I. ICT Security issues affecting EU/US ICT development collaboration

Final v1.0

Policy Briefing 2

Author: Dave Farber, Maarten Botterman, Jonathan Cave, *GNKS Consult BV*

ICT Policy, Research and Innovation for a Smart Society

May 2017

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

Disclaimer

This document is provided with no warranties whatsoever, including any warranty of merchantability, non-infringement, fitness for any particular purpose, or any other warranty with respect to any information, result, proposal, specification or sample contained or referred to herein. Any liability, including liability for infringement of any proprietary rights, regarding the use of this document or any information contained herein is disclaimed. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by or in connection with this document. This document is subject to change without notice.

PICASSO has been financed with support from the European Commission.

PICASSO brings together prominent specialists willing to contribute to enhancement of EU-US ICT collaboration. PICASSO does not represent EU or US policy makers, and the views put forward do not necessarily represent the official view of the European Commission or US Government on the subject. PICASSO cannot be held responsible for any use which may be made of information generated. This document reflects only the view of the author(s) and the European Commission cannot be held responsible for any use which may be made of the information contained herein.

Foreword

On January 1st, 2016, the project PICASSO was launched with two aims: (1) to reinforce EU-US collaboration in ICT research and innovation focusing on pre-competitive research in key enabling technologies related to societal challenges - 5G Networks, Big Data and the Internet of Things/Cyber Physical Systems; and (2) to support EU-US ICT policy dialogue related to these domains with contributions related to e.g. privacy, security, internet governance, interoperability and ethics.

PICASSO is aligned with industrial perspectives and provides a forum for ICT communities. It is built around a group of 24 EU and US specialists, organised into the three technology-oriented ICT Expert Groups and an ICT Policy Expert Group, working closely together to identify policy gaps in or related to the technology domains and to recommend measures to stimulate policy dialogue. The Policy Expert Group we are chairing also includes Jonathan Cave, Avri Doria, Ilkka Lakaniemi and Robert Pepper, and develops its insights in consultation with other specific experts in the field (depending on the topic).

This policy paper focuses on ICT security policy considerations in the EU and the US that affect and are affected by in particular ICT development collaboration related to 5G Networks, Big Data, and Internet of Things/Cyber Physical Systems. The content reflects the results of desk study and subsequent discussion of the resulting draft Briefing Paper during a PICASSO Webinar on 16 May 2017 (see http://www.picasso-project.eu/).

A Policy Paper on Privacy & Data Protection has already been published. Future subjects for Policy Papers will be Standardisation; Spectrum; and one yet to be decided – provisionally on “Smart Cities”, a subject in which all other issues come together. Intent is to provide a clear overview of the most pressing and/or challenging policy issues that confront technological, business and policy collaborations and to develop valid and practical insights into how they can be addressed from a transatlantic multistakeholder perspective operating in a global context.

Our thanks go out to all those who contributed to our understanding of the issues related to ICT security policies in the EU and the US and of the specific policy issues related to the three PICASSO domains by their active participation in our meetings. We could not have done this without them.

Please feel free to share your thoughts via email to maarten@gnksconsult.com.
Looking forward to engaging with you all,

Best regards

Maarten Botterman
Chairman Policy Expert Group
PICASSO project

Dave Farber
Co-Chair Policy Expert Group
PICASSO project

Executive Summary

On January 1st, 2016, the project PICASSO was launched with two aims: (1) to reinforce EU-US ICT research and innovation collaboration, especially pre-competitive research in key enabling technologies related to societal challenges - 5G Networks, Big Data and the Internet of Things/Cyber Physical Systems; and (2) to support EU-US ICT policy dialogue related to these domains with contributions related to e.g. privacy, security, internet governance, interoperability and ethics.

This policy paper focuses on cybersecurity policy considerations in the EU and the US that particularly affect and are affected by ICT Research and Innovation (R&I) collaboration related to 5G Networks, Big Data, and Internet of Things/Cyber Physical Systems.

Cybersecurity is high on the agenda of policy makers throughout the world. The growing incidence of adverse and highly-publicised events, including massive distributed denial of service attacks on the Internet (e.g. the Dyn attack in 2016), malware (e.g. the WannaCry Ransomware attack in 2017), hacking, and unauthorized penetration of critical services and sensitive data (including the many breaches of customer data at Yahoo and other organisations over the years) has seriously disrupted networks and compromised privacy and national information security.

There is no magic cure for the serious security issues that that have become endemic throughout the underlying infrastructures and services that have become so fundamental to the way we communicate, access information, and interact. Even more so: each 'cure' sets the stage for the next set of issues. Network security is not confined to the technical layer, but spreads to all layers and beyond to the user community. Progress made in one domain can be undermined by contagion or reinfection from others. The challenges are global and need to be addressed head-on by all stakeholders; governments who have the monopoly on the coercive power of the law, end users who must act knowledgeably and responsibly, ICT developers who are responsible both for security 'by design' and for critical vulnerabilities and businesses using and/or deploying ICT and ICT-based or –enhanced services in more or less responsible ways. A proper balance between responsible action by individual entities and collaboration among stakeholders is essential for sustainable progress.

In this paper we will first describe the current technical situation, to provide a framing perspective on todays' vulnerabilities of communication and IT systems and the worldwide Internet. Technical complexity is one aspect, deriving in part from the fact that the Internet is a network of mostly interoperable networks of varying robustness and resilience. But this is not a matter of design alone; the continuing evolution of ICT networks and systems – and of uses and users - means that old systems, code, devices and architectures will remain, interacting with their newer counterparts. Both opportunities and incentives for maintenance of this complexity are limited, and in some cases impossible. 5G networks will certainly need to deal with current vulnerabilities and at the same time to contribute to availability of more secure systems. Protection of data against destructive and insecure use and securing the utility and integrity of data depends on the ability of systems to recognise identities and protect against sniffing and access by those who should not have access and to detect and limit inappropriate use of data by those allowed access. IoT/CPS also has to address a wide range of vulnerabilities of varying criticality. [section 1]

Secondly, we describe the socio-economic-political situation and its interaction with cybersecurity. It may be clear that specific actors may step up their efforts to reduce the risk of security breaches when vulnerabilities become their clear responsibilities. Again, there are clear specific aspects reflecting the three Picasso domains. 5G networks will greatly influence mobility and offer additional forms of connectivity with different security challenges than IP networks. With (Big) Data, specificities that heighten the stakes include: concepts like data ownership, governance and value; ; the increasing significance of the algorithms that operate on (and shape) data flows; and the growing tension with value of data "in the public interest" and value of data to individual actors. With regards to IoT/CPS, specific challenges arise from the gaps between the potential, intended and actual application of "things" and systems – today there are many "unintended consequences" resulting from innovation and ways we use the technologies and services available. Many current vulnerabilities relate to commercial competition based more on competing on 'features' and minimising time-to-market rather than enhancing "robustness of systems". Many people (both customers and suppliers) consider ICT devices as gadgets even as more and more aspects of their lives depend on their reliable and secure functioning; in any case, robustness, risk and resilience of such technologies and systems are still poorly understood. [section 2]

After that we focus on new developments likely to affect the security and vulnerability of ICT systems and the information ecosystem as a whole. We find that new legislation raises the stakes for businesses and seems to seek to provide incentives for improved security by raising the severity of penalties for system failures (i.e. accountability of suppliers of ICT tools and services). But we also see further globalisation of ICT driven markets and value chains, which could open up possibilities for new forms of standards setting and certification. [This will be the focus of our next policy paper]. This section goes deeper in the three specific PICASSO technological areas, drawing on the work of the PICASSO expert groups and we will provide a starting point to collect their further input to identifying connections between policy and R&I collaboration. [section 3]

Building on these, Section 4 explores possible ways to address the challenges that cybersecurity policies pose to collaborative R&I and to improve the impacts of collaborative R&I in the PICASSO domains on cybersecurity policy. Roughly, these can be divided between ways to make the best out of what we have by reducing dependencies on insecure infrastructures or reducing the incidence and severity of cybersecurity failures on one side, and redesigning the infrastructures on which we currently rely, and/or devising new ways of using them that are relatively immune to existing and emerging cybersecurity threats on the other side. We discuss both approaches (mitigation and adaptation), what they would entail, and how they could practically be assessed and ultimately implemented. [section 4]

In conclusion: we see many opportunities for collaboration in this field, which concerns truly global issues and global technology development and applications. A number of specific conclusions lead to possible opportunities for EU US ICT collaboration, in which we will sum up our current understanding of what this means for 5G networks; Big Data; and the IoT/CPS.

- 5G networks: To ensure safety and promote trust in the envisioned networked society, common understanding and measures have to be reached in a global scale. EU and US should

work together and lead the way by devising ICT security policies that benefit both industries and societies in a long run.

- Big Data: Policies need to ensure that access to huge datasets is maintained but in secure and controlled ways that will obstruct malicious interference while enabling assessment of trustworthiness of data, wherever this resides and in whatever volumes.
- IoT and Cyber Physical Systems: Overarching policy measures are complicated because cybersecurity and privacy are sensitive topics that may make cross-national collaboration difficult to set up. Policy measures should aim at supporting and simplifying the collaboration of industry and innovators to solve these issues; the establishment of major direct regulatory measures is likely not feasible within reasonable time horizons between the EU and the US.

People within the EU and US want ICT products and services that serve them and are trusted by them, and need ICT products and services for being able to deal with a number of societal challenges and individual preferences. Better EU-US ICT collaboration can hugely advance this.

Towards the Summer of 2018, we intend to deliver a White Paper on policy issues that are most relevant to technological and commercial development in the PICASSO domains and conversely to identify the aspects of such policies that are most likely to be affected by 5G, Big Data and IOT/CPS development. Therefore we invite you to share any comments and suggestions relating this and other policy papers with the PICASSO Policy Expert Group either in person during one of our meetings (workshops or webinars) or via email to the Chairman at maarten@gnksconsult.com.

I. Introduction

One objective of the PICASSO project is to bring forward policy recommendations designed to improve EU/US ICT-orientated collaborations, specifically in the domains associated with 5G networks, Big Data, and IoT/CPS.

The aim of this paper is to establish a framework for the consideration of ICT security issues as they impact the development of future EU/US ICT-orientated research collaborations, specifically in the technological domains associated with 5G networks, Big Data, and IoT/CPS. Specifically, it will address the underlying issues of technology that are used to implement the future services as well as the international policy issues that affect our ability to control security. We focus on security of ICT – not on the potential contribution of ICT to physical security.

As has been showed repeatedly there is no magic cure for the serious security issues that have become part of the underlying infrastructure and services that hold promise in the future. The proliferation of adverse and highly-publicised events, including massive distributed denial of service attacks on the Internet, malware, hacking, and unauthorized penetration of critical services and sensitive data have caused major disruption and compromised individual privacy as well as nation-state information security. The increasing complexity of hardware and of application, operating system, platform and network protocol software has shown that increasing complexity has offered many opportunities to cause mischief – some of it disruptive, expensive and dangerous – as well as providing more sophisticated (but temporary and limited) solutions to security challenges.

The Internet was originally a research project that succeeded beyond the expectations of everybody involved in its development at that time. Today it provides critical infrastructures for all our ICT and data related services and serves as backbone for (traditionally non-ICT based) services such as energy, healthcare, traffic, etc. The Internet has major limitations that severely affect the various aspects of real security, even more so since security measures that have been developed to address structural weaknesses in security are not always widely applied. In this we acknowledge that the design of the Internet made provisions for dealing with many of these issues (not least as a result of the semi-military context) but that the development and understanding of these capabilities withered through underuse. Therefore, the response to security challenges is not simply a matter of tweaking things, but includes the need to address architecture, design and praxis and less controllable forces like evolution and disruptive change as well. Possible paths to address these limitations will be discussed.

In addition, there is a major difficulty in identification of the causes of security failures due to legal constraints and the identification of the individuals/organizations that have been responsible for many of the failures. Many of these problems have been due to a lack of international agreements on how to address legal issues, ranging from criminal behaviour using ICT to delivering poorly protected and sometimes poorly tested software and hardware with intrinsic vulnerabilities. In addition, the limitations on encryption technology is just one example of a legal system that was not structured for the international behaviour of the Internet. This, as well as “how to address the technical issues, is the policy perspective where we seek possible ways forward towards a more secure ICT environment, globally.

We recognise that whether EU/US collaboration leads to societal, technological, economic, or policy/regulatory 'solutions' will depend on a competitive struggle (across markets, labs and legislatures) as much as it does on a cooperative, neutral and civilised discussion. Pursuing this mix of modes (cooperation, competition and conflict) requires the willingness to collaborate of governments and other stakeholders.

Although PICASSO will not be able fully to address all stakeholder concerns, it aims to explore how US/EU collaboration in ICT can best be served, taking into account the differences in approach towards ICT security in the US and in Europe, respecting the law and citizens' expectations and preserving the widest possible scope for innovation and deployment.

II. The technical situation

While our computing environment has increased in power and distribution dramatically, the vulnerability of systems has also increased due to: the increasingly distributed nature of control and access (especially as a result of distributed cloud services available over the Internet and the ubiquity of wireless and mobile access); and our increasing reliance on a widening range of unseen and/or autonomous functions as part of the communications and data infrastructure underneath the applications. In addition, the following aspects contribute to the vulnerability of our technical ICT environment:

1- *Monoculture of systems*: The emergence of operating system monocultures (Windows, MacOS, Android and Linux) and the consequent vulnerability of application ecosystems that have been constructed on them – the scale of these systems (especially those used by less technologically-aware users) has created an attractive target for security vulnerabilities.
2- *Interdepence of capabilities:* The interdependence of Internet capabilities, the complexity following the interdependence, and age-range of the different Internet components has created additional problems, which have shown themselves in attacks on the Domain Name System (DNS), denial of service attacks and various flaws in the security mechanisms of the Internet software. Old, sometimes bad code often stays active for a long time, while new things are added offering new kinds and better (secured) services;
3- *Maintenance and patching*: Over-the-net (and often automatic or unscrutinised) software maintenance and patching and new products and new ways to offering products (e.g. apps rather than applications) have created an environment that allowed malware to be widely distributed on a massive worldwide capability.
4- *Vast growth of number of "connected things"*: The massive distribution of IoT (Internet of Things) devices, often based on old and sometimes defective software, especially network software, and poor security mechanisms have made it possible to exploit vast numbers of devices to mount coordinated attacks on critical infrastructures and vital system nodes alike.

While there has been significant research into processor architectures, Software Defined Networking (SDN: decoupling the network control and data planes) and Information Centric Networking (ICNs)[1] that might help to alleviate some of the problems, there has been little integrated work in the creation of a distributed infrastructure that can allow a reasonable guarantee of security in important critical areas such as power, water, financial systems etc.

In addition: *things aren't getting any better*. Consumer-centric products drive problematic behaviour that can further compromise the security of the IoT. These products traditionally pursue high speed to market and minimal cost. There are low barriers to entry for developers, distributors and users alike; combined with limited support and upgrade periods, the result is a plethora of systems. Many components of these systems are unsupported or unpatched and continue to be used long after they have been compromised or are otherwise obsolete. These forgotten (but still active) elements are the very definition of "technology debt."[2] In addition, their existence progressively complicates the design and assessment of new systems. In ecological terms, the IoT shows some signs of a malfunctioning 'natural selection' component; unfit systems do not always die out, and potentially superior alternatives may be killed off by these relics (or fail to attract a critical mass of users) before their virtues can be demonstrated and captured.

This not to say that we don't understand - from experience and research – how different technologies can, when properly used, provide a basis for increased security – even in an evolutionary and dynamic fashion. Much of this work has been going on since the 1970's. Such efforts like Multics, capability organized computer systems, industrial activities such as IBM and Intel among others have undertaken can provide key components in the creation of such systems, but the emergent nature of security, the adaptability of human users (and the commercial, etc. layers) and the value of "appropriate insecurity" (i.e. not being more confident than one should be) at the micro and meso level in fostering greater security at the macro level still needs to be taken into account.

In the past, most of these efforts have failed in the market place since industry, consumers *and* governments were not willing to "pay" for security, maybe also as the direct link with concrete security advances has not been made clear. Perhaps it is time to reconsider the past and current research in light of the real demonstrated urgency of increasing the security and reliability of our increasingly critical infrastructure, as many solutions have already been invented – they are just not widely deployed, yet. Where necessary, new solutions may need to be found, in particular relating to emergence of new technologies and services.

[1] See http://ieeexplore.ieee.org/document/7226783/?reload=true and https://arxiv.org/pdf/1603.03409.pdf

[2] Securing the Internet of Things - Explore security and privacy in an interconnected world; Hewlett-Packard Viewpoint, December 2015

III. The policy situation

With ICT technologies and services being largely developed and often deployed for global application, a number of national and regional (e.g. EU) differences in policy (including support for R&I, infrastructure investment & deployment and regulation) and international "legal" issues stand in the way of ensuring Pareto Optimal[3] cybersecurity, appropriate distribution of risk and efficient liability arrangement. This affects trust. As with risk minimisation, a simplistic commitment to trust maximisation is neither meaningful nor desirable – the levels of trust should be realistic as it otherwise increase the vulnerability of our systems ("justified trust").

We recognise that the policy environment engages with cybersecurity in a variety of ways. On the demand side, policy (especially dedicated cybersecurity policy) is often a consequence of stakeholder demand for action in light of perceived failures (reactive), or undertaken in an attempt to head off private sector actions (ranging from technical measures to changed contractual relations) that may have other adverse impacts. In addition to cybersecurity policy *per se*, we acknowledge that many other important policy domains are affected by cybersecurity-related concerns, including some that are critical to EU-US relations.

In order to frame the discussion around policy coordination and collaborative policy-driven R&I, we distinguish:

i) personal security (privacy and non-commercial aspects of security);
ii) commercial security (including protection of proprietary information, system function, reputation and IPR); and
iii) societal, critical infrastructure and essential public service security (on national or international and governmental or intergovernmental levels), which includes e.g. security of critical systems including ICT-enhanced transport, energy and political mechanisms.

A. Cybersecurity risk cannot be 'minimised'

Even at a theoretical level, complete cybersecurity is neither possible nor desirable (due to moral hazard and over-reliance). "Minimisation" is not meaningful since risk includes both likelihood and severity and measurement that dependent on the degree to which people can agree on:

i) the risks and their probabilities,
ii) the incidence of consequences (who gains and loses) and
iii) the correlation (both in terms of probability and payoff) connecting different risks.

[3] Pareto optimality is a state of allocation of resources from which it is impossible to reallocate so as to make any one individual or preference criterion better off without making at least one individual or preference criterion worse off.

If it cannot be minimised, what would be desirable? Inevitable trade-offs and correlations among the likelihood of breaches and their consequences (advantages and disadvantages) militate against a single optimal cybersecurity posture or system architecture. They favour an 'efficiency frontier' of Pareto optimal postures where any improvement in one respect necessitates sacrifices in another. The risks are not limited to the technical aspects of cybersecurity. Some breaches are nearly costless for those affected, and thus neither pose an enterprise risk nor concern for those using the system. In other cases, the mere possibility of a breach (even if it is extremely unlikely) may be regarded as a significant risk, raising the cost of capital, diminishing useful trust and provoking strong policy responses. Thus it is clear that risk may have very different meanings in the technical, organisational, commercial, economic and policy 'planes.'

Consequences are not limited to the 'attackers' and 'defenders' of conventional analysis; a security issue in one part of the system may produce benefits in other parts (e.g. cyber-insurance and cybersecurity defence providers) as well as costs (e.g. to system users and authorities). One example here is the exploiting of system vulnerabilities by security agencies, that may be useful in infiltrating information systems of criminal and/or terrorist organisation, but also create a dilemma: if security agencies are using it rather than stimulating to patch these vulnerabilities, these vulnerabilities will last longer and may be used by criminal actors (e.g. the WannaCry Ransom hack on the back of a vulnerability exploited by the NSA).

Risk cannot simply be minimised, let alone eliminated. It cannot be defined simply in technological terms because a given cybersecurity vulnerability will have greater or lesser consequences, and things going wrong will ultimately be more or less likely, depending on the assets at risk and the capabilities and incentives of security managers. Ideally, responsibility for cybersecurity risk should be allocated in ways that balance the stakeholders':

i) knowledge, understanding and information access;
ii) capacity to bear losses or benefit from improvements (including risk tolerance); and
iii) capability to act in an effective and timely manner to reduce risk, mitigate adverse consequences and reallocate roles and responsibilities in light of changing circumstances.

B. Trust cannot be 'maximised'

Trust is the intention to accept vulnerability based upon positive expectations. In an ICT sense is distinct from trust in the ordinary sense, which may be enhanced or undercut by ICTs. This is related to differences among trust in people, organisations, systems, devices and information distinction. Considerations must take into account the nature and consequences of trust, especially when ICT systems are used to collect information, analyse situations, make recommendations and/or carry them out. It should recognise the dynamics of the interplay between trust (or: perceived trustworthiness) and trustworthiness (or: justified trust), and the ultimately subjective and reputational attributes of the kind of trust with which policy and policy makers are generally concerned.

Putting the focus on improving trust rather than increasing trust allows for the distinct possibility that too much trust, or trust wrongly placed, may be harmful, and may damage useful trust in areas where it *is* appropriate (in other works, the networks formed by relationships of trust). Trust by definition

involves incomplete monitoring and information, so it is vulnerable to adverse outcomes. The greater the trust, the more serious and long-lasting the effects of betrayal or breakdown. As an old Dutch saying goes: “Trust arrives on foot but leaves on horseback”.

Consequently, trust in systems – and the success of technological and policy measures to improve such trust – give hostages to fortune. While such measures may reduce the likelihood of breakdown, they tend to increase the harm such breakdowns may cause. It is thus very important that the perception of trustworthiness aligns with real trustworthiness.

C. Trust and security are both real and imagined

Trust – or willingness to trust – is likely to arise among users of secure systems, but the different aspects of trust and security must be clearly differentiated to minimise the risk of category errors:

- Assuming that more trust, or more security is always preferable, more trust implies more security or *vice versa*;
- Assuming that trust can be given a simple unitary definition that works for all the ways
    - a single individual, firm or government uses a system or service,
    - different people, firms and or government encounter or use such systems or
    - people, firms and/or governments interacting with each other by means of ICT-enhanced systems or services trust each other.
- Treating trust and security as objectively-definable or measurable functions or properties, rather than as states of mind, (patterns of) belief or emergent norms or conventions.

We also need to recognise that (objective and subjective) security and insecurity depend on *knowledge* (e.g. of devices, systems and services and their interconnections), *beliefs* and *events*. Security is essentially concerned with uncertain or risky outcomes. Policy and research collaboration are necessary to identify and quantify (even to price):

- the probability of different outcomes (and responses);
- the severity and distribution of adverse consequences; and
- our ability to do something about them.

Beyond better understanding of these dimensions, such policy and research, reflecting as they do the different perspectives and security cultures of the EU and the US, can shed light on the correlations among different sources and aspects of insecurity, if only by helping us to understand, anticipate and take policy account of herd behaviour and other feedback processes.

D. Simplistic approaches to a complex problem

At heart, many of the thorniest aspects of cybersecurity policy have their roots in inherited ways of thinking that are inappropriate to the increased scale, complexity, speed and scope of information exchanges. Many policy ‘solutions’ are designed to create capabilities that should enable people to identify and fix problems, but which all too often rest on assumptions that are simple yet not sufficient in complex situations. The following paragraphs present some of challenges in complexity. It is lumping

together things that should be distinguished, by either dividing into separate 'stovepipes' issues that share important common elements, or by trying to impose consistency and commitment on a system that might otherwise be able to evolve towards better outcomes.

Data and its uses and abuses

One popular perspective starts from the recognition that control and use of data are of growing economic and commercial significance. This has led to three fairly-distinct strands of what might be called 'data economics.'

1- *Economic value of data*: The first concerns the economic value of data themselves. If data are treated as economic assets, there is a natural tendency for policy to treat them as with other assets, seeking to regulate their use by the creation of property and related rights to data themselves. For personal data, these may take the form of fundamental rights (e.g. the European concept of data protection as a fundamental right) or economic rights (e.g. the idea that the generation, control and use of data could be improved if data 'owners' can be identified and empowered, e.g. by giving them claims to the value of their data in use, or by mandating policies that allow data owners to withhold, modify or control their use. The growing literature on the 'data economy' deals with this at length in contexts that range over personal data, IPR and clinical trial data, commercial secrets, etc. The forms of rights and regulations are adapted from those used for other assets, including those domains (such as financial trading) where data have long been the principal source of value. This is linked to security in individual and collective ways.
    a. The individual level concerns security as an aspect of ownership; policies that seek to enhance the security of data owners' and controllers' claims, and thus their ability to bear responsibility.
    b. The collective aspect regards data as a public good, deriving its value from controlled access by others rather than by 'consumption' and sharing the defining characteristics of non-rivalry (my use of data does not limit your ability to use it, though it may reduce or increase its value to you), and non-exclusion

    It may not be possible to deny people access to data and thereby to establish its value in order to reach appropriate policy and other decisions). On this level security of data is an aspect of collective or societal security, analogous to (but often much more immediate and common) environmental, food, energy and defence security.

2- *Changed economics in data driven economy*: Beyond the economics of data lie the changed economics of a data-driven economy. The use of data flows to connect different people, services, etc. has irreversibly changed our socioeconomic structures, and has weakened or compromised the performance of markets, governments, laws and voting as societal mechanisms. This is in itself the subject of research and debate. Economies can effectively be regulated by local exchanges, national economic regulators and the formal structures and slow processes of trade policy are everyday refuted by experience. This applies to economic governance (competition, taxation, consumer protection) as well as to the use of economic instruments to address other issues such as innovation policy, control of harmful or illegal

content or the fight against radicalisation and terror. The complex dynamics of high-speed, large-scale data flows cannot easily be governed by traditional 'crash barrier' rules. This has implications for conventional security because it frustrates or distorts traditional security policies and refutes the traditional ways in which security policy is analysed (e.g. attacker-defender polarity and the prioritisation of security objectives and legal responsibilities ahead of other objectives and considerations). It also creates new forms of insecurity: people lose faith in the quality and reliability of data and information that reach them and cannot easily be assured that decisions made by others are accurate and fair, thus losing the chief advantage of *living in a trustworthy system*.

3- *Governance of algorithms*: The way data are used through algorithms creates an entirely new set of issues. The important points for policy are:
    a. such systems are almost impossible to understand or to regulate either ex ante or ex post;
    b. knowledge about the structure and function of algorithms is itself a critical 'secret sauce' that is protected but which must be disclosed or understood if laws and regulations are to be adapted; and
    c. policy-relevant outcomes depend not simply on the quality and control of data or the quality and use of algorithms, but on their combination and interactions between different 'pockets' controlled by different entities.

In other words, for some of the most important cybersecurity issues, no-one is in control, no-one understands what is happening, and no-one can usefully be held responsible.

Definitional issues

As one illustration of this, consider the way that security – especially in the ICT sense – rests on information (data and processing) and the increasingly obvious ways that insecurity of these underpinning elements (fake news and compromised algorithms, resp.) produce much more widespread and consequential insecurities.

Beyond the definitional questions, policy must deal with the behaviour of stakeholders as well as the rules that are to control them. Put simply: however trusted and trustworthy the architecture of a system, outcomes depend on (and are experienced and evaluated by) people, organizations and nations that interact with the environment and each other. Much of our legal and regulatory framework dates from before the Internet, and evolved independently of the current Internet:

- many of the issues arising on and in relation to the Internet cannot be 'handled' by existing laws and legal principles (e.g. consent as the primary basis for coercive regulation);
- many existing laws are affected by what the Internet makes possible, and how the Internet is used; and
- many of the behaviours with which laws are concerned are much older than the Internet, even if they now take place over it (and therefore have greater scope, speed, etc.).

Identification and authentication

It is sometimes necessary to ensure that a user is indeed who they claim to be (authentication), or to establish their identity even when not volunteered (identification). This is to be able to make them legally responsible for actions that they cause to happen, or to insulate from liability those who accept authentication or identification in good faith.

Even where the existence of technical means of identity verification makes it possible to hold people responsible, it does not follow that responsibility should efficiently be placed on that person. If we use technical capacity to maintain former placement of responsibility, system architects or operators can claim to have done their duty in order to escape responsibility that they should bear (e.g. age verification for access to online pornography).

Moreover, stronger identification is not always better, for example because it makes mistakes more serious and may make repudiation (of incorrect attribution) or correction much harder. Therefore, 'one-size fits all' security standards – whether for commercial or legal purposes, should in some cases be replaced by a differentiated approach based on analysis of the 'security sensitivity' of different *combinations of* individuals, technologies, services and contexts.

As a result of this complexity, and the asymmetric interests of different national legal and economic systems, international agreements on identity systems, when existing, suffer from validity and security problems, non-universal use (like the USA Social Security Number – which is often found to be insecure) or serious social pressure against the establishment of such a system. The lack of such a universal system makes it difficult to determine who owns computer accounts, email etc. and thus makes it very difficult to place the blame for malware, false news, etc.

It may be necessary to reconsider the extent to which placing blame and liability continue to be useful governance mechanisms for the activities of gathering information, choosing responses and implementing/paying for them. This reconsideration will take a different form in relation to each of the three PICASSO technological domains, e.g.:

- For 5G networks, it is clear that traffic data (including geographical position and links) and data traffic across 5G networks needs to be protected from tampering and unauthorised access. This is taken into account in the design of 5G networks. Security Breach notification laws exist both in the EU and US and further actively stimulate building in security from the outset.

- In Big Data, emphasis is on secondary use of data, and data breaches notifications are difficult to relate to collection and combination and use of data through algorithms. If anything, abuse of data (e.g. for malicious, unlawful purposes) may be more subject to protection than having access to data itself, even if the basis for this protection is different in the US (for instance: privacy is an economic right) and EU (for instance: privacy is a fundamental right).

- With regards to IoT/CPS, different IoT devices are often combined in one environment, and security of the CPS will relate to the weakest link. An important consideration is on the responsibility for failing/poorly secured parts in a CPS. Up to what point can a CPS provider be expected to double-check the quality of individual "Things" – up and beyond "certification" by the producer of such a "Thing"? This may require establishing "sufficient security" at the level of each element.

Identification primarily enables the imposition of *personal* liability; it is thus likely to have only limited effectiveness against instances of organised or corporate carelessness or criminality, especially in a global context. 'Gaps' in the coverage of identification systems could in theory be filled by a system of universal ID operating on-line, but most governments would resist such measures strenuously[4], even when it concerns federated solutions.[5]

Even were such a system to be deployed on an international basis and/or mutual recognition arrangements negotiated, it seems unlikely that identifying a suspect or a threat with a person in another jurisdiction would lead to any sort of prosecution or effective law enforcement; if ISPs were to participate in a co-regulatory initiative by seeking to block such a person, it seems probable that they would respond by changing their registered identity. We should also note that:

- Individuals are identified online by IP, MAC IMEI numbers, etc. and not by anything attached to themselves;
- Biometrics are ambiguous;
- Other forms of personal identity (esp. passwords) are becoming unwieldy and increasingly insecure; and
- Multiple enrolment is a classic, and simple, way to defeat even strong identification systems.

Data and processing integrity and quality

Another set of simple assumptions that are often made in relation to data and to cybersecurity are those derived from the artificial model of a single decision-maker acting in a vacuum; that data can be regarded as more or less 'accurate' or true, that data that are more accurate or true are superior; and that (almost in consequence) more data inevitably lead to better outcomes. Sadly, almost none of these assumptions can be verified; the fact that they are so commonly made ensures that they will be violated. This leads to both 'technical' (as distinct from technological) and pragmatic considerations.

From a technical standpoint, the issues of truth and accuracy relate to the connection between data (or processed conclusions) and some objective reality. Note, this is not an idle philosophical or epistemic conundrum, since real – and deeply serious - outcomes may result from wholly mistaken beliefs, while access to partial, but true information may likewise produce results that are in no-one's interest. Put briefly, we may need to rethink concepts of data 'quality' for a post-truth era.

[4] As shown by the widespread resistance to proposals for universal biometric identification (UBID), though solutions continue to be proposed, especially as fingerprint sensors become more widespread as means of securing devices and the information to which they give access.

[5] Like eduroam which is a federated user authentication system in use by research institutions that allows users of one university to log in to networks on most universities around the world

Truthful data and common knowledge

Epistemologically, the assumptions mentioned above derive from another; that there is a single 'truthful' description of reality[6]. Associated to this are:

- Incomplete descriptions (which leave many more possible descriptions as 'possible' but do not exclude the truth);
- Partial lies (which include some provably false elements along with some truthful ones; the set of possible worlds excludes the true world, but can include it if the false elements are dropped (bringing us back to incomplete description) or corrected; and
- Complete lies (in which every (or every significant) element is false.

There are several important complications to this.

- The normal approach to information policy treats statements as either True or False (complete lies); epistemic logic allows richer approaches (but still tends to assume the existence of a single 'true' state);
- A full or truthful description may lead individuals (based on their understanding, cognitive ability, interests and 'behavioural constitution' to make worse choices than a modified or incomplete description[7];
- Policy generally fails to distinguish among knowledge, truth and belief, let alone hierarchies of these[8]; and
- It also does not always link information[9] to actions (including expectations or predictions) that may be critical to security contexts.

One example is a variant of the chain-store paradox. Suppose a data subject (S) is associated with some records that suggest that S constitutes a security risk. A defender (D) may take enforcement action, which will have positive or negative payoffs (depending on whether S was – or could be proven to be – a risk); alternatively, D may let S know that D possesses this information in order to deter S's bad behaviour. But then S can ensure that D obtains the information in the hope of triggering D's action if S knows that the result will be negative (S as agent provocateur) or positive (clearing S's name); etc.

---

[6] Using Kripke 'possible worlds' semantics, a 'statement' or 'event' comprises a set of possible worlds, exactly one of which is 'true.' The bigger the set, the less accurate or precise the information.

[7] An example is a 'Smart Road' system that informs drivers of congestion ahead to allow them to choose alternative routes – if all drivers receive the same accurate information, traffic jams are moved, but not eased.

[8] Statements of the form "I know that you know that he knows that I know…" or "I believe that you know…" which are generally constructed atop a single (if possibly unknowable) truth.

[9] Including access to or processing of information.

Truth stands as the bedrock in all of this. Establishing the truth (narrowing the range of possible outcomes) reduces uncertainty and can be seen as enhancing security. In an interpersonal context, establishing common knowledge enhances security by providing people with greater certainty as to the beliefs of others and by reducing the potential for disasters based on misunderstanding.

Truth in that sense may not exist or be discoverable through common knowledge. More importantly, in the era of 'fake news,' scientific fraud, etc. truth may have no relevance – all that matters to those who generate, capture and or use information is that it has the desired effect on shaping beliefs and triggering actions. This lack of a common foundation (in the truth) makes things even more complex; in particular, when assigning power or responsibility to data subjects, the State or a legally designated data controller is not guaranteed to do good, and may be disastrous.

Solution 1: validation and laws

Collectively, in order to preserve the role of evidence-based policy, it is important to validate the integrity of data and information. This may mean establishing an 'audit trail' covering the provenance of the data and the history of access, modifications, uses and cross-linking. Traditionally, this has involved *de facto* ownership of data, for instance in the form of 'authentic sources' or via certification or liability contracting. Increasingly, however, more nuanced technical forms of situation dependent and jointly controlled data governance are being explored, such as distributed ledgers and smart contracts. But there may be problems in establishing quality assurance. For instance, validation is not absolute, but localised and contingent. Proper enforcement of data minimisation (amount, time and purpose(s)) could take care of much of this, but may be frustrated by:

- the interests of the state in retaining (processed as well as raw) records for forensic and security purposes; and
- the ability of commercial datavores to retain these data in pseudonymised form (secure from data protection enforcement and data subject scrutiny, if not from re-use and abuse).

Uneven distribution of knowledge and ability to use legally-provided powers to counter these abuses can make the 'protection' of laws, regulations, treaties and contracts unjustifiably and unethically unequal.

Solution 2: rights-based approaches

These can be seen as two extremes; the trusted and non-trusted ends of a continuum in which people are given limited scope to ensure the accuracy of parts of the collective body of data and knowledge.

For purely personal data, this is the dominant regulatory model, as expressed in the rights enshrined in the GDPR and the Fair Information Processing Principles. The burden (on an individual or a firm) of finding and assessing what is known about them may be enormously disproportionate. This undermines two important principles:

- data agency – the ability to trust organisations to hold and use information about a subject in order to combine it with other information that the subject does not or cannot hold in order to further the subject's interests; and

- data responsibility - giving subjects access and powers of correction[10].

Even where rights-based approaches have been implemented (e.g. for personal data protection or proprietary data and information) it has become increasingly evident that they do not scale (in amount, types, speed or global reach) and cannot handle complexity (due to the temporal, resource and cognitive limits of human beings). Moreover, they are difficult to extend to data that apply to, or are controlled by, multiple subjects.

Solution 3: the 'data home'

To overcome the problems of asymmetries of scale and knowledge, there are various solutions that seek directly to restore data agency and responsibility. An example is provided by the concept of a 'medical home' – a physician who represents the patient (via professional duty) in a complex healthcare system; collecting and managing information, helping the patient to understand and contribute to this information and supporting the patient's decision-making. Another example is provided by the 'authoritative source' concept in the context of e-Government; a single repository where a reliable record can be found, that also provides a single point of visibility and control for the data subject. This need not literally be a single data home or 'data double' of the real-world person or entity, but could instead be a federated structure of decentralised but unique data elements, identifying the location of security- and privacy-related and/or previously-submitted data, together with their provenance, permitted uses, etc.

This would provide unambiguous points of control and allow assessment of burdens and impacts, and could usefully replace fixed and potentially perverse or manipulatable assignments of rights. It would do this by explicitly changing the network structures of access, storage, processing, etc. rather than by trying to design security policies that are meant to operate independently of those structures.

The advantages seem powerful. Without a single 'data home' it may be impossible to curate our 'online identities' and avatars. No amount of rights to correct or 'right to erasure' can ensure against loss of coherence and substantially misleading interactions between people and systems or forestall inevitable abuses both by data subjects and by those involved in processing their data for fun, policy or profit.

Cyber-crime and cyber-enhanced crime

The definition, assessment prosecution and prevention of cyber-crimes vary across nations, and legal systems often make it difficult to take such cases to court. Such prosecutions do not deter future crimes: legal and prosecutorial judgements from other jurisdictions are not mirrored or recognised. This has led to the perception in some circles that some nations' laws do not recognise cybercrimes or provide legal tools to counter ICT-enhanced methods of committing conventional crimes.

[10] Note that data responsibility allows data controllers to shift undefined amounts of accountability.

This perception is not generally correct. At EU level:

- The 2001 Framework Decision on combating fraud and counterfeiting of non-cash means of payment defines the fraudulent behaviours that EU States need to consider as punishable criminal offences;
- In 2002, the ePrivacy Directive required providers of electronic communications services to ensure the security of their services and maintain the confidentiality of client information;
- The 2011 Directive on combating the sexual exploitation of children online and child pornography, addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse); and
- Directive 2013/40/EU[11] aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions

These are all backed up by the activities of the European Cybercrime Centre (EC3[12]).

In the US, see state and federal references at http://www.hg.org/computer-crime.html.

These activities are mainly focussed on defining and legislating to prevent new, specifically cyber, crimes. Within these overall provisions are new categories of crime linked to specific technological domains. Examples related to 5G, IoT/CPS and Big data related crimes include:

- DDOS attacks on 5G networks, including functional degradation, etc.
- Ransomware/DDOS attacks on Data Analytics facilities, esp. those linked to e.g. algorithmic trading, analytic engine or data centre compromise;
- Interference with the function of IoT (esp. autonomous devices) and CPS control systems, as illustrated, for instance, by the malicious Stuxnet worm that specifically targeted programmable logic control systems in industrial processes to degrade system operation and to damage, or even destroy, industrial hardware.

Beyond this, policy increasingly has to adapt to the ways in which these new technologies change the law enforcement landscape by facilitating existing types of crime (e.g. fraud, theft, tax evasion, money laundering, etc.) by making forensic and prosecutorial evidence-gathering and analysis easier or harder and by providing payment and transaction services to criminal enterprises.

Encryption

Encryption is another area of tension between national laws and technological approaches to the same or similar problems, with the added complication that the objectives of the players differ. On the policy side, encryption can be used to control access to data held by public authorities and to enable secure

[11] 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 – 2013.

[12] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

communication in insecure environments. The use of encryption by service providers and users can yield economic advantages to the sectors where they are used and can help to protect information resources (including IPR and personal data controlled by private players) held by important national (private) entities against espionage, hacking, etc. On the other hand, the use of encryption can deny public authorities access to data that they need to process for a range of legitimate law enforcement, security and regulatory reasons.

There is similar complexity on the private sector and civil society side as well. As a technical means of access control, most encryption applications are agnostic as to the contents they protect and the uses for which access is sought thus they may lack the subtlety of contractual or regulatory approaches while offering a potentially higher level of protection. Neither encryption nor alternatives are necessarily 'stronger' or more transparent. We note that business attempts to limit exposure are more likely to take the form of shifting liability to consumers than taking effective precautions, which is why so many problems have arisen through reliance on passwords (which are increasingly unmanageable). Whereas recognised, banks and payment service providers have not widely adopted alternative measure like secure biometric technologies, and instances of identity theft rarely result in compensation.

One approach is to legitimise certain forms of access and to legislate to regulate and enforce them. This is the approach taken for example by the UK.

The UK's Investigatory Powers Act 2016 seeks to accomplish three overall objectives:

- To consolidate powers already available to UK law enforcement, security and intelligence agencies to obtain the content of, and data about, communications;
- To overhaul the mechanism for authorising and overseeing these powers; and
- To ensure that powers afforded in existing legislation are fit for the digital age.

The Act had a controversial passage through Parliament because it gives government agencies far-reaching powers to require technology and communications businesses (inside and outside the UK) to retain their customers' personal data. Its two most relevant provisions are:

- Bulk powers and encryption removal: The Act gives certain government agencies access to large volumes of data through bulk interception and bulk equipment interference warrants, provided the main purpose is to acquire intelligence about individuals outside the UK (even when the conduct occurs within the UK). Similarly, interference with the privacy of persons in the UK is only permitted to the extent necessary for that purpose. When served with a notice, *communications service providers* may be required to remove encryption to assist in giving effect to interception warrants. The Act also future provides for future regulations to oblige technology providers to remove encryption.

- Overseas enforcement: The Act allows enforcement of certain obligations and powers to be against overseas companies through proceedings for an injunction or specific performance, together with local enforcement in the applicable overseas country using appropriate bi- or multi-jurisdictional enforcement agreements.

Such provisions – in particular the creation of 'official' repositories for potentially-accessible information or requirements for 'backdoors,' key escrow and other forms of enhanced access both to stored data and to communications 'in transit' raise the possibility that those same means of access can be employed by unauthorised entities, including other governments and their agents. This is not limited to law enforcement and national security alone. Similar risks and ambiguities arise in relation to contract and tort law. It is not always clear who, if anyone, is liable for potential violations of security when data storage, transmission and processing cross nation boundaries.

In recent years, these complexities have become evident through e.g. the Apple case[13], the Microsoft case[14], and the Google/FBI case[15]. In the US, such access requests are often linked to the 'all writs' act under which the US demanded decryption (or access to the plaintext).

For EU-US collaborative R&I and security policy, the key points include the following:

1- Many of the issues cannot be addressed by national technology or service policy because they involve technology supplied by one region and used to provide services in another.
2- Increasingly, the EU and the US face common challenges in the form of security threats that specifically target both EU and US entities, systems, services and users but originate or are based outside both (e.g. China and Russia).
3- Legal and policy developments reflect the growing and vital importance of *extraterritoriality*, in other words, situations where:
   - data held in one region may be sought by authorities in the other;
   - communications or technology service providers in one region my come under pressure to cooperate with authorities in another;
   - Access to data about citizens or businesses of region A by that region's law enforcement, tax etc. authorities may compromise the personal information and/proprietary data of businesses or citizens from region B due to joint records, server farms located in region B or as a result of 'incidental surveillance' that identifies entities from regions A and B; and
   - the specific importance of e.g. tax and product liability rules, where the desire to conceal information spans oceans.

[13] This concerned a demand by the US FBI for Apple to provide access to encrypted data stored on a deceased suspect's mobile device - see e.g. https://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/.

[14] This concerned a US order instructing Microsoft to hand over a customer's email that was stored in Ireland, which was struck down in the courts - see e.g. https://www.ft.com/content/6a3d84ca-49f5-11e6-8d68-72e9211e86ab.

[15] In this case, which in effect reversed the decision in the Microsoft case, Google was ordered to hand over emails stored outside the country in order to comply with an FBI search warrant - see e.g. https://techcrunch.com/2017/02/04/google-told-to-hand-over-foreign-emails-in-fbi-search-warrant-ruling/.

Security principle

Technologists and engineers have a tendency to think of security in terms of system design; something that can to an extent be built-in, but which must be adapted to human weaknesses by being made user-friendly and hardened against identifiable attacks and abuses. A policy analyst would respond that this is the right way to approach the issue once it is decided that technology will make its contribution before or after policy and the economy have acted:

- If technology 'moves first', then policy can establish regulatory limits (from standards to a priori certification and type approval rules);
- if policy moves first, then technology can be designed to fix the gaps and problems imposed by the failures of markets (due to incomplete information, market power, etc.) and regulations (which must be unambiguous, uniformly applied and changed only through slow, deliberate and transparently accountable processes).

To cope with this 'messy' combination of approaches, and to handle situations where the temporal separation of technology and law are not absolute, it may be useful for each domain to articulate design principles that help to manage the interface.

In this section, we present some security principles informed by a technological perspective, and discuss them from a more policy-orientated standpoint. This is not intended to constitute either recommendations for such standards or a refutation of them, but rather to kick off what must be a continuing dialogue. The principles were taken from points raised at the ONE Conference in The Hague[16], but their description is the responsibility of the authors of this paper. We consider two elements: device-level security and the architecture of standardisation and law.

Product security in the Internet of Things

Implementing security at device level is essential in order to enable growth towards a dependable environment. In recognition of the interconnection of these devices into dynamic cyberphysical systems, the following aspects were identified as being of particular importance[17]:

Design it right

- *Be paranoid*, in the sense of conducting risk assessments and mitigations for everything that could happen.

  Rejoinder: this requires a suitable form for the Precautionary Principle and a detailed analysis of possible arrangements for sharing risk, information, cost and (inevitably) liability. It also requires methodologies for such assessments, including ways to deal with unquantifiable risks,

[16] See https://www.ncsc.nl/conference.

priorities for mitigation and precautions against adverse selection (attracting the wrong kind of users or uses) and moral hazard (perverse incentives).

- *Standard technology is better than home grown,* to maximise interoperability, economies of scale and the pace of learning.

  Rejoinders:

  1) don't design everything (some things should be let pass if risks or liabilities for risks outweigh benefits or ability to control risks; other things should be left to evolve unless and until more is known);

  2) recognise that use of standard technology may mean vulnerability to standard attacks, attacks motivated by widespread adoption of vulnerability or simple contagion (esp. when standard approaches used for very different apps);

  3) firms may be motivated to use standard approaches as a way of minimising liability (the Safe Harbour principle), which can exacerbate security monoculture risk; and

  4) security objectives may conflict with competitive need to stand out, to cultivate differential rather than collective reputation or to escape the regulatory burdens placed on rivals.

- *The more eyes the better*, to ensure that general risks and emerging patterns are picked up. This involves
  - *Shared penetration tests because* a lively and aware whole-ecosystem approach is far superior to localised or controlled tests, provided it can be secured against manipulation; and
  - *A culture of responsible disclosure and collaboration*, though again it is necessary to guard against capture, foreclosure and corruption. From a policy perspective, because this culture involves information exchange among commercial entities, it is necessary to bring competition authorities into the discussion. It would not be useful or acceptable to sacrifice competitive efficiency and dynamism to the 'God of insecurity' any more than it is to offer up privacy and civil liberty.

  Rejoinder: this may hold in the abstract, but the sharing of information changes both competitive and cooperative relationships. In addition, not all of the 'eyes' are equally trusted or trustworthy; commercial partners may strategically use, withhold or distort their reviews and reports, and the knowledge of surveillance may directly undercut trust. This has been seen at international and systemic level in relation to the well-known 5 Eyes and 14 Eyes initiatives.

- Build a safety net and a future, which includes e.g. making sure that all systems can be monitored and updated *in situ*.

  Rejoinders:

  1) It is necessary to make suitable provision for spreading costs and responsibilities.

2) It is vital not to go too far in this direction; there have been far too many instances of 'push' updates that have crashed systems, bricked devices and imposed huge costs on organisations of all sizes.

3) Where systems are tightly interoperative, highly optimised and mission – (even life-) critical, the consequences of rapid updating (even for security purposes) could be catastrophic in the short and the long term. This is especially true when there has been extensive bottom-up or user-led innovation, in which case the knowledge necessary to anticipate and manage consequences may not exist at the place from which the upgrade is deployed.

The architecture of policy

In the standardisation world, even at the level of Internet Governance, it has long been accepted that the ultra-rapid development of technology makes it essential that the underlying ethos of legislation, as well as for technology, should be some version of "rough consensus and running code" rather than a search for multilateral perfection in advance of action.

Rejoinders:

1) This principle is not easy to reconcile with the Precautionary Principle mentioned above; it may not be clear why 'rough consensus' should apply to standards (which may have a degree of path dependent 'stickiness' or even permanence), while 'precaution' should apply to technology (which can be modified, upgraded or abandoned).
2) There are also many different types of 'soft technology for use in controlling issues; the law offers certainty while contracts offer adjudicated flexibility.
3) This approach might work in the US and the UK, but would be problematic in Civil Law jurisdictions, let alone international fora where the rule seems to be smooth consensus (nice statements) and inoperative code.
4) The advantages of either approach, or a negotiated or multistakeholder intermediate, depend on the way in which individual performance affects the system as a whole and/or other parts of the system. The ICT domain has largely adopted one of two polar approaches:
    a. the 'best effort' approach that underpins competitive markets or signal transport (e.g. TCP/IP), which is friendly to experimentation and 'meritorious' or instructive failure; or
    b. the 'weakest link' approach that has been advocated for irreversible global risks, healthcare and security, which is more often associated with a Precautionary Principle approach.
5) A synthesis can be created through the design of a system of 'natural experiments.'

IV. New ICT developments impacts

Technology impacts go two ways: legislator frameworks influence how technologies are developed, and technology developments, at times disruptive of nature, can either support or challenge legislation

and/or legislator frameworks. The three technology subjects that are in the focus of PICASSO affect and are affected by the legal frameworks on both sides of the Atlantic (as well as by new/complementary technologies like biometrics, passwords, encryption, Blockchain (no trust = higher(?) security) and so on.

This is already widely recognised, and businesses are looking for guidance on "what good practice looks like". Continuous (and increasingly rapid) changes in technology and society linked to the spread of ICTs complicate framing the issues, and at the same time highlights the opportunities that EU-US ICT collaboration can bring. ICT has become global as ICT products and services are potentially used anywhere in the world, and increasingly with localisation of data, software and hardware at places independent from the geographic location of the user. Examples of challenges that this brings include:

- introduction of the GDPR and NSD in Europe, and the uncertainty related to the solidity of the Privacy Shield agreement between EU and US;
- challenges related to mobility and location of data and thus "applicable jurisdiction (now including locations from where data can be accessed? GDRP);
- challenges related to funding of collaborative research:
    - Collaboration may be difficult on topics of high near-term commercial importance, i.e. innovation efforts that focus on products and services that may lead to large profitable businesses in the near term.
    - Generally, most of the EU funding will be used to fund EU companies and research institutes, and US funding will focus on the support of US organizations and companies.

Thus, EU-US collaboration will always be a complement, or even an exception, to local funding. In this:

- collaboration will be easiest on issues of current interest in both the US and the EU;
- the existence of potential (funded) partners may make it easier to fund collaborative than separate research, as evaluators will be able to take additionality into account; and
- In order for this to happen, issues of (research and application) security and intellectual property rights will need to be resolved.

Below we consider some specific aspects relating to the three PICASSO ICT collaboration areas: 5G Networks; Big Data; and Internet of Things/Cyber Physical Systems.

E. 5G networks

In our move towards a hyper-connected society, 5G networks are likely to play a major role. Building on the 4G achievements 5G networks will also facilitate massive amounts of sensors, both mobile and fixed, using relatively little energy, and ultra-reliable communications that can serve as (very) remote controls. Those new developments will enable 5G network to serve not only as a radio access network but also to serve different vertical industries, such as, automotive and transportation, industry automation and eHealth. This opens a lot of opportunities as well as plenty of challenges, especially considering security aspect.

In the past, the mobile network, from 2G to 4G, has been considered as relatively safe network. It provides basic connectivity service between one user and two operators (one home operator and one roaming operator). Each user equipment can be uniquely identified with a subscriber identification module (SIM) card. However, such a security model will be challenged in the 5G evolution where a single-domain network is transformed into a cross-domain network.

At the device level, an unprecedented number of devices will be connected to the network, including, e.g., mobile phones, tablets, laptops, sensors, IoT devices and machines. The qualities and security capabilities of these devices vary a great deal. For example, IoT device only needs lightweight security while high-speed mobile services need efficient mobile security features. If all the devices are connected in the same network without deploying proper security mechanisms, the low cost and security-light device could be potentially used or tapped to jeopardize and compromise the whole network. Such threat situations should be considered in the 5G security design.

At the network level, new architectures and security mechanisms need to be designed to meet the diverse connectivity and application requirements in different vertical industries. For example, remote surgery robotics require to establish and maintain communication connections with extremely low latency while factory automations emphasize the importance of protecting wireless transmission from unwanted jam signal. Those design aspects are generally not critical concerns in the current 4G network and yet impose important and challenging shaping factors on the corresponding security design in the 5G network. Meanwhile, as different vertical industries are involved, many new services will most likely be provided by multiple operators in one or multiple domains. This again indicates the need to design new security architectures in the 5G network. In particular, extremely high security level is required in case critical infrastructures, e.g., power grids, are involved.

In the 5G network, in order to reduce cost and speed up deployment and optimization process, decoupling hardware and software in the network/equipment design has been seen as a major trend, leading to, e.g., Software Defined Networking (SDN) and Network Functions Virtualisation (NFV) concepts. This implies the increased dependency on software security and decreased reliance on the use of dedicated hardware. With the mix of multiple operators and application providers on the same hardware, there is a strong need to rethink and enforce security design in the 5G network.

Considering the diverse devices connected in the 5G network, a heterogeneous identity and privacy management mechanism might be required to address the diverse differences among different applications and industries. At the same, it is important to define the ownerships and usages of data flowing inside the 5G network coming from basic connection service as well as vertical industries. This directly relates to privacy and data protection aspect of ICT security.

Last but not the least, it is always worthy to mention that the target of 5G is to address the demands and business contexts of 2020 and beyond. Cost and energy efficiency of the 5G network should be kept in a reasonable and sustainable level in order to generate good return over investment (ROI) ratio. In this context, it is important to take cost and energy consumption aspects into account for the security design in the 5G network.

Currently, network slicing that allows multiple logical networks to be created on top of a common shared physical infrastructure has been widely considered as one important technical component to address challenging aspects of 5G network design. It enables differentiated and flexible security services. For example, different logical networks can be associated with different security requirements/characteristics and operator(s) can provide security as value-added services. It meanwhile provides isolations between different logical networks for enabling improved security mechanisms.

In general, the transform of a single-domain network into a multi-domain network in 5G imposes a lot of new challenges on the security design of mobile network. Top-down approaches are required to be studied and implemented in the both technical and policy domains.

F. Big Data

Big Data is a subject of interest to many, and companies as well as governments around the world are looking into the opportunities it offers via e.g. data generation, collection, and analytics. With the connection between data through communication networks it has become possible to gain access to and to process jointly masses of data, potentially to fine detail relating to private individuals. The ability to combine masses of data comes not only with this threat, but also with the promise of new ways to be able to effectively deal with societal challenges, and business challenges.

According to multiple sources, the volume data being collected and processed is expected to double every two years. Within the realm of IoT alone, these flows are likely to grow into the brontobyte range—10 to the 27th power. Network management will go beyond distributed data centre management to a million-node scale in networks.

- *management of distributed data centres* - inherently a 'small worlds' phenomenon with the challenges of emergence, sync etc. that go with this - and
- *million-plus node network management* - most of these nodes being sensor/actuator objects doing relatively limited processing at the local level - or mobile devices – where the complication comes from the changing network neighbourhoods to which those devices are exposed.

They key point is that as networks scale up, it is not appropriate – or even feasible – to scale up network management, security, identification, etc. as used on smaller networks (where the benefits of a 'complete' approach outweigh the benefits). Instead, it is likely that we will have to adopt a mix of

- Management limited to 'local' interactions (for a suitable topology);
- Risk-based approaches that accept higher-than-zero odds of different failure modes; and
- 'Variable geometry' approaches in which governance, security information, etc. change with purpose(s), circumstances, etc.

This – in effect – again moves security away from 'the system' in the technological or design sense and closer to actual, real-time uses. Focus should be on risk management, and on where risk should be placed. Risk placement depends on different parties' access to information; objectives or motivations;

powers of action; level of understanding; and ability to engage in 'bargaining' and contracting to reallocate risk as necessary.

In addition, secondary emphasis should be on how the probability and the severity of security failures should be managed and traded off against each other; and understanding where data reside and its value by quantifying and connecting to business outcomes. In this it is important to recognize data is not information and information is not by definition "truth". Knowledge and belief are also critically important, especially in a post-truth world, where the quality and provenance of information are important and where 'alternative facts' – reinforced by being derived from data and analytics – may lead to overall incoherence in the functioning of systems.

Access to data by authorised persons, as well as integrity of data (not changed by unauthorised persons at the source or underway in communications) are key factors to secure. In the current internet this is not built in, as spoofing and sniffing and hacking activities prove every day. In fact there is increasingly a paradigm shift: security as a system property can be thought of as something objective; but we are (increasingly) concerned with security: at the service level; as a subjective belief; or a relational property.

Opportunities will be to develop ways to ensure authenticated access and assurance of integrity.

G. Internet of Things/Cyber Physical Systems

The IoT and CPS activities in PICASSO focus on the convergence of the IoT with cyber-physical systems into closed-loop, real-time IoT-enabled cyber-physical systems. Such systems can include production and manufacturing systems, power grids, oil and gas pipelines, commercial buildings, transportation systems, and other complex, critical infrastructures. Many, but not all, of these represent business-to-business enterprises, but, regardless, vulnerabilities can arise from anywhere in the global internet-connected world. In these large-scale systems, access to the information provided by IoT-connected sensors is a lot simpler and more flexible than in traditional technical systems, and the connectivity provided by the Internet of Things will become an enabling technology for cyber-physical systems of systems in which the loop from a myriad of sensors to the way the systems are operated and also to the demands of the users is closed. This will enable improved monitoring, management, and hence new levels of energy and resource efficiency, product and service quality, and safe and reliable operation.

Information security and privacy are significantly more complex and fragile with the advent of connected devices, service orientation, and the convergence of IT and operational technology (the latter referring to hardware and software that monitors and controls physical devices)[18]. Cyber-security, privacy, and trust/trustworthiness are seen as dominant topics for IoT and CPS in the US,

[18] Securing the Internet of Things - Explore security and privacy in an interconnected world; Hewlett-Packard Viewpoint, December 2015

somewhat more so than in the EU (although they are seen as important in the EU as well). It is expected that their importance will grow significantly over the next years.

The convergence of connectedness and dependence on information allows attacks and accidents to produce undesirable and even catastrophic effects on the physical environment. One example is the StuxNet virus; specifically created as IT malware that attacked plant process logic controllers (PLC) of nuclear plant centrifuges[19], and many more followed. It's not just a question of securing the "things" under an organisation's ownership or allowed to connect to an organisation's networks. Imagine a situation where a flaw in a common network-connected device is used to launch a denial of service (DoS) attack—there have already been cases of home cable modems being used in botnets. This means systems may be affected by the insecurity of "things" in general. Similarly, if "things" are designed insecurely and lack (secure) mechanisms for detecting and patching insecurities, they can act as a pool of malware capable of attacking other systems. When applied to cyber-physical systems, security implications for IoT are not limited purely to cyberspace. Coordination of cyber and physical intrusions raise additional concerns. In fact, cyber-attacks can be used to mask physical attacks and vice versa, and either can also exacerbate the other.

So, the security of IoT is a concern for the entire Internet community, not just device owners[20]. Impacts could be dire for communities and nations and internationally — including large-scale power outages, chemical spills from plants, road, air, and rail traffic congestion and accidents, malfunctioning embedded medical devices, and suppression of emergency responses to natural and human-caused disasters. The large-scale, closed-loop nature of these systems implies that there are numerous points of potential vulnerability. Furthermore, these loci are dramatically increased with IoT devices. Sensors, communication networks, data repositories, analytics engines, actuation devices, human-in-the-loop interfaces — all of these are subject to potential compromise, which, if not either diligently guarded against or mitigated, could cause extensive physical, financial, and human damage.

Several additional important policy issues arise in IoT and CPS systems that relate to cyber-security. Many IoT-enabled cyber-physical systems cross-national boundaries, which may lead to policy and legal issues and the need for policy alignments regarding data access, cyber-security regulations, and privacy. In addition, many different actors (e.g. companies, suppliers, operators) may be invested in a single IoT-enabled CPS, raising issues of data separation, liability, and ownership, and trust and trustworthiness in technical systems are seen as crucial challenge in both, the EU and the US.

We have found that it may be challenging to collaborate on privacy-related topics due to differences in approach in the EU and the US, and collaboration on cyber-security topics may be difficult as well. Nevertheless, technology-oriented research collaborations on related topics may be feasible, such as attack resilience and intrusion detection for secure real-time and mixed-criticality systems.

[19] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[20] Accenture 2013 CIO Mobility Survey

V. Possible ways forward

We are entering an era when network speeds will be dramatically increasing especially in many backbone and interconnection networks. Criminals are smart and always seemingly one step ahead of security measures. With the changing landscape of technology and applications in the connected world, threat actors and attack vectors are expected to morph even more. In the beginning, threat actors will most likely be motivated by fame, focused on the newly interesting, novel technology. They'll want to showcase their hacking expertise and expose vulnerabilities. But as ICT communications become more widespread, the technology will be attacked or compromised based on the value to the attacker—monetary, ideology, or business disruption. Since real-time interactions are key to ICT communications, actors may use jamming and interference of communications. This may include misrouting of information, impersonation, or flooding and draining of resources, which could cause Denial of Service or at least confusion.

In addition, the increase of geographically distributed and interconnected potentially real-time cloud computing will demand increased bandwidth with high availability and security. This will eventually cause us to re-evaluate many of the assumptions and mechanisms, which are, assumes in the Internet protocol designs. In many ways, the current Internet is more and more becoming the backplane of a massive distributed computer system.

Basically, there are two ways forward:

1- Making the most out of what we have today and increase the security of our ICT and communications infrastructures by better implementing what we have today, continue to develop new patches where vulnerabilities emerge, and ensure stakeholders take their responsibilities by raising awareness on good practice and enforcing responsible behaviour by all stakeholders in the value chain;
2- Redesign the ICT and communications infrastructure we increasingly depend on thus to take out the key vulnerabilities that remain from the time that the Internet was built as a collaborative research environment rather than the world-wide system for accessing and sharing information and communication.

Below we discuss both:

1- Awareness raising of vulnerability issues, patching, and ensuring stakeholders take their responsibilities.

Much of what is needed to reduce vulnerability of our ICT environment to acceptable levels is already known, and ICT security would be much higher if all stakeholders in the value chain of ICT services apply "good security practices" to their work. As was identified before, most stakeholders today feel very little economic or legal incentive to ensure application of good security practices, as there is no common view on this. Possible measures here may be a review of existing measures to improve security and development of new tools and services where possible; establishing a bottom line of "expected good practices" thus to ensure companies and individuals can be made responsible for failing living up to good practice; ensuring industry self-regulation through public commitments to

"good behaviour" with regards to securing tools, systems and services; and awareness raising towards policy makers, law enforcement and end users as to ensure people know what to live up to.

With this "solution", the system will become less vulnerable, but we will not be able to take out some of the intrinsic vulnerabilities in our ICT and communication systems, in particular those that guarantee origin of communications and integrity of information packages.

2- System-wide redesign of computing and communication systems we increasingly depend on

At the same time the mechanisms that software uses to protect and secure inter and intra computer communications strongly suggests that we reconsider (for the 4th or 5th time) the use of capability architectures to identify and protect information as it is moved from system to system and that that be done by hardware enabled methods. Mechanisms such as that would provide a way of identifying forged software and fake information (email etc.). It is beyond this paper to detail the design but just to strongly suggest that it is time to create an integrated international research to design this next generation computing infrastructure (Internet).

A way forward may be to jointly engage in what the USA National Science Foundation calls a *"grand challenge"* and create an operational test bed where the goal is to architect the next generation of network protocols/hardware, securable processor, and the software necessary to operate an integrated secure Internet as well as to be able to attach non-secure environments to the network and still protect the world against their bad behavior. Basically, the effort would be to gather all the past and current understanding of how to create secure systems and to produce a test bed that can lead the path toward as secure a distributed cloud based system as we can. The test bed would, by its nature need to partner both the academic world and the industrial world of at least the EU-USA. It would be best if the initial test bed demonstrated the technology in one of the critical areas – power, aspects of the financial systems etc.

This requires political will and economic buy-in from both governments and industry, and this may require either visionary leadership across the continents, or an increased awareness of the need as major disasters result from the inherent vulnerabilities in our communication networks today on which all ICT and data services are build.

VI. Conclusions

Security of ICT devices, data and services are broadly seen as a top priority and a concern that needs to be addressed. Without appropriate security in ICT, trust in use of the products and services that are based on ICT erodes and this reduces the opportunities to reap the benefits.

With regards to EU/US collaboration, a framework for ICT collaboration needs fully to reflect:

- Security
- Privacy
- Awareness

As the security landscape continues to evolve, so will the threat actors. Currently, there are highly capable threat actors, capitalizing on the prolific black market to buy and sell capabilities and information. This will only continue to grow as additional devices and data sources come online. The growing volume and exchange of data require new technology to protect the user device and data entity. Particular attention will need to be given to adaptive, self-defending, autonomous capabilities. Considering this, the following aspects relate specifically to the three PICASSO domains with ICT security policies:

- 5G networks: When mobile network evolves from a basic radio access network into a multi-domain network, tremendous business opportunities will be opened yet a lot of challenges will be imposed on securing the operation of the 5G network. To ensure safety and promote trust in the envisioned networked society, common understanding and measures have to be reached in a global scale. EU and US, as the most influential forces in the world economics and 5G research, should work together and lead the way by devising ICT security policies that benefit both industries and societies in a long run.
- Big Data: Entering into the era of Big Data, information is everywhere and can be both extremely valuable and extremely harmful. Policies need to ensure that access to huge datasets is maintained but in secure and controlled ways that will obstruct malicious interference while enabling assessment of trustworthiness of data, wherever this resides and in whatever volumes.
- IoT and Cyber Physical Systems: Due to the tight integration with physical systems, security breaches in IoT-enabled CPS will have drastic physical, financial, and human consequences, and cyber-attacks can mask and exacerbate physical attacks. Thus, ensuring security in these systems will be a crucial prerequisite for public safety and prosperity. The general security challenges that are mentioned in this report (DDoS, malware, unauthorized penetration of critical areas, monocultures, etc.) are important also for IoT-enabled CPS. Specific additional challenges include e.g. the internationality of many of these systems (raising numerous policy, legal, and jurisdiction issues, and needs for policy alignments between countries), the large number of involved stakeholders (companies, suppliers, operators, …) that raise questions of data ownership and liability, and tracing of attacks across multi-stakeholder systems, and the need for built-in reliability and security despite large innovation pressure in the IoT space, and consequently for international security certification standards. Overarching policy measures are complicated because cybersecurity and privacy are sensitive topics that may make cross-national collaboration difficult to set up, and because there is a wariness in the IoT/CPS space towards over-regulation, which may stifle innovation. Policy measures should aim at supporting and simplifying the collaboration of industry and innovators to solve these issues; the establishment of major direct regulatory measures is likely not feasible within reasonable time horizons between the EU and the US.

People within the EU and US want ICT products and services that serve them and are trusted by them, and need ICT products and services for being able to deal with a number of societal challenges and individual preferences. Better EU-US ICT collaboration can hugely advance this.

Opportunities for R&I collaboration:

Specific attractive opportunities for EU US ICT R&I collaboration that came forward in the dialogues include:

- Outdated security model—Traditional IT security policies and controls will be untenable. The security model for it will need to transform to support all of the new aspects of operational technology security and transition to a data-centric aspect. Security will need to be automated, distributed, context aware, and real time and will to need to leverage the added value of crowd-sourcing and peer intelligence to help form a self-protecting mechanism;
- "things" on the Internet need to be designed for security, upgradability, and resiliency, and each element needs to be designed to be secure in itself. Things and Systems (CPS) need to be self-protecting and self-healing systems:
- Embedded security—Security will need to be deeply integrated in hardware and application software layers. The diverse functionality and small form factors won't be able to withstand generalized, bolted-on security mechanisms. The technical designs will need to use contex-taware, adaptive security that senses and responds to a range of trust mechanisms;
- Biologically inspired security. With IoT and underlying interconnections, there's a significant risk with IoT devices providing a back door to systems and data. Biological constructs can help identify attacks before they happen, and also incorporate dynamic defense by directing resources to the appropriate area;
- Predictive intelligence: making best use of (IoT enabled) detection systems and (big data enabled) data analysis threats may be foreseen and early detection becomes possible;

Towards the Summer of 2018, we intend to deliver a White Paper on policy issues such as privacy and data protection, security, standardisation and spectrum that are most relevant to technological and commercial development in the PICASSO domains and conversely to identify the aspects of such policies that are most likely to be affected by 5G, Big Data and IOT/CPS development. This PICASSO Policy Paper and the ones that follow will feed in to this White Paper, therefore we invite you to share any comments and suggestions relating to these policy papers with the PICASSO Policy Expert Group either in person during one of our meetings (workshops or webinars) or via email to the Chairman of the Policy Expert Group at maarten@gnksconsult.com.