Scientific Advice Mechanism

Scoping Paper:
Cybersecurity

29 January, 2016
(Revised)

Rev. Date:01/03/2016

1. The case for cybersecurity

Cybersecurity refers to the protection of networks and information systems against human mistakes, natural disasters, technical failures or malicious attacks[1]. Not only is the notion of cybersecurity complex, relating to the protection of *systems and humans*, it is also closely connected to fundamental rights and values: security, protection of data privacy, freedom of expression, protection from crime, defence and international peace.

As digital technologies become more used in economic, social and governance matters, cyber-attacks become a bigger challenge for companies, states and individuals[2]. With the fast continuing evolution of information and communication technologies (ICT), the cybersecurity challenge will grow in importance. As ICT becomes integrated to almost every facet of modern society, enormous opportunities for innovation are created**.** ICT enables new solutions to major societal challenges and drives economic growth. Cybersecurity is part of a much broader transformation across society driven by information and communication technologies, where "digital hyper connectivity" refers to the increasing or exponential rate at which people, processes and things are connecting to the Internet.

In addition, cyber incidents and attacks can disrupt the supply of essential services for our societies, since digital technologies are complex and underpin other systems and services, like finance, health, energy, transport. Providing security to our citizens is a common European responsibility. This increasingly becomes also a question of cybersecurity.

While unleashing creativity and innovation, this ICT-enabled societal transformation could further expose the vulnerability of our digital systems, making also the physical world more vulnerable to new threats. In other words, as the digital cyber space and the physical space come closer, risks and threats in the cyber space may increasingly affect physical space and individuals' livelihoods.

Trust is fundamental for social cooperation and economic growth. But trust will be depleted if the security of the cyber space is weak – or perceived as weak by the users –turning people away from new technologies, or limiting their role[3]. In this sense, how Europe responds to cybersecurity can be a critical factor to enable (or discourage) social-economic transformations of a digital age.

2. Main issues of the debate

Technological systems and people-based 'systems' usually interact closely. Disruption of one may affect many others, often in unexpected ways, which suggests comparisons between

[1] A definition used in the EU Cybersecurity Strategy of 2013 is: "Cyber-security commonly refers to 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. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."

[2] A cyber-attack happens every minute somewhere in the world. More than 150,000 viruses and other types of malicious code are in circulation. At least a million people are victims of cybercrime daily, although many attacks go unnoticed. Attacks against companies can generate many millions in costs, additionally to market loss and reputational damage (Sony Pictures, Talk Talk). Moreover, attacks in cyberspace can have significant effects in physical space, e.g. on national security and the livelihood and safety of individual citizens. The global cybersecurity market is growing fast (near $66 billion in 2013, expected to grow to $80-120 billion in 2018.)

[3] Taking this into account the EUROBAROMETER results are quite indicative of the need for action: 85% of internet users feel that the risk of becoming victim of cybercrime increases and 73% feel that online personal information is not kept secure.

such an interconnected environment and dynamic and complex systems. In such an environment, cybersecurity can be viewed from different perspectives:

- the **economic** side, where costs of cyber incidents and attacks, current and future (due to reputational damage for companies, failing trust of individuals), co-exist with new market opportunities for European companies.
- the **security** side, that relates on the one hand to **cybercrime**[4] and on the other to **cyber defence;** it covers incitement of radicalism and terrorist acts, national and internal (EU) security, international peace aspects
- the ethics side, that focuses on **citizens' rights**, and is mainly concerned with personal data protection, privacy, and freedom of expression rights.

In addition, as more industries, including traditional ones, become more automated and connected to the digital world, policies on cybersecurity will affect their operations and their competitiveness in the global market.

It is in this context that the Digital Single Market, one of the main priorities of the European Commission, 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[5]. This means making much better use of the opportunities offered by digital technologies which know no borders.

While distinguished in the starting point and perspective, and in the main EU policies concerned (Digital Agenda, Home Affairs, Foreign Affairs and Security Policy), there is a common underlying problematic in the different views on cybersecurity described above: as the world becomes more digitalized – from the level of the experience of the individual, to national states and international governance - new challenges for citizens, companies, institutions and the internal security of EU as a whole arise. These go hand in hand with maintaining citizens' trust in a society and an economy that increasingly use – and are transformed by - digital technologies.

Viewing cybersecurity from different sides can lead to different conclusions, which makes it inherently more difficult. For example, good cybersecurity can help protect **privacy** in an electronic environment, but information that is shared to assist in security efforts, including cybersecurity, might sometimes contain personal information that at least some observers would regard as private. Cybersecurity can be a means of protecting against **undesired surveillance** of and gathering of intelligence from an information system. However, when aimed at potential sources of criminality, such activities can also be useful to help effect (cyber)security. In addition, surveillance in the form of monitoring of information flow within a system can be an important component of cybersecurity.

Reducing cyber risks usually involves removing threat sources, addressing vulnerabilities, and lessening impacts[6]. The **management of risk** to information systems is considered fundamental to effective cyber security.

The ***threats*** include corporate espionage, criminality, government driven attacks and surveillance, terrorism, hacktivism, and disgruntling. Basically anyone can be a well-equipped threat source nowadays. There are many possible ***vulnerabilities*** in such systems, stemming from accidents or poor practice and involving not only technology but also processes and people. The ***values*** at risk are assets and reputation, where the former may

[4] Cybercrime consists of criminal acts that are committed online by using electronic communication networks and information systems (crimes specific to the internet, online fraud and forgery, illegal online content, incitement to racism and terrorist acts)

[5] https://ec.europa.eu/priorities/digital-single-market_en

[6] Cybersecurity Issues and Challenges: In Brief Eric A. Fischer, December 16, 2014, Congressional Research Service ; https://www.fas.org/sgp/crs/misc/R43831.pdf

reach a few billion euros, and, ultimately, human lives. The specific risks associated with any attack, beyond loss of values, depend largely on the threats, vulnerabilities and values.

The current ***responses*** may be classified into three categories, namely the traditional (e.g. policies and regulations), the communitarian (e.g. governance, information sharing, mutual aid, coordinated actions), and the systemic (e.g. risk markets and embedded security).

In developing a scientific approach to the cybersecurity challenge with a view to inform policy making at EU level, the following observations should be taken into account:

Cybersecurity is not an isolated issue and cannot be tackled in isolation. Cybersecurity is part of a much broader transformation across society, driven by information and communication technologies towards "digital hyper-connectivity". This results in some key shifts:

- the impact of technology shifts from improving work-efficiency to enabling transformation of business operations and institutions;
- the structure of systems changes fundamentally, away from hierarchies towards networks;
- disintermediation offers huge social and economic gains, but presents new governance and assurance challenges.

Cybersecurity is not a single issue. When referring to cybersecurity, it is easy to assume that a single topic or issue is meant. However, this term refers to a set of issues that are as varied as they are distinct. A single Internet may connect all people, but the challenges abound. In the physical world, retail fraud, organized crime, invasions of personal privacy, diplomacy, warfare, intellectual property and copyright violations, terrorism and activism happen in very different ways, and different governance mechanisms (such as institutions, treaties, regulations and market mechanisms) have evolved to deal with each of them. Of course, part of the challenge of the cyber world is that these mechanisms in their current form are not reliable. Designed in a pre-digital world, they move too slowly and ignore the digital age's interdependencies. Indeed, in many cases, even the underlying values and concepts cannot be depended upon – the digital era has re-constituted ideas such as privacy, ownership and security. For instance, the common notion of security implies isolation, the protection of a defined perimeter or an objective defined by the prevention of an event. This notion of security seems quaint in a world where it is impossible to draw a clean ring around the network of one country or one company, and where large organizations can be the target of 10.000 cyberattacks per day.

The major challenges are likely to be reshaped in the near future. Game changing computer and communication technologies bring new opportunities for the European market, but also new challenges in the field of cybersecurity. Distributed ledger technologies that are based on blockchain may become widespread in public services, such as for collecting taxes, delivering benefits, issuing passports, record land registries, and generally ensuring the integrity of government records and services[7]. The Internet of Things and Cloud technology are already in the market, but they raise the risk of easy dissemination of security issues. Blockchains could be subject to new viruses and hacking methods, especially given advances in quantum computing.

[7] See Distributed Ledger Technology: beyond block chain;Report by the UK Government Chief Scientific Adviser https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Encryption would also need to be placed within this future context, since it is a prerequisite for electronic identification schemes. In particular, encryption is necessary for key features of ICT services, such as guaranteeing authentication, integrity, and confidentiality. Encryption is therefore a major issue in the construction of a trustworthy cyberspace, which is impacted by new trends, as for instance: the Internet of Things may require more compact and efficient encryption; without encryption, data in the cloud remains fragile and a target for hackers and criminals; and quantum computers pose new challenges by their potential to break existing encryption algorithms, including those used by blockchain.

Cybersecurity is a socio-economic issue. The internet environment is a socio-technical system, where the human is usually considered as its weakest link. Furthermore, from the digitally enabled car to smart cities, from energy infrastructure to air travel, from cashless banking to on-the-spot market prices for farmers in developing economies, humankind is witnessing an explosion of innovation in services intermediated by ICT. This groundswell of creativity is occurring across industries everywhere and the phenomenon has massive potential to generate economic value, given that many of its gains in recent years have derived directly from digital global connectivity. Thus, cyber risks incur lost opportunities from a significant backlash or fragmentation of the current digital ecosystem. A backlash could result from a single major event, or through gradual erosion. Governments, businesses or individuals could cause it. Fragmentation could occur intentionally, as loss of trust leads to explicitly isolationist policies. Or it could occur semi-intentionally, as governments adopt increasingly protectionist stances on digitally enabled services. Or it could occur unintentionally, as uncoordinated policy developments in different jurisdictions result in a disparate set of requirements to operate globally.

Cybersecurity is also an ethical issue. There are many ways in which cybersecurity relates to rights, harms, and interests and, hence, to ethics. These include the moral importance of cybersecurity, the relation between cybersecurity and national security, the morality of hacking and computer crime, the nature of cyberterrorism and information warfare, the moral responsibilities of law enforcers, cybersecurity researchers, and information security professionals, the moral importance of privacy, and the impact of information technology on it.

3. The EU policy landscape on cybersecurity

At EU level cybersecurity is mainly addressed under the Digital Single Market, Home Affairs policy and Foreign Affairs and Security policy. There is coordination across the Commission through an inter-service group (chaired by the Directorate Generals for Communications Networks, Content and Technology (DG CNECT), Home Affairs (DG HOME) and the European External Action Service(EEAS). DG HOME is responsible for the fight against cyber-crime. While DG CNECT has the lead on cybersecurity, DG HOME retains also an interest in the cyber-security of critical infrastructure[8].

The Joint Research Centre (JRC) is involved in cybersecurity research (see https://ec.europa.eu/jrc/en/research-topic/cyber security)

For a review of current policies and initiatives see *EU cybersecurity initiatives: working towards a more secure online environment*, and the *Factsheet* https://ec.europa.eu/digital-agenda/en/node/80942.

In summary, the main elements are:

[8] See:https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.

- **EU – Policies and legislation:**
  - The **Directive on attacks on Information systems** (2013) [now in force]. Since end 2015 to have been transposed to member states national legislation and implemented (cooperation of law enforcement authorities of MS where attacks to ICT can be criminal acts). It is 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 **Cybersecurity strategy (JOIN(2013) 1)**[9]
  - The **Directive on combatting sexual exploitation of children online** (2011)
  - The **Directive on Networks and Information Security (NIS)** recently agreed at political level aims to increase preparedness at the national level and strengthen cooperation between member states at strategic and operational level. It requires companies and organisations in critical sectors – such as energy, transport, banking and health – to adopt risk management practices and report major incidents to their national authorities promoting cross-border cooperation inside the EU. The Directive will also create a network of Computer Security Incident Response Teams, known as the CSIRTs Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks.
  - **The Regulation on the Electronic Identification and Trust Services (eIDAS)** that 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**, 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).
- **EU - networks and agencies:**
  - **EC3 European cybercrime Centre** (2013) as part of EUROPOL: for the fight against cybercrime, pooling cybercrime expertise to support MS
  - **ENISA (European Network and Information Security Agency),** support good practice exchange between MS
  - **EDA (European Defence Agency)** for cyber defence

[9] Joint Communication to The European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

- **Network and Information Security (NIS) platform** to identify best practices, develop incentives to adopt secure solutions, and propose a Strategic Research Agenda for Secure ICT
- **EASA (European Aviation Safety Agency)** for cybersecurity in aviation[10]

- **EU academies and scientific organizations**

The topic of cybersecurity has recently been addressed by the scientific community through a number of activities and publications, including:

Euro-CASE organizing a Round Table on the theme of "Digital Privacy: Citizen Rights in the Light of New Technologies, Commercial needs", together with the JRC in Brussels on 28.01.2015.[11]

EASAC underlining that addressing issues such as cybersecurity require closer cooperation between sciences and humanities (http://www.easac.eu/home/easac-news/detail-view/article/letter-of-th.html)

ERCIM White paper on cybersecurity 2014 (http://www.ercim.eu/images/stories/pub/white-paper-STM.pdf)

Awareness raising campaigns and broader dissemination

European Cybersecurity Month (ECSM) is an EU advocacy campaign that promotes cybersecurity among citizens (https://cybersecuritymonth.eu/)

Cybersecurity challenge Belgium https://www.cybersecuritychallenge.be/

Scientific American (http://www.scientificamerican.com/article/how-cybersecurity-became-your-problem/)

The cybersecurity strategy (JOIN(2013) 1) has put forward that, in cooperation with the Member States, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy will **work towards a coherent EU International cyberspace policy -** aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and private sector.

Some specific actions that are planned under EU policies covering cybersecurity from its different sides for 2016 include:

- Review of applicable legal framework for specific offenses (fraud, counterfeiting of non-cash payments) analysis of obstacles to criminal investigations of cybercrime, (better law enforcement) and enhancing the cyber capacity building actions under external assistance instruments.

- Review of ePrivacy directive – 2016 (after the data protection one)

- Partnership with the industry cPPP[12] (to launch in June 2016), currently under public consultation, for a strategic research and innovation agenda to build industrial competitiveness in Europe.

[10] https://easa.europa.eu/newsroom-and-events/events/conference-cyber-security-aviation
[11] http://www.euro-case.org/index.php/events/item/638-jrc-euro-case-round-table-on-the-theme-of-digital-privacy-citizen-rights-in-the-light-of-new-technologies-commercial-needs-brussels-28012015.html

Furthermore, in June 2016 it is planned to announce the new EU global strategy for Foreign and Security policy– that will provide a blueprint for instruments and capabilities development.

4. Areas and topics for scientific advice to inform policy making

The following questions have relevance to European policy in the next few years. The advice of the HLG could inform immediate actions (e.g. the ePrivacy Directive and the Cybersecurity cPPP), as well as provisionally a forthcoming European strategy. Some first reflections of the HLG in spring 2016 could be informative to actions foreseen in the near future (summer 2016), while the HLG's scientific advice in the second semester of 2016 could be of relevance to longer term policy development.

Science can cast new light on the question of future developments and technologies for which Europe needs to be ready, and where European policies can play an important role in preparing the market and citizens. How can Europe prepare the market for new information and communication technologies, without limiting them but ensuring overall security? What does scientific evidence tell us about the main challenges for the future, in public services as well as in private industry (e-health, self-driving cars etc). In particular, the following dimensions could benefit from scientific advice:

- **Trust in transactions intermediated by ICT**

Encryption of electronic data is an indispensable component of the socio-economic environment[13] (e.g. in fostering creativity, Internet services, and protection of IPR). Encryption can secure data in transit on the network, data at rest on a device or in the cloud, and, in a limited way, data during computations. Besides securing data and authorising users on the network, encryption makes possible the use of electronic identity (eID) to authenticate the data source, to digitally sign a document, and to safeguard the integrity of data and documents, thereby increasing trust in digital transactions. Note that law enforcement authorities need to be in a position to get lawful access to communications or specific information, an objective that in some instances may be rendered more difficult or even unattainable because of strong encryption.

Clearly the question of trust in transactions intermediated by ICT has many sides. Measures to increase trust may also increase surveillance or impose additional burden to increasingly more digitalised industries. What is the scientific evidence on the effectiveness of existing approaches and their implications for protecting citizens (use of "back doors" for example)? What are the real risks of digital identities? Is there scientific evidence that encryption of electronic data is detrimental to lawful investigations? If so, how to reconcile these divergent requirements? Are confidentiality and integrity of encrypted data safe against new and emerging technologies? Can eID thrive in case data are not encrypted?[14]

- **Evidence for analysis and informed policy-making**

[12] https://ec.europa.eu/digital-agenda/en/news/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures

[13] Report on encryption, anonymity, and the human rights framework, Report of the Special Rapporteur of The Office of the United Nations High Commissioner for Human Rights (OHCHR) on freedom of expression, David Kaye. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

[14] Read also Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, MIT Computer Science and Artificial Intelligence Laboratory Technical Report MIT-CSAIL-TR-2015-026, July 6, 2015. http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8

Cybersecurity is ill-defined, rapidly changing, influenced by powerful forces such as rapid technological change (cf Blockchain) and complex dependencies (viz the fear of a Black Swan incident). Moreover, it is playing out partly in situations that are hard to investigate (ranging from company-internal ways of working, to criminal activities, to national security). Are new approaches needed to collect and assess evidence for analysis and informed policy-making in cybersecurity? Drawing on the state of the art in science and innovations in this field, where should Europe focus its efforts?

- **Multidimensionality, risk management and a science of cybersecurity**

Scientific advice is required for a better understanding of risks and their management in an ICT-enabled society (drawing on science to better manage cyber risks). What main insights from different sciences can inform cybersecurity issues and how can a robust multidisciplinary approach be taken further to support sound cyber risk management and a science of cybersecurity?

- **Risk of isolated approaches**

With the growing importance of cybersecurity in different areas, each sector is creating its own bespoke systems, e.g. Airlines with IASA, Financial services, Government (led by Estonia), Energy, Health, Defence, or the cars industry. This will lead to an increased probability of failure (due to attacks or otherwise) and may lead to non-interoperability. There are also impacts of new technologies which must be taken into account and which must also be prepared for. What kind of solutions will be implementable across sectors, to prevent fragmentation, lack of interoperability and increased vulnerability?

Cybersecurity is a problem that cannot be fixed quickly or easily. Rather, many partial solutions and potentials paths forward exist and will need to be implemented, which will require collaboration, collective action, and—most of all—determination
(Cybersecurity Dilemmas: Technology, Policy, and Incentives: Summary of Discussions at the 2014 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum (2015), National Academies press)