecurity issues which emerged as critical to the formation of the emerging recommendations.

On 31st January 2017 the SAM HLG presented its preliminary findings to Vice President Ansip and representatives of European Commission services involved in the cybersecurity field. The meeting confirmed the relevance of the SAM HLG draft Opinion for EU policy, in particular in relation to the forthcoming review of the DSM and the cybersecurity strategy.

Towards the end of the process, on 13 February 2017, a stakeholder workshop was held in Brussels to collect feedback from representatives of the business community and citizen groups in response to the draft findings. The reactions and comments received were positive and constructive[8].

[6] See annex 1.
[7] See annex 3.
[8] See annex 4

PRINCIPLES

3. PRINCIPLES

A first set of principles which inspired the Opinion is taken directly from the Charter of Fundamental Rights of the European Union. The rights and principles expressed in this Charter entail responsibilities and duties with regard to individuals, communities and future generations, and, according to the SAM HLG, must be upheld in the digital world as they are in the physical world. These principles should lend a distinctly "European" flavour to EU cybersecurity policy. Therefore, at the core of the Opinion is the view that EU cybersecurity policy (in its legislative and other parts) should involve a citizen-centred approach upholding, *inter alia* the rights to: liberty and security of person; respect of private and family life, home and communications; protection of personal data; freedom of expression and information; access to one's personal data held by public administration; and so on.

Taking into account cross-cutting cybersecurity themes, the SAM HLG also adopted for the development of the Opinion the following second set of principles:

- Transparency – public authorities, service providers and system developers must handle data in a transparent manner.
- Duty of care towards customers - software and hardware producers must follow due diligence with respect to cybersecurity for the whole product lifecycle, starting from the design phase.
- Shared responsibility for cybersecurity - between public and private sectors, users and service providers, EU Members states, EU and globally.

Such are the principles which underlie this Opinion.

ANALYSIS

4. ANALYSIS

4.1. Privacy, digital identity and control of data

Social and human sciences are starting to provide insights into human behaviour in cyberspace, revealing much complexity and several "paradoxes". One area of empirical research is on passwords which play a key role in regulating access to sensitive information and online services (e.g. email systems, online repositories, social networks). Evidence suggests that very simple passwords (e.g., 0000, admin, 1234) are commonly used. Weak passwords are one of the ways through which humans expose themselves to cybersecurity risks. Password policies aiming to make users more secure (such as policies requiring rotation or applying restrictions) often make them less secure, because, for example, people note down their passwords in unsafe places[9]. Better understanding of human behaviour is needed to inform security policies, and to reduce the risk that policies will not achieve their aims.

Another account drawing much on sociology and psychology starts with the human experience of the self in the digital world. This theoretical approach argues that better understanding human behaviour can help reduce cybersecurity risks caused by human "sloppiness" by serving as the basis for education and awareness programmes. It investigates apparent paradoxes in human behaviour e.g. the "privacy paradox", whereby individuals care a lot about their privacy, and yet freely give private data on line via their social accounts. At the core of this approach is a theory of digital identity as being about *what we do* in the digital world rather than *who we are*[10]. Moreover, users have multiple identities, as they can create accounts for various services and social networks. Evidence shows that many users have a number of accounts i.e. they create on-line a number of

[9] Passwords and the evolution of imperfect authentication. Bonneau (2015)
[10] In order to better understand identity, one needs to examine how it is experienced and how this is being radically transformed in the digital world. This transformation, in the experience of identity of an individual as a disembodied identity, is according to some academics at the source of paradoxical behaviour of individuals or "sloppiness" on the internet (see annex 3, and L. Van Zoonen presentation at Vilnius workshop, see SAM Website https://ec.europa.eu/research/sam/index.cfm?pg=cybersecurity)

digital identities (not all of them active)[11]. Users can create different profiles to interact with different groups (e.g. teenagers having one profile for their friends, one for their parents and one for their grandparents)[12]. Some academics view multiple identities as a way to resist pressure for unique single identifiers, which they claim is linked to a hegemonic system[13].

4.1.1. Contextual identity

Notions of privacy are highly context-dependent and differ between cultures and communities (e.g. the approach to privacy in the EU is different from the US)[14]. Acatech's (2013) paper on internet privacy suggested that the definition of privacy depends on our culture – in Europe, privacy is closely connected to the right to "informational self-determination"[15]. Furthermore, some experts argue that privacy has evolved in the modern world, to the extent that personal data which are now the most sensitive, such as religion, health and sexual orientation can be better described in terms of "intimacy" rather than privacy[16]. Nissenbaum (2009) claims that citizens have a right to privacy, but this right is neither a right to control personal information, nor a right to have access to this information restricted. Instead it is a right to live in a world where people's expectations about the flow of information are mostly met. She calls this right "contextual integrity", which depends on a balance of social rules, norms, values, ends and purposes.

A key concern with digital identities and their use is the question of what elements of one's identity should be revealed for a transaction. A set of elements may be used, depending upon what the person is doing (wants to

[11] See annex 3
[12] For example, establishment of identity is being advanced in both the United Kingdom, with the Identity Assurance Programme, and the United States, with the National Strategy for Trusted Identities in Cyberspace program. These programs allow private sector companies providing authentication services to federate identity and use the right identity for the right purpose. Currently, many people use authentication services from large companies rather than government-issued IDs when accessing private-sector services. Other examples come from the research communities, such as computing grids.
[13] Lyon (2007), van Zoonen (2013)
[14] See annex 3
[15] Acatech Position Paper (2013)
[16] N. Arpagian (presentation at Vilnius workshop, see SAM Website https://ec.europa.eu/research/sam/index.cfm?pg=cybersecurity)

do), rather than who the person is. Data minimisation, one of the principles driving the European General Data Protection Regulation (GDPR)[17], is consistent with identity management models where only those elements (attributes) of the user's identity that are necessary for the specific transaction are revealed (the IRMA model *I Reveal My Attributes* – e.g. to buy alcohol I reveal my age[18]). Different levels of security are required for different transactions and different sets of attributes can be used to help establish the level of trust required in a specific context – i.e. a contextual approach. A number of technologies can be used to apply this approach[19].

4.1.2. User control, user choice

Using data to create value opens up opportunities for innovation, better services and new businesses. But data processing can also challenge individual rights and societal values, and the power relations in a society. As some scholars put it, the notion that "power follows the money" is giving way to "power follows the control of the data".

The lack of transparency about what happens to personal data provided by users on-line either knowingly or unwittingly, is a key concern. Service providers allow different identities to be created, but they can link all these data to build highly sophisticated behavioural and psychological profiles of the person, as well as of one's friends and connections. Technically, this intimate knowledge of a person can be used by different actors in different

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[18] D. Broeders presentation at Vinius workshop, see SAM Website https://ec.europa.eu/research/sam/index.cfm?pg=cybersecurity)

[19] Under the approach of "attribute-based digital identity", identities are collections of attributes (of a person of object), which are "assembled" together to respond to a specific set of requirements for a specific online service. See Koning (2014). In most computer-related scientific work a digital identity is considered to be a set of characteristics describing certain properties about an individual. This set is dynamic, and depends on the context in which the individual is known. The attribute-based credential technology (Camenisch 2015, Sabouri, 2012, Alpár & Jacobs, 2013) implements this model. See EU FP7 ABC4TRUST project, and for an overview of technologies: Danezis and Gürses, (2010). The idea of shaping technology according to privacy principles has been discussed since long, addressing among else the principles of data minimization, anonymisation and pseudonymisation – or Privacy Enhancing Technologies (PETs), covering the broader range of technologies that are designed for supporting privacy and data protection.

ways – for example to commercially target the person, monitor behaviour, influence political choices including voting, or cyberattack through spear phishing[20].

The voluntary giving of data to social accounts is one of the ways that big players (states or companies) in the digital world collect and connect data that are used to profile human users (the "data subjects"). Even those who are not active in social media or who do not provide much personal data online, leave a digital footprint when they visit sites. In the case where data are given directly by individuals on-line or provided through their digital footprint, "consent" to collect data is given by "ticking a box". However, by giving information about oneself on social networks, one also gives information about one's social circle of "friends", often without their prior knowledge or consent. Furthermore users may not be aware that they reveal information about themselves when the data take the form of metadata related to their communication devices.

There is no doubt in the scientific community that this "tick-box"-type consent is insufficient and incommensurate with subsequent data collection and usage. Freely given, specific, informed and unambiguous consent as foreseen by the General Data Protection Regulation can be realised in a number of ways. An important condition for this to happen, is that there be acceptable alternatives available to the user for services of the same level of quality. If the information for users is too much/too legalistic, or if they do not trust it, and if users do not have good alternatives to turn to, the enabling conditions for real consent are not fully in place.

Enabling citizens to make informed choices between alternative products or services is not only consistent with principles of self-determination and democratic governance but is also a key component of security and trustworthiness in the digital market. In its White Paper on cybersecurity and privacy research, the European research consortium for Informatics

[20] email or chats are sent that appear to come from someone in the social circle of the person but contain links to malware

and Mathematics concludes that technological solutions should be developed to empower users with full control over their own data as well as to provide technological support to legislations for the protection of data[21].

The GDPR is a step forward in this direction. It needs to be fully implemented, technically enabled, enforced and monitored. For example, to satisfy requirements derived from GDPR, system designers need to be provided with practical tools and guidelines[22].

4.1.3. Engaging Citizens

The human actor is commonly portrayed as a risk to cybersecurity or as "the weakest link". There is little doubt that appropriate human behaviour can limit cyberattacks and their impact, in a similar way that washing one's hands frequently can reduce the risks of catching influenza. But calling for knowledgeable and responsible users should not be used as a step towards imparting blame to users for issues beyond their awareness, control or power.

Citizens' awareness and engagement in cybersecurity may seem an easy prescription for policy making, yet it is one of the most challenging. One reason is the difficulty for non-expert citizens to understand the complexity of cybersecurity, how the system works and what the security risks are. A second reason is the lack of scientific evidence on how cybersecurity awareness can be raised. Therefore, while there is broad consensus on the necessity to increase citizen awareness there is little empirical knowledge about how to design and implement effective policies to do so. Research experiments in cities and hubs show interesting results which could, through further research and scientific analysis, help to elucidate issues of human behaviour in cyber space. For example, research at the Bold Cities Centre in the Netherlands showed inter alia that citizen engagement

[21] ERCIM (2014)
[22] Hoepman (2014)

initiatives may attract only some groups of people (often the ones that are anyway more engaged; for example young digitally active men)[23].

4.2. Economics, industry and skills base

Economic value in the digital world is derived from data ("data is the new oil"). Service providers have a business interest to collect large amounts of data, whilst governments claim a national security or criminal investigation interest to access data. The interest or return to the citizen who provides the data in the first place, is less clear. However, there are situations where sharing data clearly confers benefits to societies (e.g. sharing medical data for disease detection, or sharing preferences to improving public services, for example in transport).

Accordingly, the question of data security in the digital world is not only technical but also, to a large extent, socioeconomic and political. The classic problem of collective action in public choice theory and game theory is relevant here: all benefit from security but no one provides it for all and the parties do not "cooperate" to provide the solution for all (due to lack of trust). Economic incentives play a critical part in cybersecurity, together with the technical design of systems[24].

The growth of the credit card market is an example that shows that even with insecure systems there is widespread use when customers have safeguards which protect them from financial loss in case of fraud. In the case of credit cards continued use works by sharing the cost across customers (in the form of a hidden charge). Similar safeguards or insurance mechanisms can be envisaged for other transactions in the digital market, even though some of the consequences of cybersecurity incidents may be nontangible (for example reputation loss). From an economic perspective, proving safeguards to users may encourage continued use of digital transactions.

[23] http://www.centre-for-bold-cities.nl/
[24] Anderson and Moore (2006)

The consultation with experts at the Vilnius workshop and later stages suggested that the market is developing solutions in the field of insurance against cybercrime. It also revealed a wide range of opinions about the merits and drawbacks of insurance[25] [26].

4.2.1. Cybersecurity industry

In a number of cases, government action can enable market solutions for cybersecurity. Incentives often work faster than legal obligations and can be advantageous, especially when rapidly evolving digital technologies are involved. Incentives can take the form of rules – for example a financial/business regulatory authority may adopt rules that require data breaches to be reported regularly to investors, thereby creating an incentive for companies to pursue transparency as a competitive advantage.

The state of the cybersecurity industry in Europe has been addressed by the EU Cybersecurity Strategy (see annex 2), which highlighted that *"Europe has excellent research and development capacities, but many of the global leaders providing innovative ICT products and services are located outside the EU. It is key to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data."*

Europe should be able to verify that appropriate standards apply to products intended for the European market, whether home-made or imported. At the same, developing and applying appropriate standards is an opportunity for EU companies to attain competitive advantage in the global markets, promoting privacy-friendly products for example. Certification and

[25] Ernst and Young (2014)
[26] Under the EU Cybersecurity Strategy (2013), the Commission invites public and private stakeholders to develop, in cooperation with the insurance sector, harmonised metrics for calculating risk premiums that would enable companies that have made investments in security to benefit from lower risk premiums. In addition, in the Report of the European Cybersecurity Industrial Leaders (2016), the group of European Cybersecurity Industrial Leaders also emphasized the role of insurance in providing insurance and risk management solutions to cyber risks.

labelling are important to guide consumers, and the EU should play a key role in this domain[27].

However, the majority of leading businesses are from America or Asia, and so growing of the European cybersecurity sector is crucial. The Cybersecurity Public Private partnership launched in 2016 is a step in this direction[28]. The consultation with the scientific community reveals broad support for this approach.

The production of key components and the development of key technologies in Europe is a matter of strategic importance. Investing in core competences in cybersecurity will strengthen Europe's cyber capability and its role as a trading partner. Research, technological development and innovation are an essential part of this. Specific industrial sectors and applications are beyond the scope of the Opinion.

4.2.2. Training professionals

The issue of skills for cybersecurity in Europe has been recognized as requiring policy action[29]. The aim would be to increase the numbers of trained experts as well as match their qualifications and skills to the evolving needs of cybersecurity. Europe does not have and does not currently educate as many cybersecurity professionals as are needed.[30]

Software developers should be trained in systems engineering approach, and program software following well established secure-code development practices. Numerous software applications today are written and brought to the market by startups and freelance developers without adequate security controls, adding serious vulnerabilities. Education and building a culture among professionals that focuses on resilience of systems is the essential

[27] Report of the European Cybersecurity Industrial Leaders (2016)
[28] See annex 2.
[29] For example, under the EU Cybersecurity Strategy (2013)
[30] The discussions in Vilnius highlighted as example (that there are) ten times more cybersecurity university students in Israel than in France, where only about 25% of the needs for cybersecurity professionals (public and private) are covered. La cybersécurité, le « bon choix » Picut (2016)

approach to increase cybersecurity, while regulation that may be required, should not stifle innovation or create barriers to new entrants.

Fit-for-purpose curricula should take into account the multidisciplinary nature of cybersecurity challenges and involve a balance between technical aspects (IT, risk assessment, etc.), competences from social sciences (behavioural, psychological, situational analysis, etc.) and legal matters[31].

4.3. Trust and security

EU policies and research communities emphasise the importance of creating trustworthy systems and avoiding the loss of citizen trust in the digital world. There is a need to maintain and increase participation in the digital market, so that people do not limit or reduce their digital transactions because of a lack of trust and, in the process, deprive current and future generations of innovative economic and social opportunities. The distrust may be caused by fear of cybercrime, of identity theft or profiling, and lack of transparency regarding what happens to data. The EU can play a role in enabling citizens' trust in the digital ecosystem. When people trust that a system will protect their personal data, they may be more willing for example to share their medical records in order to promote innovations in health, rather than when they suspect strongly that their openness will be used against them.

Therefore, understanding the relation between trust and security is important for cybersecurity and the Digital Single Market. Trust involves accepting some vulnerability. This becomes evident when we define trust, following Mayer *et al* (1995)[32] as *the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.* Accepting vulnerability is common in the real world, and should not appear out of place in the digital

[31] See also ACM (2016) recommendations on cybersecurity education and workforce development; For an example see https://www.csacademy.nl/en/
[32] Mayer (1995)

one. However, there are crucial differences between trust in a social context in the real world (built over time, affected by culture and history) and trust in the digital world. Although the latter may be linked to technology and ICT infrastructure, it is also a social concept. For example, the question of centralised versus decentralised management, has much to do with trust and whether it should be completely distributed without central nodes, or distributed to a quorum (federated), or accorded to one (centralized) entity.

More trust does not necessarily mean more cybersecurity. The real issue is that too much trust exacerbates vulnerabilities. Some academics have put it in striking terms, such as "trust is bad for security"[33]. Placing more trust in the system does not necessarily make it more secure.

Blockchain (originally the backbone of cryptocurrencies, and today used for many other distributed online services) can be taken as an example of trust-enabling technology, under some conditions[34]. Blockchain appears to be a rising star of the online services domain. However, it cannot be considered a panacea, but only appropriate for some, well-defined use-cases[35].

4.3.1. Cryptographic standards and backdoors

Cryptography is widely used to build trust. Backdoors in applications and/or devices have negative effects on trust. People trust less the service providers that declares "*we do not read your messages*" than those that

[33] Gollmann (2006)
[34] A blockchain is a tamper-proof and shared data structure composed of a list of blocks of transactions and based on a trustless model (and for that reason as a paradox, are trusted as not based on the need for establishing a trust relationship). The blocks are built, validated and linked together in a way that guarantees some relevant properties under a trust perspective as: *disintermediation* (no need of trusted third parties), *user empowerment* (transactions and data are in control by the users community), *resilience* (blockchains do not have a central point of failure), *transparency and immutability* (every modification inpublic blockchains is visible to everybody and the transactions stored in a blockchain cannot be altered)
[35] For example, when to keep track of transactions (money transactions or data exchanges), keep track of chain of interactions in a secure and immutable way, execute in a reliable way Smart-Contracts, blockchain technologies are ahead, but for all those applications where data need to be stored in huge quantities, modified and searched quickly, or where events should be triggered in real-time blockchain could be used to support some functionalities, but not as the core system. See UK Government Office for Science (2016)

declare (truthfully) "*we cannot read your messages*"[36]. If strong encryption is properly implemented, deciphering an encrypted message without the key is extremely difficult, if not impossible. Encryption serves security and privacy at the same time, because it makes it harder for cyber attacks to succeed and also helps protect citizen privacy.

Cryptography backdoors can be introduced either at algorithmic level or at implementation level. Sometimes backdoors are introduced intentionally (i.e. not due to accidental human errors) by law enforcers or governments to facilitate criminal investigations. However, there is a general consensus among the scientific community that this practice should be avoided.

The expert workshop in Vilnius as well as further consultations in the later phases in the development of the Opinion confirmed the consensus of the scientists against back doors. In this field, privacy should not be sacrificed for security.

The opposition to backdoors also emerged in the literature review. For example, the Royal Society report on cybersecurity stated that "*There is a clear consensus among security researchers that introducing "backdoors" or extraordinary access measures would also open doors through which malicious intruders could attack"*[37]. ENISA, the European Agency for network and information security concluded that *"the very existence of backdoors provides an opportunity for criminals or state actors to undermine the privacy of communications and for users to believe that their communications are not secure*[38]*."* An MIT paper concluded that *"[T]his report's analysis of law enforcement demands for exceptional access to private communications and data shows that such access will open doors*

[36] Encryption allows information to be securely transmitted and stored. Encryption is used to convert 'plaintext' information into 'ciphertext', which contains all the information of the plaintext message, but cannot be read without the proper key and mechanism to decrypt it (see UK Royal Society 2016).
[37] UK Royal Society (2016)
[38] ENISA (2016) Opinion paper on Encryption

through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend[39]*."*

For small businesses, which would find it harder to resist government-mandated backdoors, a general no-back door policy may be crucial to their survival in a market where customers trust is decisive. Backdoors can harm small business and producers, who may suffer more from a loss of consumers trust, because consumers can more easily turn away to other competitors than in cases of big companies that cannot be so easily replaced or where there are no real alternative solutions/providers. Schneier *et al* (2016) in *A Worldwide Survey of Encryption Products* also stated that *national law mandating encryption backdoors will affect innocent users of products and smart criminals will easily be able to switch to more secure alternatives*.

There is scientific excellence in the field of cryptography in Europe. With new opportunities and threats in the future, from the Internet of Things (IoT) to connected or autonomous vehicles, Europe needs to continue developing and maintain its expertise.

4.3.2. Vulnerabilities

One of the big problems with cyber incidents is that they are often not detected until after a significant time lapse. It is often months between a malware infection and its discovery. Therefore if attacks cannot be avoided totally, it is important to focus on how the systems are built so as to limit the damage when hackers get in, to improve detection of attacks when they happen, as well as repair as fast as possible.

Vulnerabilities always exist in systems. Technically, more vulnerabilities could be avoided from the start and more secure systems could be brought to the market. However, the costs are generally perceived as prohibitive and the economic incentives to create more secure systems are generally

[39] *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications* Massachusetts Institute of Technology (2015).

lacking. The consultation with experts in Vilnius and further literature review revealed that vulnerabilities are both a technical issue and a question of economic cost. The result is that a perfect system does not exist and "data are never secure".

Testing and verification play a big role in addressing vulnerabilities, but not fully. For example, hardware vulnerabilities may be hidden in devices that pass testing and certification processes, and only start misbehaving after some time. For software, advances in formal verification methods can help to build safer software that operates by matching a given formal specification.

However, formal verification on a large scale is still out of reach. There was consensus in Vilnius that, in the foreseeable future, the formal verification methods could not be used to check complete software programs, because these are too long and regularly changed; instead, it will be used only on critical parts.

4.3.3. Systems approach

In a fully interconnected world where individual online services and applications are composed of literally hundreds of third-party libraries and applications, security must be achieved in a coherent and coordinated way. Adding one application to another makes fast repair increasingly difficult. The typical response is patching, and then another patching for another problem, and so on and so forth.

A more efficient way is to take into account the security considerations and the actual threat landscape from the design phase, using a robust systems-engineering approach. From the conception of the application, such an approach defines security measures and clear and secure interfaces, facilitates integration with other applications, and facilitates the fast fixing of problems as they arise. Ideally, robust systems engineering takes into account the whole ecosystem, including the students and business start–

ups engaged in writing application code. Clearly the adoption of a systems approach requires a substantial transition or paradigm shift.

4.4. Governance

There is a clear mismatch between the ease and impunity with which cybersecurity breaches occur and the means (legal, technical) deployed by public authorities and businesses to counter them. One reason is the fast evolution of ICT which can result in defensive measures becoming outdated before they are applied. Another is the unique combination of physical and virtual properties of cyberspace which makes government jurisdictional control difficult (Nye, 2014). Yet another is the failure of governments and non-state actors, including businesses, to commit to and act upon shared responsibility for cybersecurity, where both public and private actors partially cede or compromise their habitual spheres of autonomy and control in the interests of long-term benefits for all.

4.4.1. Evidence collection and sharing

Governments and public authorities are reluctant to share cybersecurity-relevant information for fear of compromising territorial security and competiveness[40]. Companies are reluctant to divulge information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive or proprietary business information including intangible assets such as reputation – to cite Carr (2016) *"The reluctance of politicians to claim authority for the state to introduce tougher cyber-security measures by law, coupled with the private sector's aversion to accepting responsibility or liability for national security, leaves the 'partnership' without clear lines of responsibility or accountability"*. For many scholars, to ensure effective public-private partnership, the tensions, competing agendas, and disjunctions in responsibilities and rights of governments and the private sector must be spoken about with clarity. Continued fragmentation and lack

[40] "we are in the midst of an intense competition for money, power and control over all aspects of the Internet and the Internet economy ... //… waged across technical, regulatory, political and social battlefields" (Hathaway, 2014).

of coordination plus emerging potential game-changers[41] will only exacerbate the situation in the future, if business-as-usual prevails.

The way out of this impasse requires more cooperation, compromise, sharing of information and effective collective action – and the more this takes place at transnational level rather than within individual countries the better, given the intrinsically global nature of the cyber world[42]. A futures study by UC Berkeley's Center for Long-Term Cybersecurity foresees public-private partnerships to be the norm by 2020 - *"Successfully forging public-private relationships will be a source of significant security advantages for cities, regions, countries, and beyond. And as these partnerships multiply and morph, it will become harder to distinguish between what a private actor is doing and what a government is doing to threaten or defend networks and data assets"* (CLTC, 2016)[43]. Elsewhere, Choucri *et al* (2013) anticipate that in time, checking the global spread of global vulnerabilities will give rise to the joining up and analysis of data sets from international and national statistics and private companies[44].

The situation in Europe is, in a sense, a microcosm of the globe. The level of capability to deal with cybersecurity issues varies widely between EU Member States. Some already have developed national cybersecurity strategies and so are somewhat locked-in to specific choices such as those regarding the division of responsibility between public and private sectors, the types of instruments and incentives to use, etc. Member State strategies are also marked by cultural and political preferences.

---

[41] E.g. new computing paradigms - quantum or DNA-based); discontinuous jumps in system complexity - the Internet of Things/ cyber-physical systems or the huge growth in social networking etc.
[42] See Eeten & Mueller (2012); Pawlak & Wendling (2013); Hathaway (2014); Tziarras (2014); Carr (2016); Netherlands Presidency (2016); Shackelford *et al* (2016); Pawlak (2016).
[43] Center for Long Term Cybersecurity (CLTC) (2016)
[44] "Over time, we anticipate the possibility of pairing international and national statistics with information from the private sector. Security and monitoring companies such as Symantec, Arbor Networks, Microsoft, and McAfee provide quantitative data that address the global spread of Internet vulnerabilities. In many cases, the volume and quality of data released by these organizations far outpaces the information released by international and national organizations; however, the true value of this information lies not in an isolated analysis, but in the intersection of private data with the national and international sphere." (Choucri *et al*, 2013)

One of the differences in Europe compared to the global situation, is that EU institutions provide a vehicle for concerted effort to overcome the afore-mentioned cybersecurity governance challenges at least at a macro-regional level. Furthermore, in spite of the intra-European differences, there is a substantial and unique level of agreement on fundamental principles and values, as well as a shared strategic interest which can be at the heart of effective EU cybersecurity governance. Existing EU legislation and coordination mechanisms (such as the NIS Directive, the European Union Agency for Network and Information Security ENISA, Europol and EC3, CERTS, and various European Commission services - see annex 2) promote evidence sharing on cybersecurity across the EU. An evolving policy agenda can take on new and reinforced measures to address emerging priorities – e.g. the development of standards, the reinforcement of information sharing and monitoring, etc.

Speed is of the essence if EU-level legislative and other measures are to be truly effective. In matters of cybersecurity, the usual time frame from conception to implementation and enforcement of EU legislation is too slow. Take for example the four-year gestation period for the NIS Directive from 2013 to its 2017 date of applicability, or the lead-time from the initial tabling of the GDPR in 2012 to its adoption in April 2016 but only applicable from 25 May 2018. To reduce the lead time from proposal to implementation, institutional and/or procedural innovations coupled with enforcement measures which stay abreast of technical evolutions – e.g. relating to standards, best available technologies, etc. - are needed.

4.4.2. EU in the World

How to develop and implement an adequate and effective system of global cybersecurity governance based on shared responsibility is not obvious. While there are a number of relevant international fora[45], no adequate global cybersecurity governance framework is emerging to fill the gap. Indeed, as Nye (2014) suggested, a single overarching regime for cyberspace is still some time off. EU involvement in global cybersecurity governance is already part of the EU's 2013 cybersecurity strategy, and was reiterated in the EU External Action Service's 2016 Global Strategy for the European Union's Foreign and Security Policy[46].

However, given the strategic importance of cybersecurity to ensure European sovereignty, to protect European values and promote them worldwide, SAM HLG strongly recommends that the EU play a more prominent leading role in establishing effective cybersecurity governance globally.

[45] E.g. non-governmental ones such as the Internet Engineering Task Force (ITEF) or the World Wide Web Consortium (W3C) which set consensus-based standards and protocols; the Working Group on Internet Governance (WGIG) with the US-based ICANN which covers only a small subset (naming and numbering) of cyber governance; or the UN agency, the International Telecommunications Union (ITU)

[46] The EU Global Strategy states *inter alia* that the *format to deliver effective global governance may vary from case to case. On cyber, global governance hinges on a progressive alliance between states, international organisations, industry, civil society and technical experts.*

CONCLUSIONS

5. CONCLUSIONS

Building on the preceding analysis, this chapter sets out the conclusions of the SAM HLG in the form of a number of Observations and Recommendations.

The Observations relate to issues which came to light in the analysis process, and are considered by the SAM HLG to be of sufficient importance and relevance for policy makers to merit specific mention. They are, however, not the object of concrete recommendations – either because there was not sufficient consensus among experts or because they affect many areas but do not directly *per se* call for policy action.

5.1. Observations

The first observation is an acknowledgement of the nature of cybersecurity as an activity and object of scientific evidence review and analysis. The complex, multidisciplinary and fast-moving nature of cyber threats, cybersecurity breaches and responses to these is not accompanied by a corpus of robust empirical studies. In other words, cybersecurity is not a well-defined and standardized scientific discipline.

The second observation is the mismatch between the lead-time for EU legislation in this area and the fast turn-over and obsolescence rates of digital technologies and cyberspace services and applications. Many cybersecurity stakeholders consider that while the NIS Directive is welcome, much of its content will be out-of-date by the time it is applicable or shortly afterwards. This Opinion does not contain any specific recommendation on how to rectify this situation. However, it offers the view that those shaping EU policy could consider innovative processes to address this mismatch.

The third observation is to acknowledge a number of tensions or dichotomies in the cybersecurity debate where there is neither evidence nor clear expert consensus to come down in favour of one or other of the opposing options:

a) One of these is the tension between centralised and decentralised IT governance for on-line transactions. There are technical arguments in favour of either one; yet ultimately the choice between the two is a question that is deeply political and has repercussions at many levels. There has not been a clear conclusion however how the different approaches fair on many criteria combined and what the impact of this factor alone is.

b) Another dichotomy exists between the proponents of open-source software and systems as a means of increasing transparency and cybersecurity hand in hand, and those who rather favour proprietary software and systems in the interest of business development. In particular, while there is a strong view among experts that open source enables easier third party auditing of the software, there was no clear consensus to recommend support for open source as a solution for a trustworthy internet. However, open source can be maintained as a "possibility", e.g. one of the ways to enable trust in digital transactions.

c) A third tension refers to the need for promoting an insurance market. There are different views on this question: on the one hand the need for some insurance intermediary is broadly recognised, as this would enable greater participation in the digital market especially of citizens and small business when they are insured against the risks of cybercrime. On the other hand, some of the cost of cybercrime, such as reputation loss, is social rather than simply economic and the victims cannot be compensated in many cases. Furthermore, support to the development of an insurance market for cybersecurity has been contested as a necessary policy intervention. Instead, the market is already developing solutions to address these problems as the cybersecurity field evolves, without need or justification for policy intervention.

5.2. Recommendations

The following Recommendations form the core of this Opinion. In contrast to the Observations, they concern issues where there was ample consensus among the scientific and stakeholder communities, and where there is a case for either an unambiguous policy line or a policy action to be taken within the EU.

CRYPTOGRAPHIC STANDARDS

Safety, trustworthiness and resilience of the information infrastructure rely on cryptography. Undermining cryptographic standards implies undermining the security of our increasingly digital economy.

There is broad consensus in the scientific community that maintaining high cryptographic standards and avoiding backdoors therein is essential for citizens, companies, governments and others in order to protect their digital assets, transactions and communications.

Any manipulation detrimental to or weakening of the cryptographic standards or the technical implementation of cryptographic mechanisms undermines security and, hence, must be strongly discouraged by the European Commission. By following this approach, the European Commission would also help to foster trust between other parties (e.g. Member States, businesses).

Ensure that cryptographic standards in the EU reach and remain at state-of-the-art levels.

To maintain the trust of users/citizens as well as protecting their privacy and providing security, neither back doors nor other ways of weakening encryption should be introduced.

SYSTEMS APPROACH

Linked to the above, there is a need for measures to deploy best-practice systemic approaches to software and hardware design and development, covering the full ecosystem of cyberspace applications and services to take account also of security vulnerabilities of the IoT.

Encourage the adoption of a systems engineering approach to the totality of on-line relevant ICT developments - starting from the design stage, and throughout connected systems, including the EU's Internet and Cloud infrastructure.

Pursue and enforce security and privacy by design and by default, covering both software and hardware, as recognised in the General Data Protection Regulation (GDPR).

TECHNICAL VULNERABILITIES

Given the impossibility of achieving a perfect system, it is important to avoid overly focusing on detection and prevention of attacks at the expense of resilience, robustness, and mitigation. One should aim to strike a good balance between prevention and mitigation to improve overall cybersecurity.

Recognizing that software and hardware vulnerabilities are at the core of cybersecurity, Europe should focus its efforts on reducing software vulnerabilities over the product life cycle, requiring "duty of care" from design to testing and verification, including formal verification where applicable, long term maintenance and fast repair. In parallel, emphasis should be placed on the timely fixing of hardware vulnerabilities, especially through supporting testing and verification of hardware.

Provide at EU level appropriate incentives (including economic and legal) to encourage responsible disclosure and repair of vulnerabilities.

CONTEXTUAL IDENTITY

Protecting privacy is consistent with practices whereby digital transactions only require a minimum amount of personal data to be divulged which is relevant to the given context and, by default, used exclusively in that context unless expressly permitted by the data subject (person). This should prevent personal data which is divulged with permission in one context from being used in a totally different one, without the individual's consent or knowledge (for example, personal medical data being used for commercial purposes).

To respect privacy, promote the development and context-tailored use of attribute-based digital identity management.

ENGAGING CITIZENS

Improving education and the awareness of citizens/ users on cybersecurity issues and the practices and behaviour they should adopt is crucial. However, this should not result in shifting responsibility to the users and removing the responsibility and "duty of care" from producers.

Promote data-literacy education and build European citizens' awareness on cybersecurity. Promote citizens' engagement in shaping the future of the digital world, respecting fundamental values.

USER CHOICE

In the digital world, "power lies with the control of data". Personal data includes information relating to an identified or identifiable natural person ('data subject'). When data subjects have (more) control over their data, power shifts away from those public or private organisations (which mostly control and/or process such data) to the data subjects – i.e. to those whose fundamental rights need to be protected.

Transparency is an important core principle. One of the areas characterised by a lack of transparency is profiling -service providers profile data subjects in non-transparent ways.

The GDPR is an important step towards increased transparency. Ensuring that it brings a change "on the ground" is a next step.

Transparency should also bring about more user–driven innovation in the digital market.

Support the deployment of the means - including technologies and processes - for user choice and control over their digital identities, footprints and personal data.

Support individual autonomy and privacy by giving users well informed options, including the opt-out right not to be profiled and the right to be forgotten.

CYBERSECURITY INDUSTRY

In order to build cybersecurity leadership in the EU, increased and improved cooperation between public and private sectors is required, as well as a stronger research base.

Support the development of an EU cybersecurity industry ("made in Europe"), including data transfer and network technologies, protection of meta data, and "cloud"-based data storage and processing, to enhance the security of digital systems and guarantee the fundamental rights of EU citizens, while also increasing job creation and European competitiveness in the global market.

TRAINING PROFESSIONALS

The skills base for cybersecurity in the EU needs to grow and evolve in line with the current needs and challenges. In particular, cybersecurity education must become more attractive as there is a lack of cybersecurity professionals in Europe.

Curricula for the training of cybersecurity professionals should mainstream structured and system approaches for the design and development of IT software and hardware systems to increase their resilience and to facilitate the identification of vulnerabilities and their repair. The curricula should ensure a multidisciplinary mix between technical aspects, knowledge and competences from the social sciences, and legal matters.

Promote cybersecurity education curricula and lifelong cybersecurity training to build talent and sustain the skills of professionals. Make cybersecurity education more attractive to students.

Educate system engineers to further develop a "security" skills base in Europe and to shift to a systems design model which incorporates security principles from the very beginning.

EVIDENCE COLLECTION AND SHARING

There is a tension between the need for collecting and, most importantly, the sharing of evidence on cyber-incidents in order to improve cybersecurity, and national security concerns, which limit such sharing. While recognising this tension, the EU should foster such Europe-wide evidence collection and sharing, including cooperation between public and private sectors.

Support the development of evidence collection methods, including sharing of evidence and best practices, between EU member states of cybersecurity-related information.

Improve the mutual trust between national entities (e.g. Computer Emergency Response Teams - CERTs) such that intelligence information can be more freely disseminated between stakeholders.

Develop and monitor cybersecurity standards and practices, and provide sufficient authority and resources to do so, including adequate technical expertise in European bodies.

EU AND THE WORLD

Experts concur that the ability of governments and businesses to respond to and attenuate cyber-attacks is hampered by the lack of a coherent, international cybersecurity governance framework. Robust cybersecurity governance is not only required to deal with the current threat landscape, but also for future-proofing against new threats, while being open to potential opportunities.

Given the global and rapidly-evolving nature of cybersecurity challenges, Europe should be at the forefront of establishing worldwide and coherent cybersecurity governance for the digital economy. This should be consistent with and build upon a strong European cybersecurity governance framework, fully aligned with European values and the fundamental rights of EU citizens.

ANNEXES

Annex 1 – Methodology

Following the request of Commission VP President Andrus Ansip in January 2016 the SAM HLG took up the task to deliver scientific advice on cybersecurity with a view to inform EU policy for the next years. The specific task is described in a scoping paper published on line in January 2016[47]. The SAM HLG members Rolf-Dieter Heuer, Pearl Dykstra, Janusz Bujnicki and Cédric Villani led the development of the Scientific Opinion (hereafter the Opinion).

This Annex sets out the approach used for the collection and analysis of evidence that has informed the development of the Opinion of the SAM HLG.

Cybersecurity as a scientific discipline?

Cybersecurity is both a nascent and rapidly expanding field of study with a growing body of research papers and grey literature. Research in cybersecurity reflects the big socio-economic stakes involved and the urgency to try to keep up with the pace of cyber-crime development. Cybersecurity has many different facets that cut across several disciplines ranging from social science to mathematics and computer security. Indeed as a topic it is arguably best viewed through a multi or inter-disciplinary lens in order to understand the complex issues that arise from the interactions between people, processes and technologies.

Partly as a consequence of its broad multi-disciplinary nature and its rapid development, cybersecurity has not yet acquired the characteristics of an established field of academic scientific investigation or endeavour. For example, a detailed literature review conducted by two MIT scholars (Ramirez and Choucri, 2016) describe cybersecurity as a new field springing out of many old ones where to date little attention has been given to

[47] https://ec.europa.eu/research/sam/pdf/meetings/hlg_sam_012016_scoping_paper_cybersecurity.pdf#view=fit&pagemode=none

standardizing terminology let alone the development of standards of research. The systematic review of inter-organisational information security by Karlsson *et al* (2015) found that most published research and studies are either descriptive, philosophical or theoretical, with most only using subjective and argumentative methods, with relatively very few studies that combine theoretical work and empirical data. Overall this investigation confirmed the commonly-held view by the academics, that the field would benefit from a more systemic and more rigorous evidence based approach.

Given that many solutions that are proposed to improve cybersecurity are not particularly evidence based, this Opinion has combined several lines of enquiry. Whilst the process included a multi-stage review of the literature, it was far from being reliant on this. Considerable effort was paid to the gathering of expert opinion, and identifying expert consensus and supporting evidence via a major workshop and through a series of consultations and interviews with a wide range of experts and stakeholders.

The evidence gathering process

Overview

The scoping paper provided a broad brief and, as a consequence, evidence gathering for the Opinion initially took in a wide range of subject matter on many aspects of cybersecurity within the context of the DSM. The contributions from a large number of experts played a significant role in the exploration of the topic. Evidence was gathered on the many different facets of cybersecurity and the DSM, ranging from people and processes to technologies and the complex interactions between them.

The evidence gathering process consisted of seven main elements:

- Review of existing EU policies and legislation plus related EU policy reports and studies
- Review of the scientific literature (including grey literature)
- Participation in conferences

- A two-day, expert workshop - Vilnius, Lithuania
- Consultations and interviews with experts
- A 'sounding-board' type meeting
- A meeting with stakeholders in Brussels, Belgium

Only publicly available evidence was used in the development of the Opinion. Different lines of evidence were combined to inform this Opinion - this is shown schematically in Figure 1:

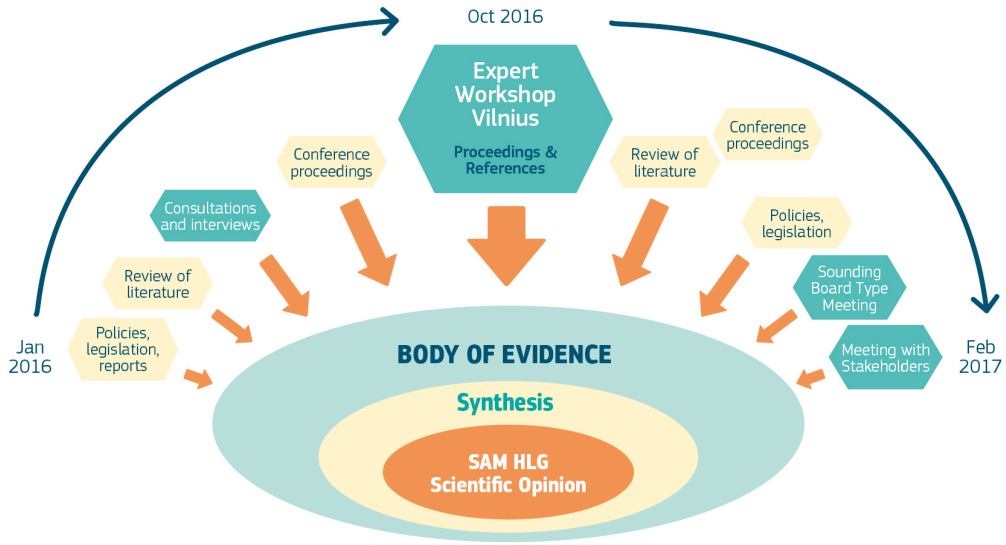


Figure 1 - Lines of evidence used in the cybersecurity Opinion

Source: Authors' elaboration

During the development of the Opinion, the SAM HLG took care to identify where there was a consensus amongst those parties consulted on the issues and possible solutions. This process helped to develop the recommendations. Where significant issues were identified but where views were divided or the evidence was lacking as to the best way forward to improve cybersecurity, these issues were reported as observations.

Review of existing EU policies and legislation plus related EU policy reports and studies

The SAM Secretariat, in support of the SAM HLG, gathered and reviewed relevant policy and legislation documents. These were supplemented by EU reports and studies that were closely related to policy formation or review. Analysis of this information provided a clear understanding of the context upon which to develop the Opinion.

DG JRC provided supplementary technical advice to the SAM HLG which assisted the development of the Opinion.

Towards the end of this work, in January 2017, a final check was made for any new developments in the policy landscape. A presentation was given on 31 January, by the SAM HLG, to Commissioner Ansip and representatives from DG CNECT and DG HOME. The discussion confirmed that the emerging recommendations are relevant to the development of EU policy in the fields of cybersecurity and the Digital Single Market.

Review of the scientific literature

A multi-stage review of the scientific literature was carried out by staff of the SAM Secretariat under the direction of the SAM HLG.

The review commenced with a broad-based assessment that covered several disciplines. The review of the literature included the use of web search engines and the search platforms: Scopus, The Web of Science, and the EC's own FIND-eR (the latter providing access to all of the Commission's scientific publications). The searches included a substantial volume of grey literature. This review was later supplemented by literature from more targeted searches.

The experts who were consulted during the process were also invited to help to identify additional key references. Over time, the references that they identified significantly expanded the body of evidence for this topic and helped to provide fuller coverage of the pertinent literature. A listing of the

literature cited in the production of the Opinion can be found in Annex 6 – References.

Participation in conferences

As part of the evidence gathering process, members of the SAM HLG and members of the SAM Secretariat participated in two conferences.

- The Netherlands Presidency of the Council of the European Union High Level Meeting on Cyber Security (Amsterdam, 12-13 May 2016), and
- 4th Annual Cybersecurity Conference (Brussels, 17 November 2016)

Two day expert workshop, Vilnius

The expert workshop held by the SAM HLG, entitled *"Secure Digital Identities for the Digital Single Market in Europe"* which took place on 25-26 Oct 2016 in Vilnius, Lithuania, was a very important event in the development of the Opinion. Approximately 50 national and international experts participated in the structured workshop. The workshop was designed to explore all the aspects of cybersecurity as set out in the scoping paper, but with particular attention paid to the role of digital identities - which provided a useful 'entry point' through which to explore the various facets of cybersecurity. Attendance at the conference was by invitation only[48].

The experts who participated were proposed by the European Academies and/or by the SAM HLG following consultation with the DG JRC and other EU Services. Attendees included Academic Fellows from the European Council of Applied Sciences, Technologies and Engineering (Euro-CASE), the European Academies Science Advisory Council (EASAC), and All European Academies (ALLEA), as well as experts from industry, business, non-governmental organisations and EC services. Thus, the workshop benefited from a wide range of expertise, views, and geographic coverage.

[48] For more information see annex 3.

The workshop provided a very rich source of evidence, knowledge and insights on relevant cybersecurity subtopics such as digital identities and cryptography. The workshop sessions were especially helpful in exploring the interplay between cybersecurity and the cross-cutting notions of trust and privacy, both in general terms and in ways relevant to the economic/ DSM focus.

Based on the workshop, the importance of sub-topics such as digital identity and the notion of "trust" emerged as central cross-cutting themes which aided the development of the Opinion. Further, the workshop highlighted the multi-disciplinary, fast developing and complex nature of cybersecurity and its associated research base.

Both prior to and after the Expert Workshop in Vilnius, participants contributed papers and other publications which significantly supplemented the literature gathered by the desk-based literature search.

Consultations and interviews

As part of the evidence-gathering process, members of the SAM HLG and the SAM Secretariat met with the following organisations and people:

- European Commission's Joint Research Centre (DG JRC) Multiple consultations including a 'fact finding' visit to the Joint Research Centre, Ispra, Italy on 4 March 2016. Information about the visit can be found on the SAM webpage.
- Association for Computing Machinery (ACM) – Europe Several meetings with Dr Fabrizio Gagliardi, European Chair of EU-ACM.
- KU Leuven University (Belgium) Consultation with Prof. Preneel, Professor of information security at KU Leuven University
- ENISA (European Network and Information Security Agency) Discussion with Steve Purser, Head of the Core Operations Department of ENISA
- DG HOME (Migration and Home Affairs) and DG CNECT (Comms, Network, Content and Technology) Meetings with policy representatives.

'Sounding board' type meeting

In January 2017, as a follow up to the Vilnius workshop, the SAM HLG held a 'sounding-board' type meeting with three of the experts who had significantly contributed to the Vilnius workshop: Bart Preneel (KU Leuven), Stephan Lueders (CERN) and Erol Gelembe (Imperial College) and one "new" expert, Bart Jacobs (Radboud University). The meeting considered the draft findings of the Opinion and involved discussion and debate that focussed on a number of possible recommendations that the SAM HLG were developing. The experts provided valuable comment and supporting evidence.

Meeting with stakeholders

Towards the end of the evidence gathering process, a half day meeting was held with approximately 30 stakeholders in Brussels on 13/02/2017. Several stakeholder organisations were represented at the meeting, mostly from consumer and civil society organisations but also including a number of service providers and regulators. At the meeting, the SAM HLG presented the objectives, scope, and draft findings of the Opinion to the stakeholders. This was followed by an extensive 'open floor' discussion and an informative exchange of views between the participants. The meeting was very constructive, and provided useful comments on the draft findings of the Opinion. It also provided the SAM HLG with feedback about which issues and recommendations were of the greatest concern to the various stakeholders.

For more information see annex 4.

Annex 2 - EU landscape

Core EU Policies to which the Opinion relates

This annex lists the EU legislation and policies most relevant to the Opinion.

The relevant policy landscape when the SAM HLG started its work, described in section 3 of the cybersecurity scoping paper, consisted of the following:

- **EU Cybersecurity Strategy** (2013) - jointly adopted by the Commission and the High Representative, it outlines the EU's vision, clarifies roles and responsibilities and proposes specific activities at EU level. It seeks to ensure strong and effective protection and promotion of citizens' rights so as to make the EU's online environment the safest in the world.
- **Digital Single Market Strategy** (2015) - one of the main priorities of the European Commission, it aims to make Europe a world leader in information and communication technology, with all the tools to succeed in the global digital economy and society.
- The **Directive on attacks against information systems** (2013) - designed to help EU countries deal with large-scale attacks against businesses and government organizations. It penalises illegal access, system and data interference, among other areas.
- The Directive on combatting sexual exploitation of children online (2011)
- The Directive on Networks and Information Security (NIS) (see below)
- **The Regulation on the Electronic Identification and Trust Services (eIDAS)** (2014) **-** this puts in place a single set of rules on electronic trust services (electronic signatures, seals, time stamping, delivery services and website authentication) and electronic identification directly applicable throughout Europe. One of its objectives is to boost trust, security and convenience on-line, for government, businesses and consumers.
- **The European Agenda on Security** (2015) - this addresses new threats and threats that are more international, cross border and cross sectorial, with cybercrime as one of the three top priorities (alongside terrorism and organised crime).

Since January 2016 when work on the development of the Opinion started, the policy landscape has evolved. An up-to-date and comprehensive overview of the EU cybersecurity initiatives (including the legislative actions to fight cybercrime) is provided in a European Commission publication[49], the main elements of which are summarised hereafter.

Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (5 July 2016)

Delivering on the EU Cybersecurity Strategy and the Digital Single Market Strategy, the Commission adopted this Communication which includes a set of measures aiming at:

- **Stepping up cooperation across Europe**: the Commission encourages Member States to make the most of the cooperation mechanisms under the forthcoming **Network and Information Security (NIS) Directive** and to improve the way in which they work together to prepare for a large-scale cyber incident.

- **Supporting the emerging single market for cybersecurity products and services in the EU**: for example, the Commission will explore the possibility of creating a framework for certification of relevant ICT products and services, complemented by a voluntary and light weight labelling scheme for the security of ICT products; the Commission also suggests possible measures to scale up cybersecurity investment in Europe and to support SMEs active in the market.

- **Establishing a contractual public-private partnership (PPP) with industry**, to nurture cybersecurity industrial capabilities and innovation in the EU (more details below).

[49] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16540

Public-private partnership on cybersecurity (5 July 2016)

The Commission launched a new **public-private partnership on cybersecurity that is expected to trigger €1.8 billion of investment by 2020**. The goal of this partnership is to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, building trust between Member States and industrial actors as well as helping align the demand and supply sectors for cybersecurity products and solutions.

The partnership will be supported by EU funds coming from the **Horizon 2020 Research and Innovation Framework Programme (H2020)** with a total investment of up to **€450 million** until 2020 (the Commission hopes private money will be triple that amount in a few years). The Commission aims at launching the first H2020 calls for proposals under the cybersecurity PPP in the **first quarter of 2017**.

Network and Information Security (NIS) Directive (6 July 2016)

The Directive builds on three main pillars:

- Ensuring Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;

- Ensuring cooperation among all the Member States, by setting up a 'Cooperation Group', in order to support and facilitate strategic cooperation and the exchange of information among Member States, and a 'CSIRT Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;

- Ensuring a culture of security across sectors which are vital for our economy and society and rely heavily on information and communications technologies (ICT). Businesses with an important role for society and economy that are identified by the Member States as operators of essential services under the NIS Directive will have to take appropriate security measures and to notify serious incidents to the relevant national authority. These sectors include energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

Data Protection and Privacy: The two main pillars of the data protection legal framework in the EU are the **General Data Protection Directive** and the **e-Privacy Directive**.

General Data Protection Regulation (GDPR)

The **EU Data Protection Reform** consists of two instruments: the **General Data Protection Regulation** and the **Data Protection Directive for the police and criminal justice sector**.

The General Data Protection Regulation will enable people to better control their personal data. At the same time modernised and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market by cutting red tape and benefiting from reinforced consumer trust. **The Regulation entered into force on 24 May 2016**.

Citizens regain control of their personal data

Two-thirds of Europeans (67%), according to recent Eurobarometer data state they are concerned about not having complete control over the information they provide online. Seven Europeans out of ten worry about the potential use that companies may make of the information disclosed. The data protection reform aims to strengthen the right to data protection, which is a fundamental right in the EU, and allow citizens to have trust when they give their personal data.

The new rules address these concerns by strengthening existing rights and empowering individuals with more control over their personal data. Most notably, these include:

- **easier access to one's own data**: individuals will have more information on how their data is processed and this information should be available in a clear and understandable way;

- **a right to data portability**: it will be easier to transfer one's personal data between service providers;

• **a clarified "right to be forgotten"**: when one no longer want your data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted;

• **the right to know when one's data has been hacked**: For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible so that users can take appropriate measures.

Clear modern rules for businesses

In today's digital economy, personal data has acquired enormous economic significance, in particular in the area of big data. By unifying Europe's rules on data protection, lawmakers are creating a business opportunity and encouraging innovation.

• **One continent, one law**: The regulation will establish one single set of rules which will make it simpler and cheaper for companies to do business in the EU.

•**One-stop-shop**: businesses will only have to deal with one single supervisory authority. This is estimated to save €2.3 billion per year.

• **European rules on European soil**: companies based outside of Europe will have to apply the same rules when offering services in the EU.

• **Risk-based approach**: the rules will avoid a burdensome one-size-fits-all obligation and rather tailor them to the respective risks.

• **Rules fit for innovation**: the regulation will guarantee that data protection safeguards are built into products and services from the earliest stage of development (Data protection by design). Privacy-friendly techniques such as pseudonomysation will be encouraged, to reap the benefits of big data innovation while protecting privacy.

e-Privacy Directive

The Directive on Privacy and Electronic Communications, known as the ePrivacy Directive (which was amended in 2009), sets out rules on how providers of electronic communication services, such as telecoms companies and Internet Service Providers, should manage their subscribers' data. It also guarantees rights for subscribers when they use these services. Most of the articles of the current e-Privacy Directive apply only to providers of electronic communications services, i.e. traditional telecoms companies. Information society service providers using the Internet to provide communication services (e.g. Skype) are thus generally excluded from its scope. The review of the ePrivacy Directive is one of the key initiatives aimed at reinforcing trust and security in digital services in the EU with a focus on ensuring a high level of protection for citizens and a level playing field for all market players.

Following a public consultation from April to July 2016, in January 2017 the European Commission adopted a legislative proposal to reform the e-Privacy directive as foreseen in the EU Digital Strategy (para. 3.4, p. 13).

Annex 3 - Experts Workshop

'Cybersecurity in the European Digital Single Market'

Workshop of the High Level Group (HLG) of Scientific Advisors of the European Commission's Scientific Advice Mechanism (SAM)

Lithuanian Academy of Sciences, Vilnius, Lithuania (25-26 October 2016)

Overview

In preparing its Opinion, the SAM HLG held a dedicated two day long workshop on cybersecurity with approximately 50 expert practitioners, regulators and academics. The discussions and insights from the workshop contributed to the formulation of the SAM HLG's Scientific Opinion which was delivered to the Commission in March 2017.

The workshop provided an interactive platform to gather evidence and initiate discussions that greatly contributed to the SAM HLG's opinion to the European Commission on cybersecurity. The workshop was multidisciplinary in nature, with scientific experts from the domains of information technology and security, social sciences and humanities, and from law, all contributing to the body of the scientific evidence upon which the scientific opinion was developed. In addition, the workshop cast light on the current and future challenges and opportunities of the fast changing world of cybersecurity as viewed by different groups of stakeholders – ranging from businesses and consumers to public administrations.

The workshop was chaired by Rolf-Dieter Heuer, and each session was co-chaired by two SAM HLG members. The participants, included 50 experts, ranging from academics in digital technologies to social sciences and law, government officials, civil society and business professionals. All presentations, workshop documents and list of participants are publicly available (via the web-link at the start of this section). To encourage openness and the sharing of information, the Chatham House rules were

applied in the discussions, whereby discussion points were noted but not attributed to individuals.

The workshop mainly addressed the following four topics:

1. Understanding digital identities through a multidisciplinary approach
2. The Strengths, Weaknesses, Opportunities and Threats (SWOT analysis) of digital identities
3. Privacy and security
4. Security and trust in the digital world

The following is a summary of the wide ranging discussions at the workshop. This summary, is structured around the topics discussed. It provides an overview of the various points made and arguments put forward. It shows both the diversity of views expressed and the areas where there was consensus among the experts.

Given that the workshop followed Chatham House rules, comments are not attributed except in cases where they are part of one of the workshop presentations published on the SAM website.

DIGITAL IDENTITIES AND CYBERSECURITY

The first part of the workshop concentrated on **digital identities** starting with a discussion of how these should be defined.

A dictionary definition of identity refers to the name and qualities that make a person different from others[50]. It is therefore important to define the elements that comprise an identity. We may know some elements of a person's identity, but when do we know enough to identity them correctly/

[50] According to the Oxford Dictionary, identity is defined as the fact of being who or what a person or thing is, and more specifically the characteristics s determining who or what a person or thing is „ while for an object it is serving to establish who the holder, owner or wearer is by bearing their name and often other details such as a signature or photograph: an identity card.

unambiguously, and what concretely are these elements that we need to know[51]?

There are individual and collective aspects of identity, i.e. elements that make someone unique or part of a group (gender, ethnicity, profession etc.). On the other hand, there are elements containing **personal data,** which in many cases are given "freely" by citizens to Facebook and other social media accounts (e.g. age). Other identity elements however are less easily divulged by a person, and considered areas of not only privacy but "**intimacy"** (such as sexual orientation, religion or belief, health information). According to the presentation by the keynote speaker, N. Arpagian, privacy is already "given up" by users when they give data to social media accounts. There are three important concepts to distinguish: **identification, authorization and authentication**[52].

To better understand identity, one needs to examine how it is experienced and how this **experience** has changed from the past and is being radically transformed in the digital world. The transformation in the way people experience individual identity has become an experience of a "disembodied identity" (i.e. our digital identities not being experienced as our "true selves"), is purported to be one of the main explanations for the **paradoxical behaviour** or "sloppiness" of individuals on the internet. In other words, it has been argued that people do not feel the same kind of ownership of their digital identities as they do of their personal identities.

According to this theory, our online identity appears to us as single and fixed, virtual, the result of a registration (what we do and have done) - a set of data. Therefore, the bond between the digital identity and the actual person is weak, and this weakness is claimed to be one of the sources

[51] This was illustrated at the workshop with the example of three Picasso paintings, very different in style, where, from what most people know about Picasso, one of the three is easily identified as a Picasso painting, while for the other two, most people who know of Picasso's work would fail to identify them as his (N Arpagian, keynote presentation at Vilnius *)*
[52] This is illustrated by the example of entering one's house: *I can enter my house because I have the key, not because the house checks that the person who tries to enter is "me".*

leading to the view of the human user as the **weakest link** or **"risk"** in cybersecurity terms.

An example of human actors as a cybersecurity risk is the problem of **weak passwords** (e.g. common passwords such as 1234… or a series of 0 digits ….). It was also remarked that password policies aiming to address this problem (rotation, restrictions...) may actually make things worse, as users write down their passwords in unsafe places, especially when they are quite complex in order to be "safe", leading to the opposite result.

Another view is of the human user as a "**victim"** of cybersecurity. This is in line with an approach that argues for a need to "protect" citizens from malicious attacks. As some participants have pointed out, it is important to consider the question of data literacy for citizens as well as their rights and responsibilities. There is a fine line here between "protecting" and "blaming" the victim.

An important distinction to make is between **identity** and **identifier.** An identifier is a person or thing that identifies someone or something. It is often used in computing as a sequence of characters. From a mathematical point of view, identity is about assigning an identifier to a person or a group of people. The identifier is directly measurable and has a list of attributes. There are also pseudo-identifiers, given by third parties. When identifiers are assigned, the rules for so doing must be agreed and clear. However, the discussion also pointed out that even if the rules are appropriate, they may be improperly (incompletely) implemented, which can actually exacerbate the problem by giving people false assurance.

Participants broadly agreed that there are many good, already "known" ways to define (unique) identifiers for people. There are also different models or approaches regarding how many attributes to reveal:

- Less is more: IRMA (I reveal my attributes; to buy alcohol I reveal my age)
- More is better: data as a resource (internet economy, data brokers)

People have **multiple identities** (in the "real" world as well as in the "virtual" world). They present themselves at different times and sometimes conflict with one another.

There are many places on the internet where people can give up data that constitute "identity elements" (part of their identity used to identify them). A person can easily create many identities on line, and according to known data on the use of social media accounts, many people have several accounts but do not use all of them (so there are more digital identities than actual users)[53]. Provision and certification of identities for citizens in the past fell under the responsibility of the government, but increasingly private sector solutions have become available.

Multiplicity of digital identities also occurs in citizen interaction with public administrations: i.e. when different government departments require you to register separately for their specific service (for example, as one participant put it: *you have to register for one certificate - so one identity - and then you pay taxes with another)*.

An important factor for the success of any ID management approach is **societal acceptance.** Firstly, citizens will try to circumvent a system if they do not agree with its purpose, and secondly, citizens may be hesitant to trust governments (in some countries more than others, largely depending on history). In contrast, people may "trust" businesses with their data, not necessarily because they feel more secure but as one participant put it, *simply because business provide rewards.*

The importance of citizen acceptance is reflected in identity management systems where control over data lies with the data subject permitting **"opt out"** procedures (e.g. in Austria, if a person does not want to participate in an electronic health system, he/she is required to bring his/her health records to a medical appointment). Another option available to citizens in such systems is the right to be **"forgotten"** by commercial businesses (e.g.

[53] Globally: 5.5 accounts, 2.8 of which are active

to have one's digital history deleted), as well as the option to deny an identity (e.g. if one's identity has been hacked/ stolen, the citizen has the right to reject/ deny payment for fraudulent transactions and cannot be forced to pay). This approach suggests that citizens should have the option to have their digital shadows erased.

In this context, reference was made to the **General Data Protection Regulation (GDPR)** that will apply in all EU Member States from May 2018 on, giving greater control over one's data to the so-called "data subject".

Overall the discussion in this (introductory) part of the workshop broadly supported the view that human factors, technologies and systems are all important in their interaction and that one needs to think **holistically,** taking into account the human user and the technical/systemic aspects.

* * *

Following the discussion on how to better understand digital identity/ies drawing on a multidisciplinary perspective, the workshop then focused on the relationship between digital identities, cybersecurity and the digital market, before going into broader issues of cybersecurity (beyond the issues of digital identities).

It was broadly accepted that the question of digital identity and its relation to cybersecurity has at least two different facets: on the positive side it is an **asset** for citizens, but on the negative side, it is **a target for criminals**. An understanding of digital identity needs to take this tension into account.

As far as cybersecurity is concerned, identity is not the only purpose, but only the first step towards something else. Stolen identities are used to open doors, get information about businesses, etc. As one participant put it, *"you can be the target, sometimes just because someone needs an identity to commit a crime".*

According to data presented at the workshop (https://ec.europa.eu/research/sam/index.cfm?pg=cybersecurity), ID thefts are the second most common complaint to the US Federal Commission for Trade. Other data show that the cost of cybercrime in leading economies is significant, at $100 billion fraud in the US, and $400 billion globally.

However, despite such problems, digital identities remain essential for the digital economy. There was broad agreement on the point that, for the EU and the DSM (Digital Single Market), strong digital identities can help to increase **trust in business** and this could increase digital transactions and therefore the overall socio-economic value and importance of the DSM. In the EU, the main aim of the eIDAS Regulation is to promote business.

One of the points made by some participants in relation to the costs of cybercrime is that there is a lack of an **insurance** market for cybersecurity, and this has serious effects in limiting people's participation in the digital market. Others however remarked that this is changing, and market mechanisms are more appropriate to address this issue without need for policy intervention.

There was broad agreement that securing digital identities is to a large extent an economic problem rather than a technical one. Digital identities are a key feature of the **business model** of the internet whereby businesses provide services in exchange for data. In discussing the economic (business) rationale for strong digital identities, it was explained that for a government, the **economic incentive** to create strong digital identities fails because the level of use is too low (because the interaction with a citizen that uses digital identity is usually not more than a few times a year). Incentives could encourage companies to develop more secure software and devices. The issue then would be, whether and to what extent, **public intervention** is justified or required to help to address an apparent lack of private sector incentives and market failures to improve security.

Participants also discussed **credit cards**, as a case where the business model, some claimed, has provided a **good solution**, in the sense that despite credit cards being insecure, they are widely used by consumers. For those supporting this view, this is an example of a functioning business model where security improved after the detection of frauds, and where there is a quick repair and compensation mechanism, which instils trust among consumers because their interests are safeguarded by the credit card company. However, others explained that the credit card is not really a good example, because the costs are hidden and are merely shared across all the credit card customers.

Where many participants however agreed, was on the fact that **legal systems take long to adapt** to crimes in the digital world, including identity theft. In many countries the law is tailored to the physical world and only recently developed for digital ID theft. Despite the fact that identity theft is so common and can have big economic consequences, penalties are low compared to penalties of stealing someone's ID in the real word. An example illustrated at the workshop was the case of penalties to offenders in the real and online world in France.

While the economic costs of attacks on identity can be significant, the **social cost** can also be very high and it is not captured in data and statistics. Attacks targeting a person's reputation can be disastrous for an individual, who is often left without compensation or rectification.

Some participants claimed that one of the main problems making it difficult to have more secure systems lies with the very way both software and hardware are developed. When the internet was originally designed, it did not need to consider the current threat landscape. This has changed with the expansion of the internet.

According to these experts, the lack of a **systematic approach** to designing identity management or systems that take into account the actual threat landscape is currently very problematic. Systems are designed without having a rule-based model of the whole system. Almost no systems

document their desired functionality and the threat landscape they are (or should be) designed for. This leads to recurrent **patching** and makes it increasingly difficult to provide cybersecurity.

A systems-designs approach to security is therefore needed to reduce the amount of *ad hoc* patching. But a **"systems-designs" approach** is not simple, and may take a long time. Other participants also emphasised that rather than deal with threats, developers should **consider how to manage risks.**

While recognising these challenges, participants stressed that the EU has some strengths in this field, namely excellence **in cryptography** and a very good research base. It was also noted that advantage could be taken of EU public procurement of innovative solutions -especially for SMEs and creative industries - in the context of increasing awareness and creating an environment for innovative ideas.

A major weakness according to a broadly shared view is the lack of sufficient **skills base** in Europe.

The case of **Estonian e-Identities** was presented by Ahto Buldas. Estonian ID cards contain a cryptographic microchip capable of creating digital signatures. The Estonian X-Road is the backbone that connects the decentralized databases of all institutions. Over 2000 services are used over X-road. Cryptographic mechanisms are used to prevent the abuse of pseudo-identifiers. The model used in Estonia relies on Trusted Third Parties (TTPs), but it is insufficient for detecting misbehaviour of TTPs. There are no scientific theories that enable an adequate estimate of the probabilities of such threats. In terms of user experience, the Estonian id-card is needed for all activities as Estonian citizen. This allows transparency over the use of data: one can see who has access to their data (for example which doctor has access to tenor medical records) as well as who had changed their data. The latter is especially important as it allows citizens to detect who has been tampering with their data, and there are sentences for this ("people have been sentenced for tampering data").

To secure identities, two basic opposing concepts can be used: classical high quality **encryption** and **block-chain** (or **distributed ledger**) technologies. Many scientists favour classical encryption because block-chain techniques potentially might result in very high electricity consumption with high demands on processing power and data storage capacity. Distributed ledger enables full transparency of transactions. However there were many concerns at the workshop regarding wide application of this technology, including regulatory uncertainty. In addition some participants suggested that privacy issues are not sufficiently handled, especially in the cases where personal data protection is needed. Participants also noted that devices (software and hardware) must be safe also, not only the communication. Systems must be patched and up to date to avoid compromise. For all these reasons, there was some agreement that any wide application of distributed ledger technology is currently "not a good idea" and would not generate the trust needed for growing the Digital Single Market.

On the other hand, as many experts explained, there seems to be currently **no real technical challenge** for hackers to steal digital identities. There is even a lot of information on the internet about how to hack: it is technically relatively easy and cheap. It is also easy to pretend you are someone else, even if this is an institution. In addition, the threat to privacy is real, with **profiling technologies** used by service providers, where they can, make an 'overall picture' of your social behaviour to identify you.

In a similar argument, data cannot be completely secure. Moreover, even if they could become so, the investment required for this would not be justifiable. Furthermore, the impact of a fully secure system if they were possible to achieve, would be, according to this view, highly questionable. For example, in a system of almost fully secure identities it would be very difficult for a citizen to contest an identity-based claim against him/her (for example to deny a fraudulent online purchase they did not make but which is debited to their account).

To summarise, this discussion concluded, among other things, that:

- There is no such thing as "secure" identities;
- Today, digital identity implementations should be revisited considering the threat-detection principle, and looking at the system as a whole (a systems approach);
- This also requires that IT education principles are revisited, and students are educated in this approach (as system-engineers, rather than software programmers).

The question of a rigorous scheme for digital identity in Europe concerns not only the current state of the art, but also the future, particularly in the context of the **Internet of Things (IoT).** Many expert voices at the workshop strongly suggested that IoT security is poor (see also section 3).

There are a number of different options in order to increase security, which do not require quasi fully secure digital identities. Such options are for example:

The **1-time code, e.g. identity for a single purpose**: Create an email just for one use, and after that cut all the links with people who try to access it. Pre-paid SIM cards worked this way. The characteristic of this approach is that there is no way to identify someone if this method is used.

Anonymisation of users' personal information: There are two main approaches to achieve anonymisation, either to remove personally-identifiable information from a database, or to protect identifiable data through controls on the queries. This approach, for some experts, has strong advantages, notably that, by reducing the importance of digital identity it also makes identity theft less interesting (for cybercriminals). According to this line of argumentation, *ID thefts are so dangerous because IDs can be sold. If we had an anonymous world, then ID theft would not be attractive.* Or, as some participants put it, when payments are involved there is motivation. If there is less emphasis on ID verification, alternative solutions can be found going away from the risk-prone focus on ID.

Other experts emphasised the principle of **minimal disclosure** of data as the way forward. This approach is in line with those experts who focus on privacy - known as the "privacy community" in the field. The objective in the privacy community is to have minimal identity, e.g. to ensure that the economy can function without full identity disclosure.

PRIVACY

The discussion broadly acknowledged that different digital identities apply to different contexts. In order to securely identify someone, what needs to be taken into account is primarily the **particular context of the transaction**. This determines what attributes are needed for the identification (attribute selection, attribute aggregation). In other words, according to this view *"requirement analysis is necessary – not a one-size-fits-all approach".*

Other issues that came up in this discussion include:

- Engage citizens and increase data literacy in different ways - there is data on citizen engagement in related areas (hackathons, etc.).
- A better understanding of human behaviour is required.
- All technologies have various advantages and weaknesses. There may be a need to separate activities by sector.

Much emphasis was placed on data protection as a **fundamental right in the EU.** Some participants have taken this further to argue that power relations are necessarily implicated in the design of ICT infrastructures. The view suggested was that, when designing systems, one needs to think what the effects on people are, and on the balance of power in society. In other words, **"architecture is politics".**

While data protection is respected across the EU, there are **differences between Member States** in how the question of privacy is perceived and treated. For example, Germany has one of the highest standards for data privacy, but there evidence of companies not respecting privacy and transparency standards was provided by experts at the workshop (e.g. a

Deutsche Telekom AG case where non-executive board members, employees, and journalists fell victim to a spying scandal subject to the German telecommunications secrecy law in 2005–2006).

Differences are also due to cultural and historical reasons, and linked to citizens trust in government. It was noted for example that in the UK trust in government is low, while in Scandinavian countries it is high, and this has an impact on citizen attitude to the use of their data and to making them publicly available.

In a global context the differences are more striking: it was argued that in the US identity management is perceived to be linked to surveillance, while in Europe it is a lot more perceived as a service to citizens. This was also linked to the **US /EU - privacy shield,** with some experts stressing that data protection in the minds of Europeans is an expression of individual rights and freedom. Moreover there are technologies that are privacy sensitive or protect privacy (**privacy protecting technologies**).

The GDPR clearly will play an important role in this field. However, some participants remarked that "rules about giving control to people over their data are "very fragile", and some commented that the GDRP is targeted at the processing entities, while it should (also) be targeted at producers. Finally, some commented that large internet service providers are doing a kind of "mass surveillance" which they claimed is completely contrary to principle of data minimization.

To know where data have been, detailed measurements are required as well as storage. This poses a huge technical challenge in mapping the kinds of things you would like to have to protect the data (link between technology and legal cases). A lack of technical means is particularly relevant in this context. **Forensics** on the internet are difficult, paths are difficult to follow (IP addresses can be spoofed; routing can go all over the world). Most importantly, the means for tracing cybercriminals (terrorists) are the same as those used by terrorists.

In addition, increasing amounts of data come from mobile phones; and there is very sensitive information in mobile health devices (such as health implants). In this sense, it has been argued that Europe needs to come up with a design and catch up fast with existing techniques. Some experts suggested that a data base of solutions could also help in this direction. Some of the more notable conclusions from this part of the discussion include:

- There is a fine line between privacy and national security: the same techniques are used by criminals and by policing authorities
- National security and internet security are not necessarily aligned
- National intelligence agencies have special powers. With the emergence of new techniques, it is not always clear whether new legislation needs to be introduced or whether existing can be stretched.

Law enforcement is trying to track terrorists through websites (via IP addresses), posing very interesting challenges. In addition to considering direct needs of citizens, there is also a need to consider the needs of law enforcement and security agencies and how they carry out their work to protect citizens. Monitoring the practices of abusers (e.g. websites of radicals that attract visitors and follow them and analyse their identity) and mirroring them can be used as countermeasures.

Some participants suggested that an important issue is how scientists could help privacy analysts. This would have to take into account also policemen and border protection services, and the issues around internet radicalization. Such an approach would complement the "citizen" perspective.

EMERGING TECHNOLOGIES, NEW RISKS

It was broadly agreed that the Internet of Things (IoT) poses serious cybersecurity issues, "*new risks in complex ecosystems....".* The devices or "things" provide an easy first entry for hackers to reach more central systems. In other words, there was broad consensus that IoT is an

enormous vulnerability when it comes to security and privacy protection. For this reason, some participants explained that no device should be connected to Internet if there is no way to update its vulnerability level.

Overall there was broad agreement that in the future, the need for risk management will increase. It cannot be denied that there is a range of threats - but according to many participants there are justifiable reasons to work with individual data, to not be risk averse, and to manage the risks in a practical way.

The human factor, a recurrent theme in most areas of discussion, also featured in relation to new and emerging technologies. There was a broad consensus on the necessity to increase citizens' awareness, to enable citizens to be responsible and knowledgeable users of new technologies. Participants broadly suggested that more evidence on what works and evidence of best practices in making citizens more aware should be at the core of cybersecurity policy. Some also suggested that while there is important research and innovation (most of the solutions come out of academic labs) it is not clear what is going on in the market and what solutions are out there in individual Member States. More data gathering and comparison of approaches is needed.

Highlighted conclusions of this section include:

- A lot can be done by working directly with citizens. Engagement of citizens, increase data literacy, in different forms.
- There is a need for designing systems that make a citizen know what is going on with their data.

TRUST

Trust has an enormous social and economic relevance. At the level of the whole economy, it is essential for growing and maintaining participation. At the level of a digital based enterprise, losing trust can lead to major economic loss and failure in the market.

The level of trust in the digital world can make a difference to the growth of the digital single market, to jobs and the application of new technologies in addressing societal challenges and creating new opportunities. Ultimately it will make a difference to the kind of society that is being shaped in a digital world in Europe, notably the forms of civic participation and protection of individual rights.

One of the presentations focused on the issue of trust and the complex relationship between trust and security (//ec.europa.eu/research/sam/cybersecurity). As a definition of trust the presenter proposed the following: *the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party (Mayer et al, 1995).*

This part of the discussion brought together issues from previous sessions, notably the role of the human actor, the question of vulnerabilities, verification, standards, cooperation at EU and international levels and information sharing between authorities, as well as the question of citizen security, national security and the relation between security and trust.

According to the broad view, **trusting is accepting some vulnerability**, which obviously has important implications when it concerns software and hardware vulnerabilities. A second important observation is that trust is inversely proportional to risk. Taking this even further, some of the participants explained that **"trust is bad for security".** One way to see this is that when trust increases beyond a certain point, security decreases because fewer security measures are taken (because the system is assumed to be secure enough to be trusted) and attacks become more widespread and are more successful.

Others highlighted that the importance of trust should not be overestimated, but on the other hand the importance of a lack of trust should not be underestimated.

A theme continued from previous sessions was software and hardware vulnerabilities. The broad consensus in the workshop was that **fast repair** is more important than trying to fix everything from the start.

A difficult challenge to develop trust and security is in the **production line**: we mainly import components and devices from outside EU. As one participant put it, *How can the EU ensure that cybersecurity standards are met if we are not producing ourselves?*

The question of trust was also placed within the broader social context of rights, power relations and transparency. As a social concept trust requires **transparency.**

There is also the question of centralised versus decentralised structures, which is linked to whether trust should be completely distributed without central nodes, or distributed to a quorum (federated), or there should be one entity that is entrusted (centralized).

Within the EU, some experts stressed strongly there seems to be insufficient trust among **national governments** to enable optimal coordinated cybersecurity action at EU level – because security issues are implicated in the highly-sensitive national security debate.

Many experts stressed at this point that **data are never secure**, because even if we have strong cryptography, there is no end to end security analysis (black box, no real estimation of the phone device). On the other hand, something we think is secure, we overly trust it.

Some experts suggested that **Open source** (OS) enables trust, and prevents backdoors. However, there was no clear consensus among the experts that open source is the solution. Instead, open source "is a possibility". For supporters of OS, a solution would be to develop an open (source), fully-transparent and resilient ICT infrastructure at the European level and support formal verification. One of the advantages is that open-

source software facilitates third-party auditing of the software by security researchers and academics, as there is no need for "reverse engineering".

A different view was expressed by some experts, who questioned the whole meaning of trust. According to this view, "*the importance of trust is overrated".* An example to illustrate this is to think of how many actions of our everyday life are really depending on trust. An alternative way to approach this is by recognising the need for trust when something goes wrong (when I am sick, I need a doctor I can trust). Furthermore, in most transactions we do not need to know much about the other party - as one participant put it, *when I sell my house I do not need to know much about the buyer, but I need to trust the whole system around the transaction to ensure it goes through*.

There is a variety of **standards** (security management standards, technical security standards, vulnerability management standards, security assurance standards, regional and domain-specific standards). Standards do not only concern security; mobile phones have an option (standard) to be not connected; but this causes signalling storm; increasing energy usage; attack on band width; so sometimes there are negative side effects of standards.

In general, experts agreed that standards are beneficial to security. However, some standards can be exploited and are very bad for security, e.g., allow the signalling storm attack. Some standards are outdated.

Many participants agreed on a suggestion for the EU have a common voice on standards, but stressed the need to determine the scope, and only employ standards where it is clearly beneficial.

Another example discussed was the case of **Zero-Knowledge Systems (**in zero-knowledge proof I can prove that I can give the password, without giving it away), however there was no overall consensus for a conclusion on this. The issue of **verification** was a major point of discussion, and many experts suggested that it is important to trust but also to verify (e.g.

against a mathematical definition of what it is). There was broad consensus among experts for the need to support formal verification. It was also noted that it is probably not possible for all parts (issue of modularity). Others highlighted that formally-verified software should be mainly for long term and only for smaller parts of overall packages, and that it is still out of reach for large and fast-moving code bases.

Many experts stressed that hardware can also have (intentional) backdoors. More awareness is needed, as well as a repair mechanism. Especially in hardware this is tricky, because a component may behave as expected at the start (so no problem is detected) but start to misbehave after a while. In other words, bugs introduced in H/W can go undetected for some time.

Another remark made in the closing discussion was that trust is not a motivation for someone to do something. It is a "hygiene factor" (as one participant put it, "*it is like cleanness in restaurants, you appreciate it and if it does not exist it may drive you away, but it is not the reason why you go to a particular restaurant*").

Web link: https://ec.europa.eu/research/sam/index.cfm?pg=cybersecurity

See section entitled *Workshop on Cybersecurity - Vilnius, 25-26 October 2016.*

Annex 4 - Meeting with Stakeholders

'Cybersecurity in the European Digital Single Market'

Scientific Advice Mechanism High Level Group (SAM HLG)
Meeting with Stakeholders

Brussels - Monday 13 February 2017

The meeting aimed to present the SAM HLG's draft findings to stakeholders - civil society, consumer organisations, businesses, as well as some policy representatives - and receive feedback. Around thirty stakeholder representatives were invited and took part[54]. Following presentations by members of the SAM High Level Group, the floor was opened to collect reactions, comments and questions from the stakeholders.

On the whole, the discussion revealed agreement with the draft findings presented. No specific disagreements or concerns were voiced but rather many helpful suggestions and remarks were given. One overriding message was a need for clarity in presenting the recommendations regarding their intended relevance for going "beyond" the current EU cybersecurity policy agenda.

The main points which were raised in the discussion were as follows:

- A number of stakeholders stressed that in order for Europe to compete globally in cybersecurity much more investment in basic/ fundamental R&D is needed than is currently the case, in addition to the investments made in more applied ICT R&D such as high-performance computing, etc.

- A number of stakeholders expressed the view that while the *aquis* so far goes in the right direction much more is needed to protect privacy, to cater adequately for profiling concerns, opt-in versus opt-out questions, data minimisation, etc. and in the process to impact upon a fast-moving target. This includes policy actions to promote sharing, cooperation, training, a fit-for-purpose ENISA-type

[54] For further information on the meeting, including agenda, presentations and list of participants, please see on the SAM Website https://ec.europa.eu/research/sam/index.cfm?pg=cybersecurity

capability and so on. It was also pointed out that profiling can be beneficial and desirable to the service user and it can also play a role in increasing cybersecurity as well as provoking concerns.

- It was stated also by a number of stakeholders that the long lead time and a *de minimis* harmonization approach for EU legislation (e.g. NIS) is incompatible with the rate of change in and the ambition required for the CS area. The importance of information sharing between not just Member States but also with the private sector was stressed by many stakeholders.

- There was a strong endorsement of the SAM HLG's emphasis on training and in particular the need to increase technical expertise in relevant public authorities and oversight bodies bringing it up to a par with legal expertise which currently dominates.

- Emphases on fundamental rights and transparency were welcome by many stakeholders, particularly in so far as they *inter alia* help to eliminate inegalitarian and discriminatory practices built into algorithms ACM's Principles for Algorithmic Transparency and Accountability released in January 2017 were cited in this regard.

- Regarding software vulnerabilities, it was pointed out that there are new agile models that involve multiple releases.

- Some stakeholders pointed out that "Duty of Care" regarding follow-up patching/ repair requires reciprocation so that producers are not held legally responsible for costs resulting from failure on the part of the client/ user to take the repair on board.

- A number of participants spoke in favour of developing European technical and business capabilities for strategic reasons linked to trust, lessening foreign dependency, etc. - analagous to Gallileo vis-à-vis GPS, etc. Protectionism should be avoided as well as anything that would limit access to the best available technologies and skills.

- European participation in the setting of global (ISO-type) standards was deemed to be most desirable.

- Legal reporting obligations of cybersecurity incidents under different pieces of legislation and to different public authorities was deemed to be a heavy burden which could possibly be replaced by a more one-stop-shop approach, according to some views of the stakeholder community.

Overall, the meeting confirmed that the areas the SAM HLG is covering with the Opinion are of much interest to the stakeholder community. The chair of the SAM HLG and rapporteur for the topic Rolf Heuer thanked all participants for their contribution and ensured them that the SAM HLG took note of their comments.

Annex 5 - List of experts and stakeholder representatives consulted

Amann Philipp *(EUROPOL)*
Amendola Antonio *(American Chamber of Commerce)*
Arpagian Nicolas *(Orange Cyberdefense)*
Benetis Vilius *(Norway Registers Development AS)*
Berbigier Nicolas *(FAMOCO)*
Bhargavan Khartikeyan *(French Institute for Research in Computer Science and Automation)*
Bourdon Steeve *(Huawei France)*
Briggs Pam *(University of Northumbria)*
Broeders Dennis *Erasmus University Rotterdam; Netherlands Scientific Council for Government Policy)*
Buldas Ahto *(Tallinn University of Technology)*
Camenish Jan *(IBM research centre Zurich)*
Caristan Yves *(Euro-Case; Science Advice for Policy by European Academies (SAPEA) – supported by Horizon2020)*
Castex Christoph *(European Commission Directorate General for Migration and Home Affairs (DG HOME))*
Christou George *(University of Warwick)*
Clémot Olivier *(Safran Identity and Security)*
Commers David *(I am the Cavalry)*
Demerlé Maxence *(Syndicat de l'industrie des technologies de l'information – SFIB)*
Dickman Peter *(Google)*
Domingo-Ferrer Josep *(Universitat Rovira I Virgili)*
Donio Jean *(Université Paris II Panthéon-Assas)*
Ferreira Afonso *(EC Directorate General for Communications Networks, Content & Technology (DG CONNECT))*
Froetscher Alexander *(AustriaTech)*
Gagliardi Fabrizio *(Association for Computing Machinery (ACM) - Europe)*
Gelenbe Erol *(Imperial College London)*
Georg Laura *(Norwegian University of Science and Technology)*
Goodey Joanna *(European Union Agency for Fundamental Rights (FRA))*
Goranin Nikolaj *(Vilnius Gediminas Technical University)*
Hämmerli Bernhard *(Swiss Academy of Engineering Sciences)*
Hankin Christopher *(Imperial College London)*

Hansen Marit *(Data Protection Commissioner of Land Schleswig-Holstein)*
Hecht Brit *(BBVA)*
Hoepman Jaap-Henk *(Radboud University Nijmegen)*
Holla Rogier *(Computer Emergency Response Team (CERT-EU))*
Holla Rogier *(Computer Emergency Response Team (CERT-EU))*
Jacobs Bart *(Radboud Universiteit Nijmegen)*
Jacobs Frederic *(I am the Cavalry and Spin Research)*
Jervan Gert *(Tallinn University of Technology)*
Katsikas Sokratis *(Center for Cyber and Information Security, Norwegian University of Science and Technology)*
Kert-Saint Aubyn Mari *(Guardtime)*
Knobloch Martin *(Nixu Benelux, the free and open software security community (OWASP), I am the Cavalry)*
Koch Rainer *(Deutsche Telekom)*
Korwek Justine *(Trans-Atlantic Business Council)*
Krahulcova Lucie *(Access Now (member of EDRi))*
Krimmer Robert *(Tallinn University of Technology)*
Kutylowski Miroslaw *(Wroclaw University of Technology)*
Lenoir Noëlle *(Kramer Levin Naftalis & Frankel)*
Lozano Jesús *(BBVA)*
Lueders Stefan *(European Organization for Nuclear Research)*
Lukasik Jacques *(European Council of Academies of Applied Scien*ces, Technologies and Engineering (Euro-CASE))
Maple Carsten *(University of Warwick)*
Markatos Evangelos *(European Cyber Security Organisation (ECSO))*
Martin Ruiz David *(BEUC - European Consumer Organisation)*
Martinelli Fabio *(Italian National Research Council)*
Martinez Marina *(Spanish Office for Science and Technology (SOST))*
Mattatia Fabrice *(Ministère français de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche)*
McCanny John *(Queen's University Belfast)*
Meitern Maarja *(Association for Computing Machinery (ACM) - Europe)*
Milisavljevic Nada *(European Commission Directorate General for Migration and Home Affairs (DG HOME))*
Muckle Nikki *(University of Warwick)*
Muir Stuart *(Dell)*

Nai Fovino Igor *(European Commission Directorate General Joint Research Centre (DG JRC))*
Nijk Anjos *(European Network for Cyber Security (ENCS))*
Nordvik Jean-Pierre *(European Commission Directorate General Joint Research Centre (DG JRC))*
Novais Goncalves Jorge *(European Commission Directorate General for Internal Market, Industry, Entrepreneurship and SMEs (GROW))*
Plovie Anca *(Nokia)*
Precsenyi Zoltàn *(Symantec)*
Preneel Bart *(Katholieke Universiteit Leuven)*
Purser Steve *(European Union Agency for Network and Information Security (ENISA))*
Razumas Valdemaras *(Lithuanian Academy of Science)*
Realmuto Mads *(UL)*
Reiser Helmut *(Leibniz-Supercomputing Centre & Ludwig-Maximilians University)*
Riesco Granadino Raúl *(Spanish National Institute for Cybersecurity)*
Riley-Smith Tristram *(Cambridge University / Partnership for Conflict, Crime & Security Research)*
Rouillec Gwenael *(Huawei France)*
Sample Char *(Carnegie Mellon University & University of Warwick)*
Savola Reijo *(VTT Technical Research Centre of Finland)*
Schulz-Kamm Eva *(NXP)*
Servida Andrea *(EC Directorate General for Communications Networks, Content & Technology (DG CONNECT))*
Shaikh Siraj Ahmed *(Coventry University)*
Shamir Adi *(Weizmann Institute)*
Socco Michele *(European Commission Directorate General for Migration and Home Affairs (DG HOME))*
Thomas Franck *(Eurosmart)*
Tschirhart Céline *(All European Academies)*
Urzay Basarrate Iñaki *(Panda Security)*
Vaitkevičienė Rita *(State Data Protection Inspectorate of the Republic of Lithuania)*
Van der Linden Geodele *(Marsh & McLennan Companies)*
van Zoonen Liesbet *(Erasmus University Rotterdam)*
Vandewalle Joos *(Katholieke Universiteit Leuven)*

Waidner Michael *(Technische Universität Darmstadt and Fraunhofer Institute for Secure Information Technology)*
Whalen Alexander *(Digital Europe)*
Žintelis Gintautas *(Lithuanian Academy of Science)*

Annex 6 - References

ABC4TRUST project: *ABC4Trust Attribute-based Credentials for Trust*. https://abc4trust.eu/

Acatech (Ed.) Position Paper. (2013). *Internet Privacy - Taking opportunities, assessing risks, building trust*. Heidelberg et al.: Springer Verlag 2013. http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Stellungnahmen/acatech_Internet_Privacy_Pos_eng_final.pdf

Acatech (Ed.) Study (2013). *Internet Privacy. Options for adequate realisation*, Heidelberg et al.: Springer Verlag 2013. http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Projektberichte/acatech_STUDY_Internet_Privacy_WEB.pdf

Association for Computing Machinery (ACM) - Europe Policy Committee. (2016). *Advancing Cybersecurity Research and Education in Europe - Cybersecurity Policy White Paper*. http://www.acm.org/binaries/content/assets/public-policy/2016_euacm_cybersecurity_white_paper.pdf

Alpár, G., & Jacobs, B. (2013). *Credential Design in Attribute-Based Identity Management*. In Bridging distances in technology and regulation, 3rd TILTing Perspectives Conference, pages 189–204.

Anderson, R. and Tyler Moore T. *The Economics of Information Security.* http://tylermoore.ens.utulsa.edu/science-econ.pdf. This review originally appeared in Science 314 (5799), pp.610–613, October 27, 2006.

Arpagian, N. (2016). *Digital identity : an asset for citizens, a target for criminals.* Presentation at the Cybersecurity in the European Digital Single Market workshop held on 25-26 October 2016, Vilnius, Lithuania. http://ec.europa.eu/research/sam/pdf/presentations/vilnius_2016/vilnius2016_nicolas_arpagian.pdf#view=fit&pagemode=none

http://ec.europa.eu/research/sam/pdf/presentations/vilnius_2016/vilnius2016_nicolas_arpagian.pdf#view=fit&pagemode=none

Bonneau, J.; Herley, C.; van Oorschot, P.C.; Stajano, F. (2015) *Passwords and the evolution of imperfect authentication.* Commun. ACM 58(7): 78-87. (2015) http://cacm.acm.org/magazines/2015/7/188731-passwords-and-the-evolution-of-imperfect-authentication/abstract

Broeders, D. (2017), *Opportunities, threats and issues in on line identity management*. Presentation at the Cybersecurity in the European Digital Single Market workshop held on 25-26 October 2016, Vilnius, Lithuania. http://ec.europa.eu/research/sam/pdf/presentations/vilnius_2016/vilnius2016_dennis_broeders.pdf#view=fit&pagemode=none

Camenisch, J & Lehmann, A. (2015). *(Un)linkable Pseudonyms for Governmental Databases.* CCS, October 12–16, 2015, Denver, Colorado, USA'15, 1467–1479. https://www.zurich.ibm.com/pdf/csc/pseudonyms_paper.pdf

Carr, M. (2016). *Public-private partnerships in national cyber-security strategies.* International Affairs, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Cash, D., Grubbs, P.,. Perry, J. & Ristenpart, T. (2015). Leakage-Abuse Attacks Against Searchable Encryption. Computer and Communications Security (CCS) '15 Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security , 668–679. https://doi.org/10.1145/2810103.2813700

Center for Long-Term Cybersecurity (CLTC). (2016). *Cybersecurity futures 2020*. Retrieved from https://cltc.berkeley.edu/scenarios/ https://cltc.berkeley.edu/files/2016/04/cltcReport_04-27-04a_pages.pdf

Choucri, N., Madnick, S., & Ferwerda, J. (2013). *Institutional Foundations for Cyber Security: International Responses and Global Imperatives, Information Technology for Development, 20:2, 96-121, DOI: 10.1080/02681102.2013.836699* https://doi.org/10.1080/02681102.2013.836699

Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* JOIN(2013) 1. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *Public-private partnerships in Horizon 2020: a powerful tool to deliver on innovation and growth in Europe.* COM(2013) 494. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0494&from=en

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *The European Agenda on Security*. COM(2015) 185. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0185&from=EN

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *A Digital Single Market Strategy for Europe.* COM(2015) 0192. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.* COM(2016) 410. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0410

Danezis, G., & Gürses, S. (2010). *A critical review of 10 years of Privacy Technology*. Surveill. Cult. A Glob. Surveill. Soc., 1–16. http://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 on *e-Privacy* amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&from=FR

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on *Combating The Sexual Abuse and Sexual Exploitation of Children and Child Pornography*, and replacing Council Framework Decision 2004/68/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on *Attacks Against Information Systems* and replacing Council Framework Decision 2005/222/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN

Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning *Measures for a High Common Level of Security of Network and Information Systems (NIS) across the Union*. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1

Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the *Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or The Execution of Criminal Penalties, and on the Free Movement of such Data*, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

ENISA European Union Agency for Network and Information Security. (2016). *ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity*. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption/view

ERCIM (2014) *White paper on Cyber-security and privacy research*. Version v0.91, Oct. 2014. https://www.ercim.eu/images/stories/pub/white-paper-STM.pdf

Ernst & Young Report. (2014). *Mitigating cyber risk for insurers*. http://www.ey.be/Publication/vwLUAssets/EY_-_Insights_into_cybersecurity_and_risk_(Part_2)/$FILE/ey-mitigating-cyber-risk-for-insurers.pdf

EUR-Lex. (2012). Charter of Fundamental Rights of the European Union 2012/C 326/02. *Official Journal of the European Union*, *55*, 391–407. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:FULL:EN:PDF

European Commission (2017). *EU cybersecurity initiatives working towards a more secure online environment.* http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

European Cybersecurity Industrial Leaders (ECIL). (2016). *European Cybersecurity Industry Leaders - Recommendations on Cybersecurity for Europe*. https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders

European Union Global Strategy (2016). *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy.* https://europa.eu/globalstrategy/sites/globalstrategy/files/regions/files/eugs_review_web.pdf

Gollmann, D. (2006). *Why Trust is Bad for Security.* Electronic Notes in Theoretical Computer Science, *157*(3), 3–9. https://doi.org/10.1016/j.entcs.2005.09.044

Hathaway, M. E. (2014). *Connected Choices : How the Internet Is Challenging Sovereign Decisions.* American Foreign Policy Interests, *36*(5), 300–313.

Hill, R. (2015). *Dealing with cyber security threats: International cooperation, ITU, and WCIT*. 7th International Conference on Cyber Conflict: Architectures in Cyberspace. https://doi.org/10.1109/CYCON.2015.7158473

Hoepman JH. (2014) *Privacy Design Strategies.* In: Cuppens-Boulahia N., Cuppens F., Jajodia S., Abou El Kalam A., Sans T. (eds) ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology, vol 428. Springer, Berlin, Heidelberg

Karlsson, F.; Kolkowska, E. & Prenkert, F. (2016). Inter-organisational information security: a systematic literature review. Information & Computer Security. 24 (5), 418-451.

Koning, M.; Korenhof, P.; Alpar, G. & Hoepman, J.-H. (2014). *The abc of abc: an analysis of attribute-based credentials in the light of data protection, privacy and identity.* In Privacy Enhancing Technologies Symposium 2014, Amsterdam, Netherlands. https://petsymposium.org/2014/papers/Koning.pdf

Lyon, D. (2007). *Surveillance Studies - An Overview*. Polity Press (4 juin 2007). http://www.sscqueens.org/publications/surveillance-studies-an-overview

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). *An integrative model of organizational trust.* Academy of Management Review, 20(3), 709–734.

Massachusetts Institute of Technology (MIT) (2015). *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications.* Computer Science and Artificial Intelligence Laboratory Technical Report. https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

Netherlands Presidency of the Council of the European Union. (2016). *Programme of the Netherlands Presidency of the Council of the European Union 1 January - 30 June 2016*. Retrieved from https://english.eu2016.nl/documents/publications/2016/01/07/programme-of-the-netherlands-presidency-of-the-council-of-the

Nissenbaum H. (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press. http://www.sup.org/books/title/?id=8862

Nye, J. S. (2014). *The Regime Complex for Managing Global Cyber Activities*. Global Commission of Internet Governance. CIGI Publications. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

Pawlak, P. (2016). *Capacity Building in Cyberspace as an Instrument of Foreign Policy.* Global Policy, *7*(1), 83–92.

Pawlak, P., & Wendling, C. (2013). *Trends in cyberspace: Can governments keep up?* Environment Systems and Decisions, 33(4), 536–543. https://doi.org/10.1007/s10669-013-9470-5

Picut, G. (2016). *La cybersécurité, le «bon choix» d'Emmanuel.* http://www.lemonde.fr/emploi/article/2016/04/12/la-cybersecurite-le-bon-choix-d-emmanuel_4900656_1698637.html

Ramirez, R., & Choucri, N. (2016). *Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review*. IEEE Access, 4, 2216–2243. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7437356

Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on *Electronic Identification and Trust Services for Electronic Transactions in the Internal Market* (eIDAS) and repealing Directive 1999/93/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the *Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, and repealing Directive 95/46/EC (General Data Protection Regulation). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Proposal for a Regulation of the European Parliament and of the Council *concerning the respect for private life and the protection of personal data in electronic communications* and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003 (COD). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

Sabouri, A., Krontiris, I., & Rannenberg, K. (2012). *Attribute-based credentials for trust (ABC4Trust).* In: Fischer-Hübner S., Katsikas S., Quirchmayr G. (eds) Trust, Privacy and Security in Digital Business. TrustBus 2012. Lecture Notes in Computer Science (LNCS) (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7449 vol 7449. Springer, Berlin, Heidelberg, 218–219. https://doi.org/10.1007/978-3-642-32287-7_21

Schneier, B., Seidel, K., & Vijayakumar, S. (2016). *A Worldwide Survey of Encryption Products*. Berkman Center Research Publication No. 2016-2. SSRN Electronic Journal, 2, 1–23. https://doi.org/10.2139/ssrn.2731160

Shackelford, Scott J.; Russell, Scott; and Kuehn, Andreas (2016). *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors.* Chicago Journal of International Law: Vol. 17: No. 1, Article 1. http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1700&context=cjil

Tziarras, Z. (2014). *The Security Culture of a Global and Multileveled Cyber Security.* In book: Cyber-Development, Cyber-Democracy and Cyber-Defense. Challenges, Opportunities and Implications for Theory, Policy and Practice, Chapter: 13, Publisher: Springer, Editors: Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos https://www.researchgate.net/publication/261986826_The_Security_Culture_of_a_Global_and_Multileveled_Cyber_Security

UK Royal Society. 2016. *Progress and Research in Cybersecurity. Supporting a Resilient and Trustworthy System for the UK*. https://royalsociety.org/~/media/policy/projects/cybersecurity-research/cybersecurity-research-report.pdf

UK Government Office for Science (2016) *Distributed Ledger Technology: beyond block chain.* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

U.S. National Academy of Sciences (2014) *At the Nexus of Cybersecurity and Public Policy - Some Basic Concepts and Issues.* Clark, D.; Berson, T. & Lin, H.S., Editors. The National Academies Press, Washington DC. https://www.nap.edu/read/18749/chapter/1

van Zoonen, L. (2013). *From identity to identification: fixating the fragmented self.* Media, Culture & Society, 35, 44–51. https://doi.org/10.1177/0163443712464557

van Zoonen, L. (2016). *Identity: online and offline.* Presentation at the Cybersecurity in the European Digital Single Market workshop held on 25-26 October 2016, Vilnius, Lithuania. http://ec.europa.eu/research/sam/pdf/presentations/vilnius_2016/vilnius2016_liesbet_van_zoonen.pdf#view=fit&pagemode=none

World Economic Forum (2016). *The Global Risks Report 11th edition*. http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf

Annex 7 – Glossary

Attacks	A web application attack consists of feeding vulnerable servers and/or mobile apps with malicious input or unexpected sequences of events. The objective is to inject malicious code, alter site content or breach information.
Attribute	Small pieces of information that make up a digital identity. Attributes may include name, phone number, group affiliation, etc.
Attribute-based authentication	Attribute-based authentication aims to provide a mechanism for precisely doing this: allowing transactions on the basis of those attributes which are required for the transaction. The main advantages are: • it is privacy-friendly, in the sense that it is based on the idea of data minimisation and that it provides unlinkability among user transactions; • it offers protection against identity fraud: if one's identity is not involved in a transaction,• it cannot be stolen; • it provides a new, more flexible approach in identity management and authentication, in particular, an approach that is based on attributes instead of unique identities.
Authentication	Electronic authentication is the process of confirming a person/entity's identity.
Backdoor	A backdoor is a type of malicious code that, once installed on a system, allows attackers to bypass normal security access controls and access the system. A backdoor is a method, often secret, of bypassing normal authentication in a product, computer system, cryptosystem or algorithm etc. Backdoors are often used for securing unauthorized remote access to a computer, or obtaining access to plaintext in cryptographic systems.
Block chain	A block chain is a type of database that takes a number of records and puts them in a block (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions.

Cloud computing	Model for enabling convenient on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Users do not need to invest in their own infrastructures. Storage and processing takes place in the cloud rather than at the user's premises or on the user's devices. Cloud services can rapidly scale up or down according to demand, giving the "illusion of unlimited resources". Computing becomes an operating, rather than a capital expenditure item.
Computer Emergency Response Team (CERT)	A service organisation that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental or educational organisation, a region or country, a research network or a paid client.
Cybersecurity	Cyber security commonly refers to the safeguards and actions available to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. The term cyber security also covers prevention and law enforcement measures to fight cybercrime.
Cryptography	The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable.
Data confidentiality	The protection of communications or stored data against interception and reading by unauthorized persons.
Data integrity	The confirmation that data which has been sent, received, or stored are complete and unchanged.

Data protection and privacy	Data protection refers to personal data, gathered and processed in a safe and secure manner. Legal provisions are laid down in EU legislation (95/46/EC Directive and 2002/58/EC Directive as amended in 2009). New DP legislation is under consideration by European Parliament and Council. Privacy is the prerogative of indviduals to be left alone, out of public view, and in control of the collection and sharing of information about themselves (informational privacy). For the FP7 PRESCIENT project (http://www.prescient-project.eu/prescient/index.php), the research consortium has identified seven types of privacy: of a person, of thought and feelings, of location and space, of data and image, of behaviour and action, of communications, and of association, including group privacy. The concepts of data protection and privacy therefore overlap, but do not coincide.The right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12), the EU Charter of Fundamental Rights (art 7,8) as well as in the European Convention of Human Rights (Article 8).
Data subject	The data subject is the person whose personal data are collected, held or processed.
Digital Identity	A digital identity is a set of information (attributes and credentials) about an individual that is maintained in order to associate them with an organization.
Digital Single Market	The Digital Single Market could be defined operationally as "an area where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, irrespective of their nationality or place of residence." The notion of Digital Single Market does not represent a new concept outside the traditional concepts of the Treaties. It primarily reflects new developments and the "reality" of the Single Market that is undergoing digital transformation. The overall objective should be a "single market ready for the digital age", where the free movement of goods, persons, services and capital is enhanced by digital technologies.
Distributed Ledgers	Distributed ledgers are a type of database that is spread across multiple sites, countries or institutions, and is typically public. Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when the participants reach a quorum.

DDoS (Distributed Denial of Service) attack	A type of attack used to prevent legitimate users from accessing online services or resources. Typically, a network is brought down by flooding it with traffic so legitimate traffic cannot pass through.
Electronic Identity Card (e-ID)	The electronic identity card (eID) is an official electronic proof of one's identity. It also enables the possibility to sign electronic documents with a legal signature.
e-commerce (electronic commerce)	Generic term used to describe trade over the internet. The activities concerned include selling goods online, offering online information or commercial communications, providing tools allowing for search of products and services, access and retrieval of data.
Egovernment	Use of ICT tools and systems to provide better public services to citizens and businesses. ICTs are already widely used by government bodies and businesses. eGovernment means much more than just the ICT tools; effective eGovernment also involves rethinking organisations and processes and changing behaviour so that public services are delivered more efficiently to the people who need to use them. Implemented well, eGovernment allows citizens, businesses and organisations to carry out their business with government more easily, quickly and at lower cost.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text ; encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.
Formal verification	In the context of hardware and software systems, formal verification is the act of proving or disproving the correctness of intended algorithms underlying a system with respect to a certain formal specification or property, using formal methods of mathematics. Formal verification can be helpful in proving the correctness of systems such as: cryptographic protocols, combinational circuits, digital circuits with internal memory, and software expressed as source code.
Identity Federation	A setting where a federation is a trusted broker between identity providers (e.g. campus, research institutions) and content providers (e.g. publishers, software vendors, web services) and ensures the legal and secure exchange of attributes between parties.
Identity Management (IdM/IM)	Identity Management is the act of using processes and solutions for the creation and management of user or connected device information.

Information Technology (IT)	**Technology components (computer systems, networks, applications, telecommunications, technical support and service desk).**
Internet of Things	"The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."
Meta data	Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information.
Patches	A type of programming code that is used to repair an identified software bug or vulnerability. Other definition:A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities[1] and other bugs, with such patches usually called bugfixes or bug fixes, and improving the usability or performance.
Personal data	Any information relating to an identified or identifiable natural person, or "data subject".(Source: GDPR Article 4)
Risk	The potential that a given threat will exploit vulnerabilities of an asset [G.3] or group of assets and thereby cause harm to the organization.
Security	All aspects related to defining, achieving, and maintaining data confidentiality, integrity, availability, accountability, authenticity, and reliability. A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way.
Threat	Any circumstance or event with the potential to adversely impact an asset [G.3] through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
Vulnerability	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event [G.11] compromising the security of the computer system, network, application, or protocol involved.
Zero-day exploit	A zero-day exploit is defined as a software or hardware vulnerability that has been exploited by an attacker and of whose existence the general information security community remains ignorant. As a result, no patch or fix is available to defend against it.

Annex 8 - List of acronyms and abbreviations

ACATEC	German National Academy of Science and Engineering
ACM	Association for Computing Machinery
CERT	Computer Emergency Response Team – European Union
CLTC	Center for Long-Term Cybersecurity
CSIRT	Computer Security Incident Response Team
DdoS	Distributed Denial of Service
DG CNECT	European Commission Directorate General for Communications Networks, Content & Technology
DG GROW	European Commission Directorate General for Internal Market, Industry, Entrepreneurship and SMEs
DG HOME	European Commission Directorate General for Migration and Home Affairs
DG JRC	European Commission's Joint Research Centre Directorate-General
DG RTD	European Commission Directorate General for Research and Innovation
DSM	Digital Single Market
e-commerce	Electronic commerce
e-ID	Electronic Identity Card
eIDAS	The Regulation on the Electronic Identification and Trust Services for Electronic Transactions in the Internal Market
ENISA	European Union Agency for Network and Information Security
ERCIM	European Research Consortium in Informatics and Mathematics
EU	European Union
Europol	European Union's law enforcement agency
GDPR	General Data Protection Regulation
H2020	Horizon 2020 Research and Innovation Framework Programme
SAM HLG	Scientific Advice Mechanism - High Level Group
ICT	Information and Communication Technologies
ID	Identity
IdM/IM	Identity Management

IoT	Internet of Things
IP	Internet Protocol
IRMA	I Reveal My Attributes
IT	Information Technology
MIT	Massachusetts Institute of Technology
MS	Member States
NIS	Directive on Networks and Information Security
OS	Open Source
PKI	Public Key Infrastructure
PPP	Public-Private Partnership
SAM	Scientific Advice Mechanism
SAPEA[55]	Science Advice for Policy by European Academies
SWOT	Strengths, Weaknesses, Opportunities and Threats
TTP	Trusted Third Parties

[55] The SAPEA consortium is comprised of Academia Europaea (AE), All European Academies (ALLEA), the European Academies Science Advisory Council (EASAC), the European Council of Academies of Applied Sciences, Technologies and Engineering (Euro-CASE) and the Federation of European Academies of Medicine (FEAM).

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

This Scientific Opinion responds to a request from European Commission Vice President Andrus Ansip for scientific advice on cybersecurity in the EU in the context of the European Digital Single Market.

The advice in this Scientific Opinion is based on analysis of publicly-available scientific literature as well as extensive consultation with the scientific community. The High Level Group also bases its advice on relevant principles in the Charter of Fundamental Rights of the European Union and others which are particularly pertinent to cybersecurity policy including transparency, duty-of-care towards customers and shared responsibility.

The advice takes the form of ten recommendations and a number of observations.

The first few recommendations deal with technical matters such as cryptography, backdoors, vulnerabilities and the importance of a systems approach. Others deal with contextual identity, user choice and engaging citizens thereby giving the advice a strong citizen-centred character. The remainder deal with training professionals, industry, evidence collection and sharing, and cybersecurity governance, thus the advice also addresses economic and strategic issues. The observations – issues pertinent to cybersecurity policy but on which there was no clear expert consensus - highlight the complex nature of cybersecurity from a scientific perspective, the delay between EU legislation conception and implementation and the corresponding lead-time and the rate of evolution of the threat landscape, as well as some other tensions.

This Scientific Opinion was adopted by the SAM HLG at its 7th meeting on 24 March 2017 and submitted to the European Commission. It will inform the revision of the EU's Cybersecurity Strategy and the further development of the Digital Single Market strategy.

Studies and reports

Publications Office