EUROPEAN FORESIGHT CYBER SECURITY MEETING 2016

Public private academic

recommendations to the European

Commission about Internet of Things and

Harmonization of duties of care

The following partners of the Dutch Cyber Security Council provided input to the meeting:

Belgian Cyber Security Council

CSIS Security Group

CSO Confidential Ltd.

Energinet DK

European Union Agency for Network and Information Security (ENISA)

Directorate General for Communications Networks, Content & Technology (DG CONNECT, European Commission)

Europol

European Cyber Security Group (ECSG)

Harvard University

International Federation for Information Processing (IFIP)

Internet Society

NATO Communications and Information Agency

Microsoft

Radboud University

Royal Philips

Symantec

World Economic Forum USA

The European Foresight Cyber Security Meeting has been initiated and chaired by the Dutch Cyber Security Council within the framework of the Dutch EU Presidency between 1 January and 31 June 2016. The Cyber Security Council wants to express its gratitude to the participants of the meeting.

This document reflects the conclusions and recommendations of the Chair.

INDEX

1 FIRST EUROPEAN FORESIGHT CYBER SECURITY MEETING

More than twenty international and influential experts in the field of cyber security and information technology gathered in Haarlem, The Netherlands, on May 11th to attend the first European Foresight Cybersecurity meeting. This meeting took place under the Dutch Presidency of the European Union (January - June 2016) and was an initiative of the Dutch Cyber Security Council. Experts from the public, private and academic sectors discussed themes such as the Internet of Things and the Harmonization of duties of care within the EU, both major developments that require attention within the EU.

In preparation for this discussion, each participant composed a paper on both topics. Based on these papers and the discussion, recommendations have been drawn and will be presented to the European Commission. In this report you will find a summary of the papers, the recommendations to the European Commission and the papers we have been given permission to publish.

The Internet of Things

"The Internet of Things (IoT) will change society in ways that we cannot imagine yet," says security expert Bruce Schneier in Forbes business magazine. He argues that the IoT will become the greatest robot in the world. This robot will collect all sorts of information, and will act in an autonomous way in due time. Thanks to IoT a sort of internet-robot materializes, with senses, the ability to think and to act. "We are building a global robot that is not equal to anything else and we don't even know it. IoT will change everything, but we shouldn't let us astonish too much by these rapid changes." This view is consistent with that of Daniel Burrus, as he stated in Wired magazine: ''the Internet of things is much bigger than everyone thinks, because the focus is too much on machine-to-machine communication. This is only part of the story," says Burrus, ''because it revolves around IoT sensor-to-machine communication and vice versa. Sensors collect data, but you can't use them if there is no infrastructure available to analyse these data in real time. IoT brings sensors and equipment together and helps develop new smart products and services''.

Disruptive change

With the IoT, the online connectivity of applications, systems, surfaces and environments has increased. This is a major and fundamental change in our society. It is one of the most disruptive technologies in our time that offers many opportunities, similarly to the rise of the Internet. Our society will permanently change with the IoT. Success in the domain of IoT and taking advantage of the opportunities to improve prosperity, living comfort, health-care, operational efficiency and innovation has its price. The IoT is not only the connecting of smart devices and the analysis of data through the cloud, the IoT also calls for a need for security, privacy and trust.

Dick Schoof

Eelco Blok

The Three main pillars

Security, privacy and trust are the three main pillars upon IoT should be built upon. If we look at security, we see that many IoT devices and sensors entail new cyber security risks. The fact that devices are becoming increasingly interconnected, it creates new dependencies and, and thus reveals new vulnerabilities. Manufacturers are in a competitive “rat race” to launch new products to the market, causing some to pay less attention to the security of their hardware and software.

Concerning the second pillar, privacy, we see that more and more data are being collected and analysed. It is important to ask if consumers know what their personal data is being used. Do consumers have control over their personal data? is it possible for them to intervene? or is this control out of their hands?

The third pillar of IoT, and possibly the most important one, is trust. Users of IoT devices and services should be confident that the software and the hardware components are secure enough to be used for the purpose that is intended. If this trust is not consistent, and consumer feel that their data are being misused or that they might be impacted negatively, consumers will turn sway from IoT technologies. This effect would be detrimental to the economic growth of this market and to the possibilities for innovation.

These questions and potential negative consequences provide amble reasons for the need to discuss the future of the Internet of Things and figure out how the different sectors in society can benefit from this new technological phenomenon while at the same time ensuring high levels of cyber security.

Harmonizing duties of care in the EU

Establishing confidence in the IoT is possible with good regulation and a sense of responsibility for cyber security. Individuals, and society as a whole, will become increasingly dependent on IoT devices and services in the coming years. Disruption and misuse of hardware and data can negatively impact its users. The responsibilities of governments, industry and end-users should be clear in order to take adequate cyber security measures and show how they are accountable when incidents occur. Currently, it is not easy to clarify these duties of care within the EU because Member States have different laws and regulations in this domain. This fragmentation leads to legal uncertainty, in particular in the business community, which has an inhibitory effect on the development and advancement of IoT technology. Due to these reasons, the harmonization of duties of care within the EU is of key importance during this meeting.

EU Foresight

Within the EU, it is acknowledged that there is a need for forward-looking, strategic advice on new technological developments, and on cyber security issues and measures. The European Foresight Cybersecurity Meeting is an occasion to provide certain advice. The public, private, and academic composition of this meeting, the subjects of the Internet of Things and the Harmonisation of the duties of care within the EU were discussed from various points of view. This approach proved to be valuable in the collection of insightful advice that can be incorporated into EU policies and regulations. It is important to note that all participants were positive about this multi-stakeholder approach.

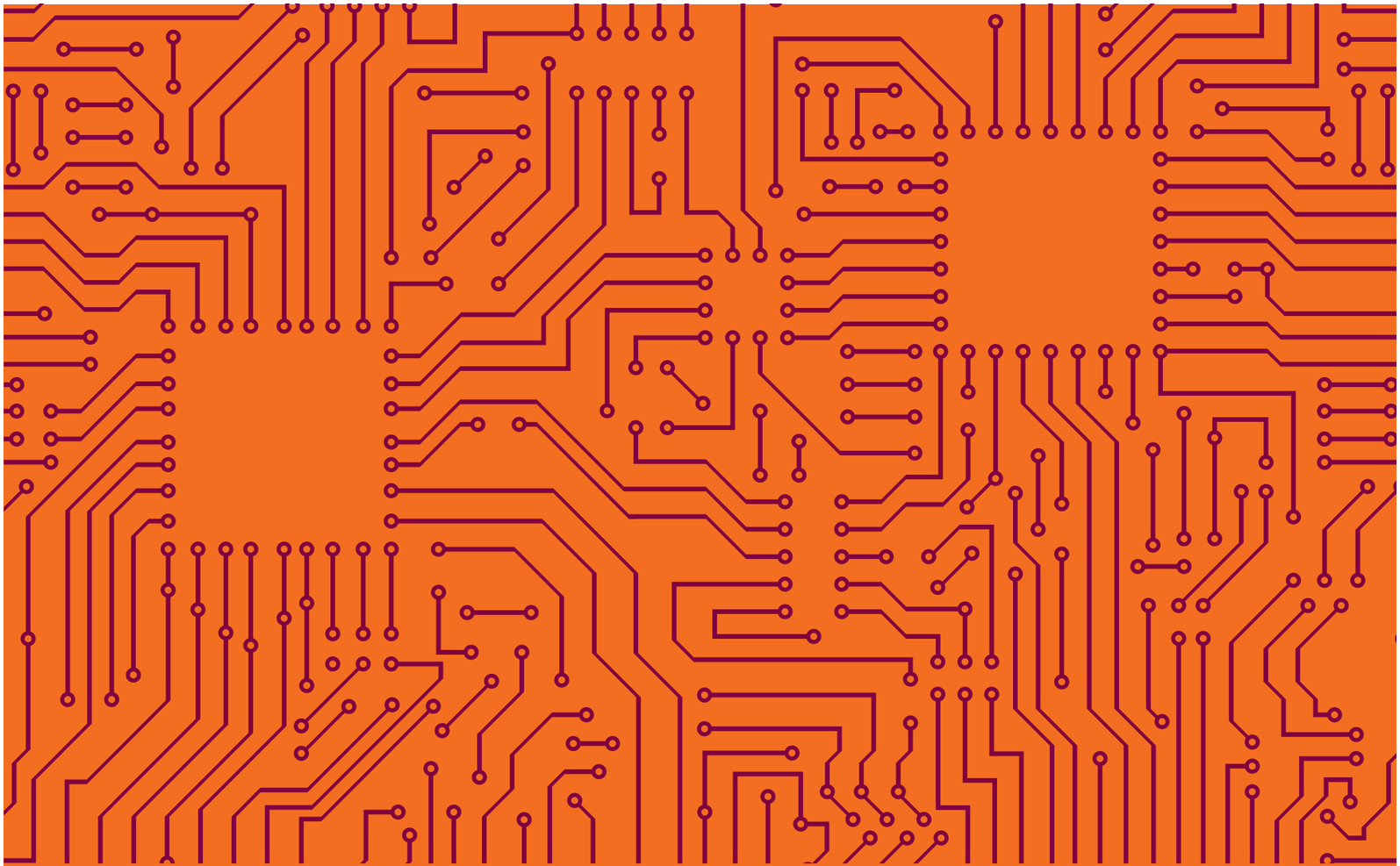
We hope that the EU Foresight Cyber Security Meeting in public-private-academic composition can continue to exist as a platform and will give both solicited and unsolicited advice to the European Union when it comes to matters in cyber security. We express the wish for the European Union to adopt the conclusions and recommendations of this First European Foresight Cyber Security in its policies, laws and regulations and legislative proposals.

Dick Schoof
Co-Chair

Eelco Blok
Co-Chair

CSR Cyber Security Council

The Dutch Cyber Security Council (CSR) is the independent advisory body to the Dutch Cabinet when it comes to strategically relevant developments in the field of cyber security. The Council looks forward, signals what is coming to the Netherlands and gives solicited and unsolicited advice to take measures in anticipation of the regular policy. The CSR is composed of eighteen senior representatives of public and private organizations and academia. They are committed to increase the level of cyber security in the Netherlands and Europe.

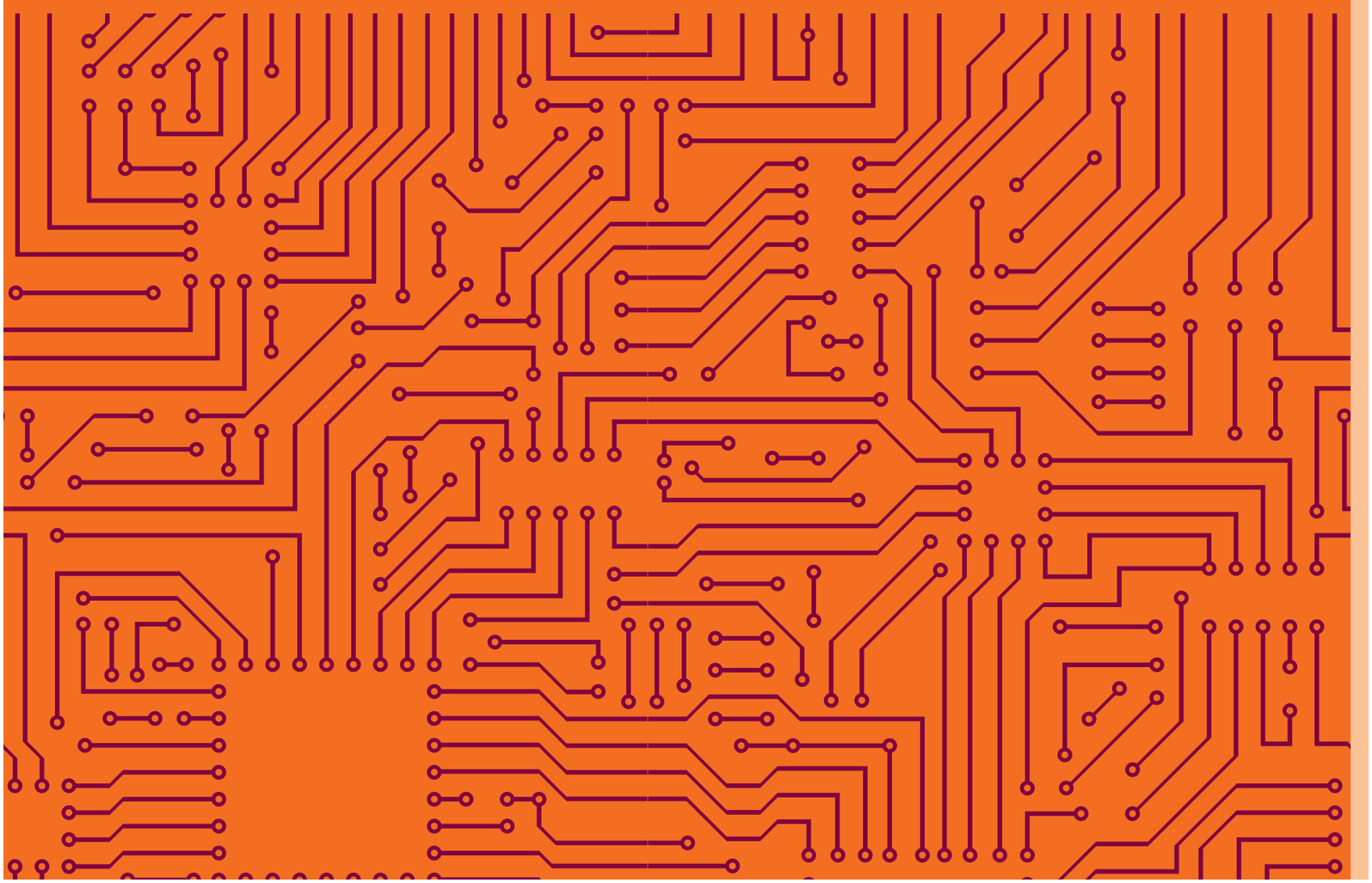


PART 1

RECOMMENDATIONS TO THE EUROPEAN COMMISSION

INDEX OF PART 1

2 PARTICIPANTS OF THE EUROPEAN FORESIGHT CYBER SECURITY MEETING 2016



Ulrich Seldeslachts
CEO, LSEC
Member of the Belgian Cyber Security Council

Jesper Aarup
Partner, Director eCrime
CSIS Security Group

Morten Gade Christensen
CIO, Energinet DK

Steve Purser
Head of Core Operations Department
ENISA

Paul Timmers
(personal contribution)
Director Digital Society, Trust and Security
DG CONNECT
European Commission

Philipp Amann, MSc
Senior Strategic Analyst
Team Leader Strategy and Development
European Cybercrime Centre, Europol

Daniel Shepherd
Chief Marketing Officer, S21sec
Chairman, European Cyber Security Group (ECSG)

Ryan Budish
Senior Researcher
Berkman Center for Internet & Society
Harvard University

Leon Strous
President
International Federation for Information Processing (IFIP)

Maarit Palovirta
European Regional Affairs Manager
Internet Society

Koen Gijsbers
General Manager
NATO Communications and Information Agency

Benedikt Abendroth
Jochem de Groot
Manager Government Affairs
Microsoft

Paul Verbruggen
Business and Law Research Centre
Radboud University

Pieter Wolters
Business and Law Research Centre
Radboud University

Ilias Chantzos
International Government Affairs Leader
Senior Director Government Affairs EMEA, Global CIP and Privacy Advisor
Symantec

Danil Kerimi
Head of Digital Economy and Technology Policy, ICT Industries
World Economic Forum USA

The European Foresight Cyber Security Meeting 2016 is an initiative of the Dutch Cyber Security Council. Participants:

Dick Schoof
National Coordinator for Counterterrorism and Security
The Netherlands
Co-Chairman Dutch Cyber Security Council

Bart Jacobs
Professor of Computer Security
Radboud University, Nijmegen
Member Dutch Cyber Security Council

Lokke Moerel
Senior of Counsel Morrison & Foerster LLP
Professor Tilburg University
Member Dutch Cyber Security Council

Jos Nijhuis
CEO Schiphol Group
Member of the Dutch Cyber Security Council

Elly van den Heuvel
Secretary of the Dutch Cyber Security Council

Organization and support:

Eline Attema
Adjunct-Secretary and policy advisor of the Dutch Cyber Security Council

Martin Bobeldijk
Communications Advisor Dutch Cyber Security Council

Special thanks:

Carlijn Hofland
Ministry of Security and Justice

Tuomas Tiihonen
Leiden University

Pauline Hutten
Leiden University

Administrative Support:

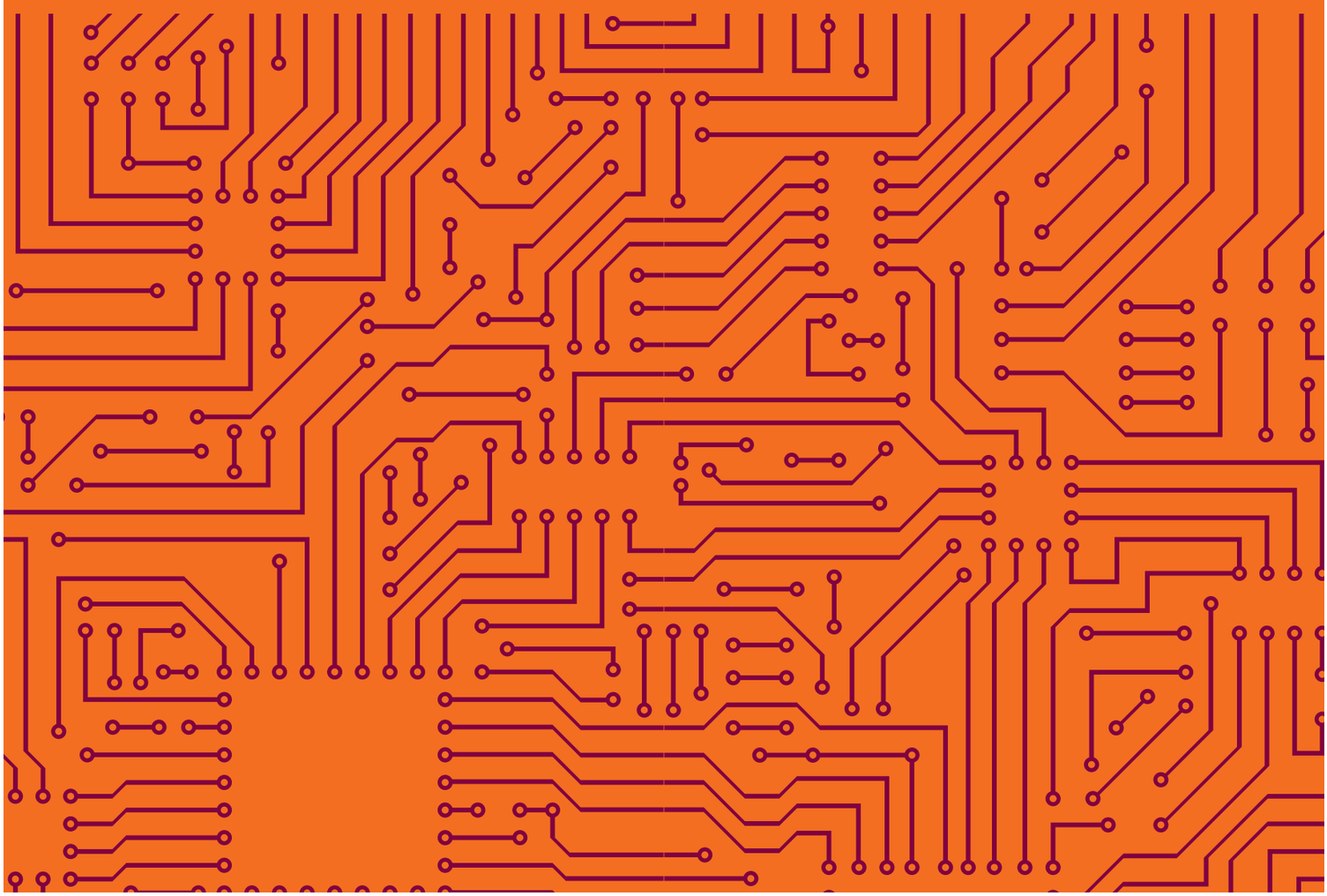
Sandra Minnaard
Ministry of Security and Justice

Hans Altimari
Ministry of Security and Justice


EU
2016


Conclusions
1. Emphasize the value of
non-connectedness
+ the right of choice
limitations to connectivity must be possible
(don't let it become
+ the
2. Let the market do the
work in setting
3. Defend European values

3 THE INTERNET OF THINGS FROM A CYBER SECURITY PERSPECTIVE



The Internet of Things (IoT) is a development that affects all areas of our economy and society. Everyday objects are becoming connected to networks and databases and are beginning to exchange data. With the IoT, the possibility to combine physical objects and the virtual world is on the rise. The IoT brings opportunities, such as living comfort, operational efficiency, innovation (e-health for example) and it creates new forms of employment.

With these opportunities also come certain risks and dilemmas. This brings up the question of what the possible actions are to facilitate the rise of IoT technologies and to mitigate their risks to an acceptable level. Failure in answering these questions and allowing IoT technologies to develop without supervision will make it more difficult to guide the safe implementation of these technologies.

The main risks of the IoT are in regards to security and privacy. According to the paper of the Dutch Cyber Security Council, these perceived risks can be clustered into five categories:

1. Manageability
   The IoT playing field is vast, limitless and has a complex composition of international, national and regional contributors, making it difficult to shape their controllability.

2. Lack of security incentives
   There is a lack of incentives to produce secure hardware and software, and to ensure they are adequately maintained.

3. Impact on behaviour
   The amount of data on human behaviour is a new form of intelligence, which influences human behaviour without notice and without the underlying transparency of interests.

4. Surveillance and industrial espionage
   The large number of devices that will be connected to the Internet in the near future presents new avenues for communication to be intercepted and monitored by governments and malicious parties.

5. Big Data and privacy
   It is currently unclear whether the data collected by IoT devices are covered by existing data protection laws.

Various perspectives can be explored in order to facilitate the benefits and opportunities of IoT technologies and mitigate their risks. These perspectives are described in the report titled: ‘The opportunities and risks of the Internet of Things: Perspectives for Action’ written by the Dutch Cyber Security Council.

Outline papers

The authors of the briefing papers share a wide consensus on the scope and scale of technical, socio-technical and economic implications brought by the emergence of the Internet of Things.

Technical significance

The submissions revealed that the technical significance of the IoT is understood in a fairly uniform way by all participants. The number of connected devices facilitates the exponential growth of more dynamic and complex networks, requiring a more adaptable network infrastructure and consequently facilitating further steps towards ubiquitous connectivity. Primitive devices without encryption and security functionality pose additional requirements to the network infrastructure for a basic level of security to be provided regardless of the device's capabilities. Added complexity and heterogeneity in connected devices and increased dynamism in networks are also viewed as fertile ground for wider targets and additional attack vectors for malicious operators.

Socio-technical implications

The socio-technical implications of the IoT are generally regarded positively, albeit heightened security requirements and concerns for data manipulation on devices that provide decision support feature prominently in the submissions. In the established cyber security triad of confidentiality, integrity, and availability, the importance of integrity will increase as data gathered from the devices will be used for decision support both automatically and through a human filter.

The increasing role of the individual users (the human factor) as the first line of defence in an increasingly complex cyber security environment is acknowledged as impetus for educating the users more extensively. In essence, the gradual loss of perception of network topology and the amount of diverse connected devices contribute to overwhelming the average user, who usually acts also as an administrator of their local network, but rarely has the knowledge to execute more advanced tasks even in the current environment. Trust on the delivery of expected levels of privacy, data protection, and security of the IoT is essential for swift adoption of the new technologies and early realisation of the opportunities foreseen for both the industry and the users. Educating the user is seen as a way to foster trust in IoT technologies.

Security, data protection and privacy by design and by default are offered in multiple submissions as guiding principles for device and software design. While the principles are understood quite clearly, especially in the framework provided by the EU General Data Protection Regulation, the implementation of the principles in a uniform way is regarded as a challenge. Any further legislation should be designed with sufficient adaptability to keep up with innovation and technological development.

Law enforcement, military opportunities and concerns with the cyber security of the IoT are closely aligned with viewpoints put forward by industry, as attacks against the private sector can have negative implications on national security. Cooperation of all sectors through fora facilitated by the government is essential for building a secure and resilient cyberspace. Law enforcement-specific opportunities derived from the combination of the IoT and Big Data include predictive policing based on quantitative analysis, and better threat detection and prediction. The added complexity and diversity poses special investigative challenges for law enforcement in cross-border cooperation and data extraction.

Economic opportunities

The economic opportunities of the IoT are found directly in the development of secure software and devices, and in facilitating the flawless operation of IoT technologies, such as educating users and providing outsourced services in general. More specific opportunities in the service sector are identified in data analytics, algorithm development, vulnerability identification, and authentication and identification of the devices. Economic considerations in product development, like the importance of first-to-market and maximisation of short-

term returns, are a source of concern if they are competing against creating secure products. This underlines the importance of global standards for the minimum level of security required from IoT products. The European industry is well placed to become world leader in cyber security and IoT, and standardisation of the minimum level of security would enhance the competitiveness of the market with the most encompassing privacy and data protection laws.

The Internet of Things is an emerging topic with enormous technical, social, and economic implications. It plays a crucial role in new types of critical infrastructure, advanced public policies, accurate data, effective business processes by facilitating aggregation of data from different sources and exploiting new connections. Besides a growing amount of connected devices, it is likely that the complexity and diversity of the IoT will further increase. Consequently, the exponential development and deployment of IoT also presents major challenges for cyber security. Due to this, interdisciplinary partners from both public and private domains should cooperate and coordinate on current and future security issues, such as monitoring of the evolution of cyber threats, implications of the IoT and design choices. The new and vulnerable character of the IoT requires on-going dialogue on topics such as the balance between risks and costs, between all stakeholders of the early stage of this fast moving industry.

Role of the European Union

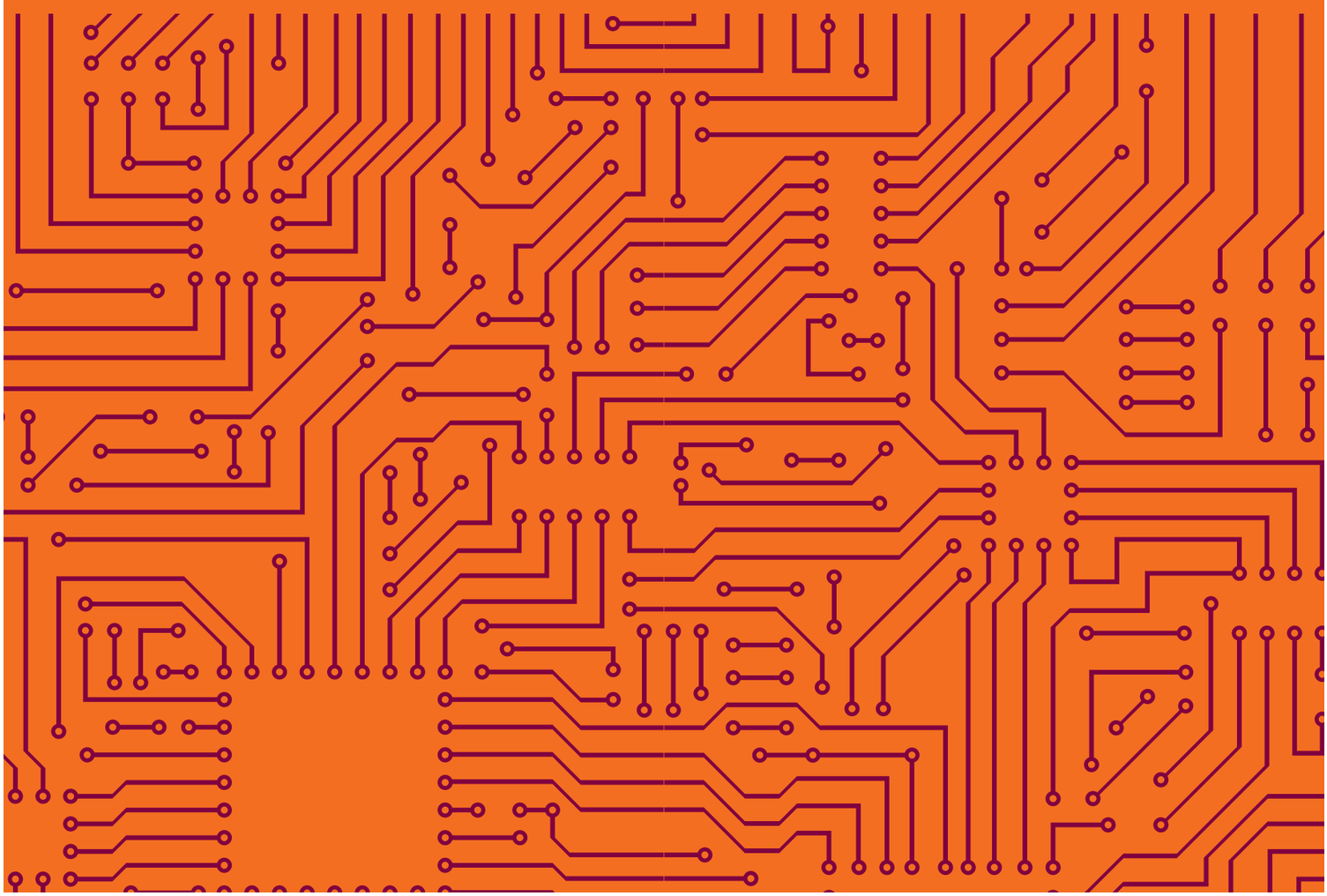
It is commonly understood that the EU is an important actor since it deals with both the source of demand and the system of solution providers. The submissions differ considerably on the general role envisaged for the European Union in the creation of a safe, economically conducive, and secure IoT technologies. The EU is perceived as an educator; facilitator of research and provider of fora for discourse; initiator of standards, certifications and labels both internally and on an international scale; legislator, regulator, co-regulator, and facilitator of self-regulation; the public actor in a public-private-partnership; and the creator of economic opportunities through the Digital Single Market.

Public-private partnerships have been selected as a main approach of the EU to aligning interests of a wide variety of stakeholders and develop an environment that fosters development of a thriving IoT industry. A requisite level of regulatory and legislative activity is envisaged to complement the partnership. It should be noted that the Alliance for Internet of Things Innovation (AIOTI) is rarely mentioned in the papers as an important venue for stakeholder cooperation, while the EU has envisaged it as such in the IoT public-private partnership.

Internal and international standardisation is also seen as a crucial activity pursued by the EU, though views differ on the role of the Union in this activity. Recommendations are made for both a supporting role in market-led standardisation and an a more prominent agency in establishing (global) minimum standards for security. Voluntary certification of products and granting of security labels would offer a way to build trust on products with a high level of security.

Emphasis is placed on the Union's ability to pre-empt diverging national legislation to IoT and cyber security by harmonising the policy space. This would ensure the creation of a level playing field for the IoT industry in Europe, enabling it to compete more effectively against other large markets with harmonised policies.

4 NEED OF HARMONIZATION OF DUTIES OF CARE WITHIN THE EUROPEAN UNION



The multi-stakeholder and cross-border nature of Internet of Things has fundamentally changed the scope of responsibility and accountability of organisations in relation to their customers. This has raised a discussion for the need to harmonise legal standards for duties of care and diligence in cyber security. Duties of care are the legal obligations to act with due care or use professional diligence towards the legitimate interests of others.

The increasing dependence on ICT goods and services in today's society emphasizes the need to ensure their security. ICT is responsible for economic growth in Europe and is at the core of daily life. With these positive developments also come with an increasing risk of ICT dependencies, disruption and failure as well. The question arises on who is responsible for ensuring cyber security and cyber resilience. This is not an easy question to answer as government, consumers, ICT providers, companies all have an equal stake in this field.

Legal uncertainty

There seems to be a considerable amount of legal uncertainty as there are limited and very diverse legal frameworks for duties of care in the EU Member states. Individual users frequently find themselves confronted with serious legal obstacles that prevent them from bringing a claim against ICT providers who are neglecting their duties of care. Citizens who have suffered a loss because of lack of cyber security should have effective legal remedies against the actors responsible for providing the service. At the moment, the legal implications are too complex to enforce this.

Structural disadvantage

It is important to consider the influence of commercial competition, politics and personal motivation on fostering confidence in the Internet and on ensuring the continued success of the Internet as a driver for economic and social innovation. Existing legislative instruments of the EU provide a framework for introducing harmonised duties of care through product liability. If the risks of the operating environment for a product cannot be known in advance, a security-centric solution would be to apply a high level of security on all products as a default, even if this would come with costs to the ease of use of the technology.

Security by design

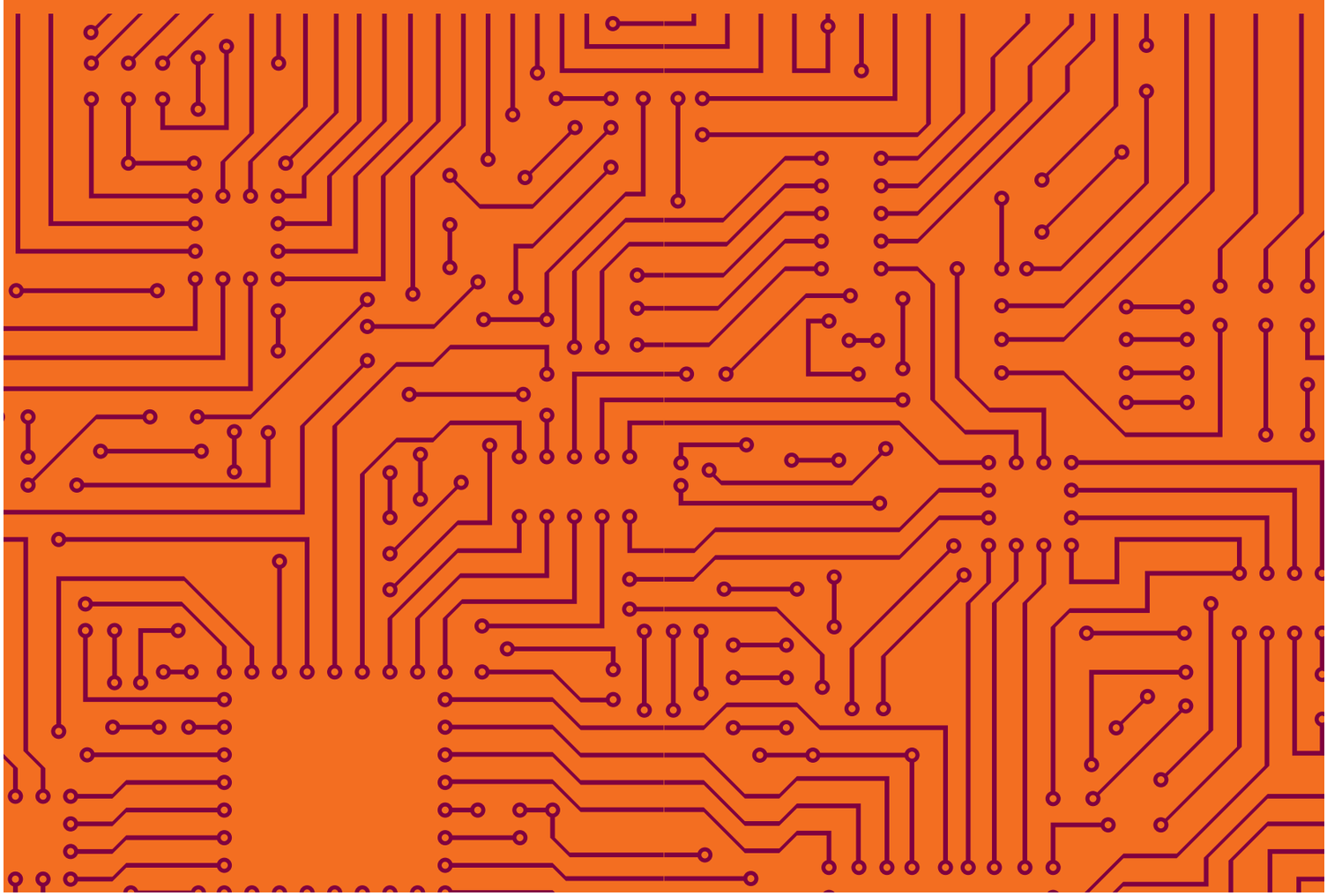
Consider for instance the task of security by design as viewed by the software developer. To a large extent, the degree to which the product will need to be secured will be dependent on the operating environment in which it will run. In other words, when the target environment is not known, software developers have to deal with *threats* and not *risks*. One way to deal with this issue would be to implement a high level of security on all products as the default approach. Unfortunately, however, this is likely to be very costly and may kill the business case for many IoT technologies. If security is not to be a barrier for the deployment of emerging technologies, the concept of security by design will have to incorporate trade-offs such as these and the duties of care will also have to be applied with these considerations in mind.

A harmonized legal framework

When the EU launched the strategy for the Digital Single Market, which included cyber security, it also produced Directives on General Data Protection Regulation and Network and Information Security, to strengthen the protection of consumers. However, the general legal framework in the EU that applies to the sale of goods and services from ICT providers to consumers was not covered properly. Fragmentation is still a major issue. A single market following international standardization is necessary to ensure a consistent approach to the IoT and cybersecurity. The development of national efforts that would lead to further fragmentation should be avoided, as it could hinder IoT technologies to unfold its economic and social positive impact.

Since it is very important for Member States to increase economic growth and maintain a levelled playing field between them, the Dutch Cyber Security Council has asked Radboud University to write a White Paper on this subject (see appendix), to provide an advice to the EU on the harmonization of legal frameworks and to help drive the Digital Single Market for the IoT and cyber security.

5 RECOMMENDATIONS ON INTERNET OF THINGS



According to the submitted reports and the discussions at the European Foresight Cyber Security Meeting 2016, follows the conclusion that cyber security issues of the Internet of Things often have a link with human behaviour. This means behavioural changes are not only necessary for governments and private industry but also for consumers. Another conclusion was that all participants recognize the need for harmonization of duties of care in the EU. The participants noted that the current legal frameworks are abstract. This situation creates room for legal uncertainty. Currently, courts in different EU Member States have differing policies regarding cyber security and IoT technology issues, creating legal fragmentation within the EU.

The participants of the European Foresight Cyber Security Meeting 2016 are willing to make the following recommendations to the EU and its Member States about cyber security issues related to the Internet of Things.

Standards and labels

1 Develop an EU baseline for security around key components of IoT infrastructure and various standards for various components of IoT such as interoperability and connectivity as a part of the Digital Single Market.

- Develop IoT standards within sectors and supply-chains and publish requirements where there already is a consensus. The dynamic character of the IoT and the development of new technologies should be internalized.
- Adoption of regional and global standards can contribute to a greater advantage in exporting goods worldwide.

Harmonization of Duties of care

2 Create harmonization of duties of care among relevant partners and prevent fragmentation between countries through standards at EU level.

- The frameworks for duties of care should address the profession and professionalism, and the duty of care should be an element in such a framework since codes of conduct and codes of ethics are part of a profession. As a starting point, The EU could encourage Member States and businesses to establish such frameworks and give guidance on the minimum acceptable requirements.
- Since the development and production of IT systems and the threats to them are not limited to Europe, it is important to have a long term vision on duties of care.
- Requirements and frameworks will be aligned, within the EU but also on a global scale. Until frameworks are aligned, courts should address duties of care and develop case laws. Best practices should be developed and used as examples.

European values

3 Defend European values in the digital world and promote them.

- Citizens should have the freedom of choice to be connected to the Internet of Things. They also should have the right not to be disconnected from the Internet of Things. Citizens must have access and control over their data.
- Stimulate the development of open source software. Evaluate this software structurally within the EU so that it can be further improved and professionalised. The creation of seed funds should be made available for open source software developers.

Public-private-academic partnership

4 Strengthen the public-private-academic partnership. This partnership is indispensable in the effort to increase the level of cyber security within the EU.

- Encourage public-private- academic cooperation within the Member States with regard to cybersecurity issues. The contribution of young people here is highly desirable.
- Facilitate and encourage the sharing of knowledge and information between sectors and communities that deal with cyber security at all levels (horizontal) and between the different levels (vertical). Ensuring confidentiality is crucial.
- Encourage the exchange of results from research and development projects within the EU Member States, governments, businesses and academic institutions and use it for targeting policy.
- Enter Responsible Disclosure mechanisms in all Member States and include the ethical hacker community to raise standards to achieve a higher level of cyber security within the EU Member States.

Incentives

5 Develop incentives, make the industry adopt cyber security measures and apply the concept of security-by-design. Supervision of this process will be needed.

Possible incentives:

- Finance: non-compliant organizations should be met with fines, legal fees and general “naming and shaming” (reputation).
- Cyber Hygiene: Organizations should be encouraged to develop a dashboard that will help them monitor their processes and show how cyber secure their operations are.
- Community: Citizens in their respective communities should be incentivized to review the security standards of their devices, software and the organizations providing services.
- Oversight committees: strengthen the role and expertise of oversight committees so that they can initially have an advisory role on cybersecurity issues before proceeding to take enforcement measures.
- Uniform rules: At the moment, not all EU Member States have implemented cyber security related EU directives, and there different interpretations of these directives.
- Compliance: Compliance with standards and obtaining certificates for larger EU market positions companies in a privileged position.
- Competitive advantage: Cyber security is turning into a differentiator that can be used as a competitive advantage for companies in the EU and globally. The EU can take the lead in the field of cyber security with the right incentives.

Interrelationship

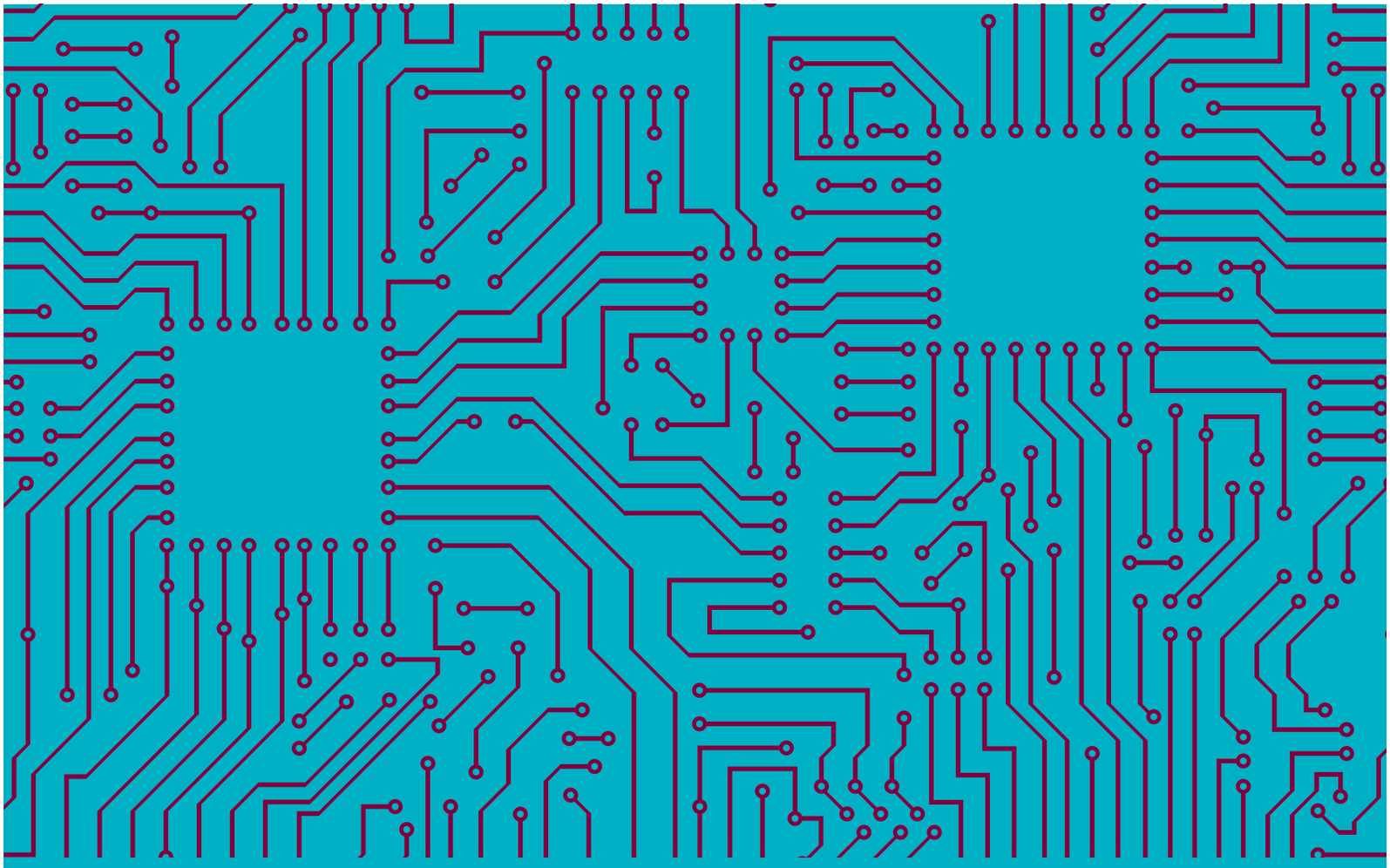
6 Team up and work together in creating interrelationship between all the relevant players in the area of the IoT and prevent fragmentation within the EU and within the EU Member States themselves.

- The topic of cyber security is fragmented across multiple European organizations and bodies in the Member States. Policies should be solidified so more organizations can work together as a team in the same direction.
- The coordination of EU and national organizations dealing with cyber security issues should be improved. They should also exchange solutions and best practices, so that everyone with the same information operates according to the same guidelines.
- Boundaries between Member States are a reality. We need more discussions between different communities, opening them up and making sure we achieve interrelationship of ideas. This would further stimulate the efforts to achieve a competitive and innovative EU.
- Thought leaders should be grouped at the Member State level to start initiatives in the area of IoT. Successful initiatives should be considered for implementation at a wider EU level.

Awareness and education

7 Invest permanently in awareness, education and information campaigns targeted at young and old, so citizens and small, medium and large companies can better assess cyber risks.

- The public attitude towards cyber risk is changing. Citizens show more interest and are concerned about their digital security. In this context, education and training are important for people to better understand the value of their online safety and take appropriate action.
- Governments and companies should be made aware of this changing attitude. They should be encouraged to be transparent about their cyber security practices. Prior to this, they should be aware of their risks so they can take action and prepare preventive measures in the event of an incident. Companies should know what is at stake for them and for the European market. Collect best practices and communicate these within the EU.
- A sector or industry leader should be encouraged to take responsibility and create momentum for action. This approach can be quicker and more efficient than taking a legal approach.



INDEX OF PART 2

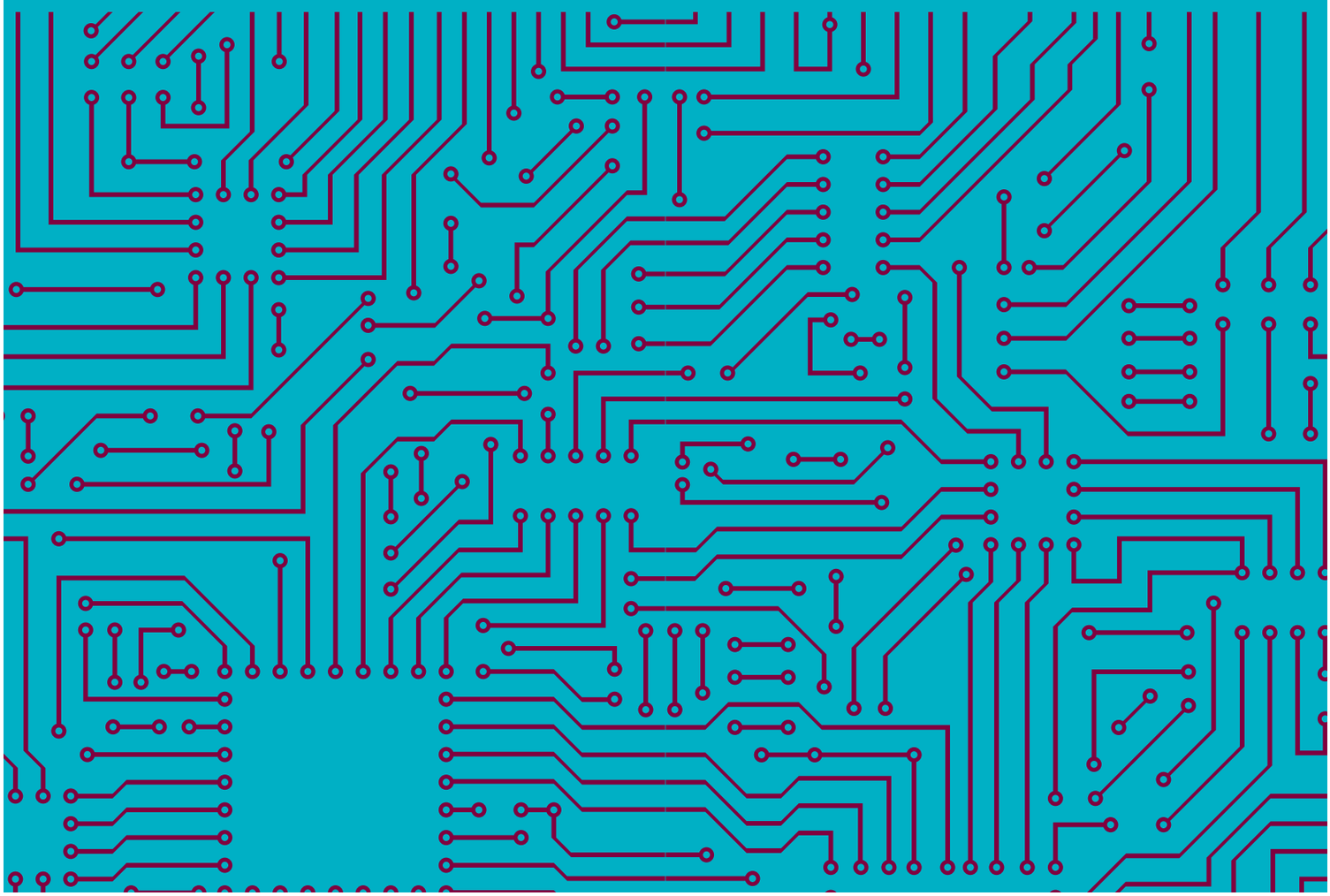
PART 2

FULL PUBLICATION OF THE PAPERS*

* We only publish the papers which we have received permission for.

1 FORESIGHT CYBER SECURITY IOT - A VISION PAPER FOR CYBERSECURITY PROFESSIONALS

Ulrich Seldeslachts
CEO LSEC
Member of the Belgian Cyber Security Council



INTRODUCTION

This paper was created in reaction to the call for a "short paper Internet of Things and duties of care, foresight Internet of Things", to prepare the first European Foresight Cybersecurity-meeting

About the authors:

LSEC – Leaders In Security is a European industry association of ICT Security companies, an IT Security cluster bringing together over 230 security technology companies, system integrators, advisory services and research centers from Europe and around the world; connecting to over 7000 ICT Security professionals. The cluster facilitates thought leadership and innovation in Europe by means of joint industrial projects and activities promoting the use of ICT security measures and activities.

3IF is an LSEC led initiative to promote the development of the digitalization of industrial automation and manufacturing by utilizing IoT, Industrial IoT, Industrie 4.0, Industrial Internet, FiWare and other technological advances. It focuses on the opportunities for factories in the first place, but extends into other sectors and has a main interest in applying ICT security measures in processes, technologies and services provided.

IOT PERSPECTIVES FOR THE EU

What possible action perspectives do you see for the EU to facilitate the chances of IoT?

1. Support Market Uptake

a. Continue to support EU wide, regional and local use cases for various vertical markets, showcasing benefits for IoT use and supporting local expertise in discovering opportunities and challenges
b. Facilitate the uptake of IoT
c. Continue supporting R&D funding in general IoT (ICT) developments, specific industry related IoT initiatives (FoF, Cloud, Digital Security, Transport, …) and use case developments
d. Support initiatives allowing for further industry alignments and reduction of fragmentation (IoT, Industry 4.0, FiWare, Smart Home vs Smart City, …)
e. Continue to support and further intensify the AIOTI, to ensure a better collaboration amongst industry and research, trying to align various industry standards under development
f. Allow for industrial development kits, such as Netduino or Raspberry Pi-alikes for industrial purposes to be taken up swiftly, with low cost use cases and examples
g. Provide transformational support, advisory packages on a local basis beyond the technology, facilitating easy to go Proof of Concept uptakes in various vertical sectors

2. **Support Security Advancements**

    a. Provide sensible use cases (for security) (walled garden, home proxies, transparent eco-systems, …)
    b. Drive towards end-to-end security
    c. Provide solutions for basic IoT (security) challenges such as authentication and privacy preserving technologies
    d. Speed up security by design & privacy by design principles.
    e. Ensure transparency
    f. Conceive and develop solutions towards patch management and updating IoT on all layers
    g. Allow for security monitoring services developments for IoT to develop, without the constant challenges of the GDPR and local privacy protection regulatory frameworks as inhibitors

3. **Support development of Core Technologies**

    a. Advance in r&d for fast and efficient handover in between low-power local area networks and amongst wide area networks
    b. Identify on a regular basis core European assets – expertise – initiatives and support those on a European-wide level, such as specific technology platforms, industry capable devices, core computing engines, the use of development kits
    c. Support development of a European cloud infrastructure capable of providing trustworthy cloud offering for IoT devices, both in wide are Cloud and Fog / Edge Networks

4. **Promote European IoT expertise and facilitate its uptake in Europe and abroad**

And what can be done to mitigate or reduce it to acceptable levels of security risks?

1. Ensure high common standards in baseline security (such as the industrial internet architectures or , and improving them rapidly over time,
2. but not simply adding standards over standards, as technology standards by themselves cause an additional security risks, amongst other:
    a. standards are always outdated, whilst vulnerabilities can be exploited quite fast when found. It takes reasonable time for standards to adapt in this case
    b. standards by definition allow technologies to be integrated and due to this openness, they present external risks, and vulnerabilities
3. Increase the capability and the ability for monitoring and active defence activities, allowing for near-real time analysis also on operational systems and allow for automated mitigation actions and reactions following suspected threats and identified vulnerabilities

What developments do you see in the field of Internet of Things?

Developments are happening **on every level in the society and every layer of technology.** There is an **increased awareness and acceptability**, and an **increasing level of expectation** for things to be smart.

Standards are developing rapidly, fragmentation is everywhere. Expectations are being exceeded in some applications and remain unsatisfied in other. Huge discrepancies in pricing on the same functionality exist. Transparency is missing and leading to distorted markets and missed opportunities.

IoT is still today on the top of the hype cycle, not yet hitting mainstream as IoT itself, but many descriptions are trying to apply the same general description with smart home, smart cars and smart everywhere; which do not always utilize the Internet as a transmission carrier, or even data source (as would be the case for smart watches).

IoT means different things to different people and sectors, even with base definitions common, due to the many applications, expectations and different sectors, IoT has different perspectives ranging from a mini-token to serve as identifier up to a connected car, with dozens of different sensors and actuators. The complexity and requirements of both of course differ significantly. The generalization is also happening as a result of definition by both industry, research and policy makers; but a more specialized, sectorized or even application approach should be considered.

What economic opportunities brings Internet of Things according to you? Think of opportunities in the areas of innovation, comfort of living, industry analysis, cost reduction etc.

For the ICT Security market in general, IoT brings a) opportunities for additional sensors and actuators acting in line, but also independently from the current network and application architecture. These are opportunities, in that they could provide additional intelligence, but also that they could help remediating some of the challenges in ICT Security maintenance. In addition, all things will need to be equipped with b) monitoring applications, collecting and transmitting data to central monitoring solutions. These challenges have already been tackled by ICT security vendors as end point devices, but have not yet been applied to all different things. This trend has started with a series of intelligent appliances, which have seen the installation of security software solutions, including targeted IDS and firewall functionalities. Additional opportunities exist in the c) domain of in depth analytics, developing specific algorithms for specific applications, for specific sectors and functionality specific identification of potential vulnerabilities, next to the challenges of high volume data transmission. Finally, d) ICT Security challenges will need to be faced in terms of ensuring future-grade industrial encryption capabilities, both in low-power, 8 bit processors and high availability 32 bit or higher type processors, in environments where business continuity is of utmost importance. In the same context, challenges related to e) authentication and identification leave many issues unresolved. Current white listing techniques, will be enhanced with specific hardware token identifiers, such as being put into consideration by the Trusted Computing Groups. Moreover, all IoT devices and application vendors will have to consider f) mechanisms to ensure transparency in their security policies, applications and will need to allow external security applications to take over from boot level in order to ensure end-to-end security in some environments.

Once connected, the devices will be g) transmitting over various networks, which by themselves are being challenged with current and future security challenges, which have not yet been resolved. The data transmitted will likely increasingly be sent into h) cloud environments from sometimes remote locations. Cloud security techniques will need to adapt to sensors and actuators in the field, i) also requiring over the air remote management.

Can IoT be used strategically as a possible solution to major issues? If yes which one?

IoT is a strategic solution to **advance many legacy application** challenges. Systems being connected increasingly, which have not been developed with an always-on type consideration, can now easily be connected by implementing IoT. This allows for quick proof of concept cases, **showing immediate results and indicating quick ROI**. IoT can also strategically be used for new types of applications, which have been conceived in specific industrial environments offering new types of capabilities and opening up new services and capabilities. IoT is one of the key components to revolutionary developments in many industries, such as automotive, healthcare and manufacturing. Already in automotive some of these developments have been making significant process, in the last 12 months due to for instance the consumerization of the self-driving car by Tesla. Putting this in action, in combination with the regular updates over the air and constant improvements of the applications, presents drivers not only with ideas but also allowing to experience the model where IoT becomes strategically important, to develop a whole new service model of shared self-driving vehicle. In manufacturing IoT, in forms of sensors and actuators, is key in facilitating the Factory of the Future and Industrie 4.0 – Industrial Internet. Today sensors

support remote monitoring, preventive maintenance and increase safety on the production floor. The produced goods themselves, being equipped with similar functionalities allows manufacturers to explore new business models, reaping the benefit of utilizing data which was available but never being put to use before. Examples such as Thyssen Krupp, show how a traditional offering of lifts and elevators, can turn around into a services oriented model. At Mars foods factories, candy bars can be made to measure in volume and end product, while the factory is maintained by the industrial automation suppliers.

FORESIGHT DUTIES OF CARE

Cyber Security is the sense of security and safety on the internet, similar to sense of security and safety in the physical world. This is partially taken care for because of the responsibility that citizens as persons or as organizations are applying, intentionally or instructed by law and regulations. It is the barrier between freedom and security that is being put under pressure on regular occasions as a social debate. Citizens and organizations carry responsibilities in ensure the freedom of the other, the balance is a momentary lapse of time that has to be dynamic. All actors should be having the capabilities in adjusting that balance accordingly and should therefor allow measures and systems to change these balances dynamically, throughout the whole supply chain of the digital world.

Technology providers should provide security measures, according to the State of the Art applicable in a certain timeframe. This SOTA can be identified on a periodic occasion, identified by an industry led-group of experts, supported by research and end user organizations, following frameworks set up by policy makers in terms of measures on identity, authentication, processes, controls, monitoring, security by design, end point protection, active defense, ...

Services providers should be taking up these security measures within a reasonable time, and act on top on a more social responsible level, taking care of their duties providing measures in “clean” information superhighways and sanitized host stations.

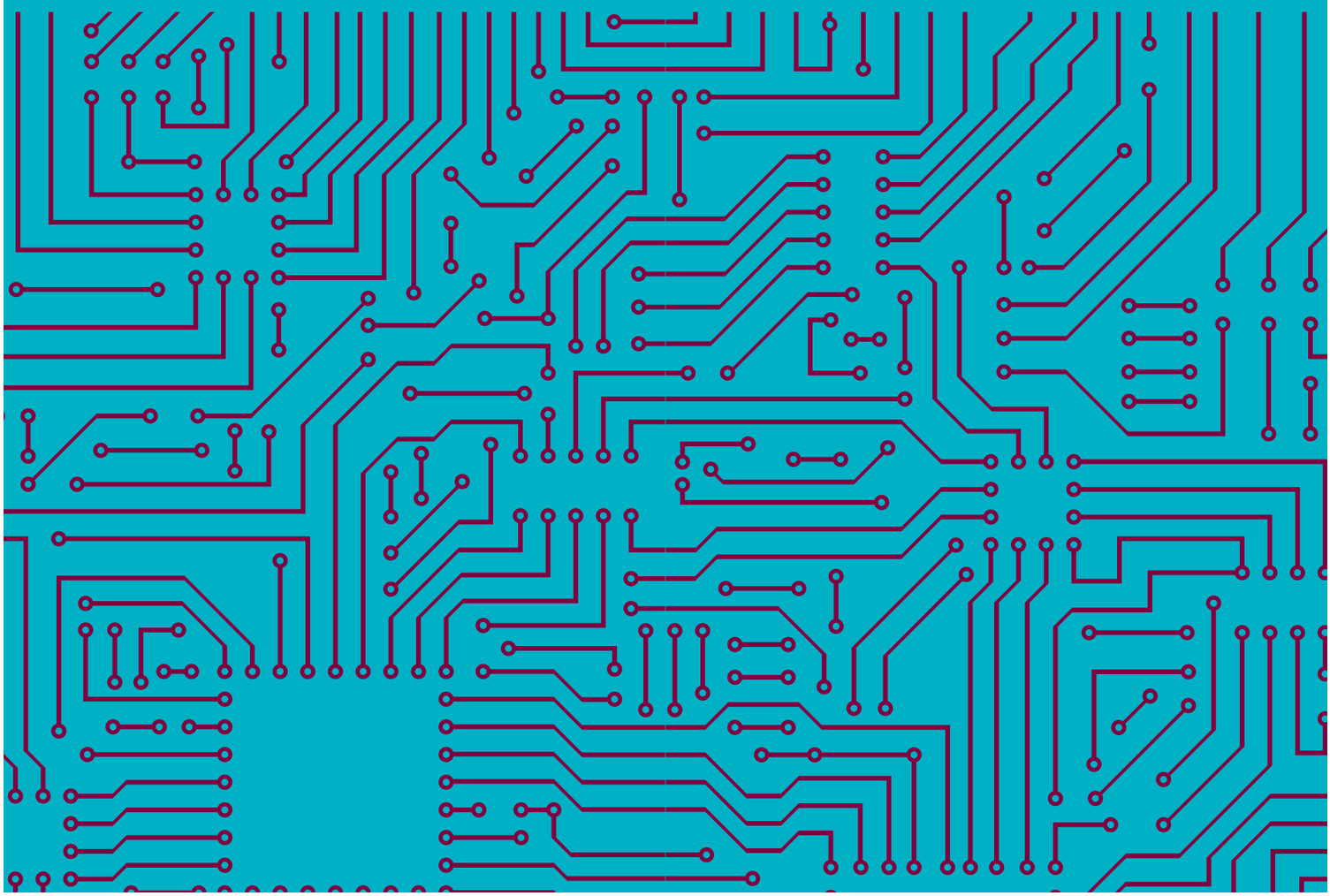
Prosumers and End Users from both corporate and personal level, should be made aware of their social responsibilities, their need for care taking similar to the fact that they have to sanitize public road facilities. An internet driver’s license could be both an inhibitor and a facilitator, but will in any case normalize the situation.

The current internet has been a free space for the last 40 years and should continue to be so. It does impact the freedom of some, because of others are abusing some of their internet social responsibilities. An overregulated regime will hinder the freedom, the free delivery of goods and services and the open market.

Organizing the debate and open discussion is the first step, having industries and organizations being stimulated to self-organizing should be a next step. Initiatives to this effect should be started and supported from a policy level. Initiatives should be studied and evaluated, and industry led, but evaluated and validated by research and prosumers and consumers.

2 SECURING THE INTERNET OF THINGS (IOT)

Dr. Steve Purser
Head of Core Operations Department
European Union Agency For Network and Information Security
(ENISA)



INTRODUCTION

This short paper looks at some of the security challenges associated with the development and deployment of distributed objects (often referred to as the Internet of Things). Ideas for resolving these issues are presented before examining to what extent the concept of 'duty of care can be applied to these environments.

SECURITY CHALLENGES

The main differences between the Internet of Things (IoT) and more traditional computing models are mainly technical in nature. It therefore makes sense to provide a few examples of the issues that developers and implementers of IoT will need to resolve in order to provide a level of security that will meet the expectations of the user community. This description is of course by no means exhaustive, but is offered in order to illustrate those security challenges that are particularly (but not uniquely) associated with the IoT model.

Scalability is undoubtedly the issue that is easiest to understand in this context. The Internet of Things can be thought of as a vast network of independent objects capable of talking to each other under certain conditions. The standard method for securing communications such as these, when they occur over untrusted networks (such as the Internet) is to use cryptography. Cryptographic services are used in this context for a variety of purposes, including authentication (knowing who you are talking to), protecting the confidentiality and/or integrity of the data exchanged (and sometimes to protect the integrity of the exchange itself, which is a slightly different concept) - cryptography can even be used to prevent actors from denying their role in a transaction - so called 'non-repudiation' services.

The most powerful cryptographic services however require the entities that are communicating to use keys, which need to be kept secure. This will be challenging where IoT is concerned, as there will be a requirement for a large number of such keys. In principle, each object will require its own keys, which implies (a) the need for a framework that is capable of managing these keys, (b) a consistent set of procedures and technical standards to support interoperability and (c) secure key storage for objects that will probably have a low cost in order to be competitive in the open market. All of these points are challenging even for current applications and become even more so in the context of IoT.

Another issue that will have to be dealt with is that of ownership and administration. A smart home could conceivably deploy a significant number of objects, supplied by different vendors (fridge, washing machine, thermostat, locks etc.), which is likely to imply a range of different interfaces for accessing the devices. In such a scenario, it is difficult to imagine that home owners will administer all these devices themselves – and, even if they do this, it will be difficult to achieve a coherent level of security across the home. The alternative model, where suppliers apply security patches and updates is also not without issues and presents supplier with similar challenges.

Security patches and updates are not only an issue for the consumer; vendors will also need to design update mechanisms and software distribution mechanisms for managing security that can successfully cope with the potentially large number of objects 'in the field', many of which may only be accessible over the network at particular times. In addition, over time it is to be expected that several different versions of an object will co-exist at any particular time and certain objects may need to be decommissioned after a certain period. All of this needs to be achieved in a structured manner with minimal inconvenience to the end user.

A common design assumption for highly distributed systems is that the user doesn't need to know where the object that is providing the service is located. Whilst this is true from a usability perspective, it is problematic from a security perspective. In particular, the location at which the storage and processing of data takes place will probably define the legal framework which applies. This is particularly important where privacy and data protection legislation is concerned.

Last but not least, for some objects safety will be a critical factor and mechanisms for ensuring the safety of the user will have to be developed alongside the security mechanisms that are used to protect the device. That this is not always straightforward was illustrated by the recent incident in which a pilot is believed to have used a security mechanism (security of the cockpit door) to gain control and deliberately crash an aircraft1. Where incidents do occur, it will not necessarily be easy to reconstruct the chain of events that led to the incident when several devices are involved, which will also complicate the process of deciding responsibilities and liabilities.

TOWARDS A SOLUTION

Correctly securing IoT environments will require developers and implementers to carefully balance several factors, some of which may be antagonistic in certain cases:

- Security measures will have to be correctly aligned with safety features.
- A sensible balance between cost and level of security will have to be struck. This balance will depend on the operating environment in which the object or device is expected to function.
- Where devices are expected to function in a variety of circumstances, the design of the device should allow for a level of security that will enable the device to function in the environment of highest risk.
- Security mechanisms should not impose unreasonable requirements on any of the actors necessary to make the model work. In particular, considerable attention should be given to expectations placed on the citizen as an end user.

Suggestions for achieving these goals include:

- Developing risk analysis and management techniques specifically geared towards the IoT environment.
- Incorporating the concept of 'security by design' into the software development lifecycle an systems integration methods.
- Optimising the level of granularity of security controls.
- Developing a coherent set of standards to ensure interoperability.
- Appropriate use of certification schemes – especially where safety is concerned.

Developing risk analysis and management techniques specifically geared towards the IoT environment.

The threats that affect the IoT environment are similar to those affecting any IT environment, but the probability of the threat materialising is likely to be quite different due to the differing nature of the vulnerabilities that are to be expected in such environments. Such vulnerabilities will not necessarily be purely technical, but will probably reflect the

1 http://news.aviation-safety.net/2016/03/13/final-investigation-report-released-into-germanwings-flight-4u9525-pilot-suicide-accident/

complexity of the way in which people, processes and technology are combined to create effective security solutions.

For this reason, threat and risk analysis approaches that take into account the specificities of the IoT environment could lead to a better understanding of how the ensuing risks can be successfully mitigated.

Tighter incorporation of the concept of 'security by design' into the software development lifecycle and systems integration methods.

The concept of 'security by design' is easy to understand at an abstract level, but can be difficult to apply in practice. This is most easily seen when considering products that are produced for a variety of operating environments (should a spreadsheet application incorporate advanced security features because it may be deployed in a nuclear power station?). Security by design is a complex process that involves making choices and such choices should be motivated by careful thought and logical argument.

Of course, security design must cover the entire life cycle of devices and products: from their conception, to their end-of-life, including the integration and operation with other connected systems. The concept can therefore also be sensibly adapted to system integration approaches, where a lot of critical decisions are made in defining security architectures.

Optimising the level of granularity of security controls.

Whilst the ability to define granular controls is certainly a good thing, it is by no means an obligation. Implementers should carefully consider what constitutes a manageable level of granularity and advise users accordingly.

Developing a coherent set of standards to ensure interoperability.

There are a number of organisations working on standardisation topics related to IoT, but this area of standardisation is still relatively young and there are many aspects which are as yet uncovered. The 'IoT Ecosystem Study' published by the IEEE Standards Association in 2014 notes that standardisation efforts tend to be aligned with vertical business segments and also provides a list of items that are missing from the standardisation perspective.[2]

Appropriate use of certification schemes – especially where safety is concerned.

Certification schemes can be a useful mechanism to assist end users in selecting appropriate devices for their particular operating environment. Such schemes, when correctly deployed, can also increase consumer confidence. However, in order for such schemes to add real value, consumers must understand the meaning of the certification (i.e. what exactly is being certified) and it should be easy for the user to verify the validity of the certification.

DUTY OF CARE

According to one definition, 'In tort law, a duty of care is a legal obligation which is imposed on an individual requiring adherence to a standard of reasonable care while performing any acts that could foreseeably harm others. It is the first element that must be established to proceed with an action in negligence'.[3]

Duty of care is a principle that could sensibly be used in the area of the Internet of Things, as long as the extent of influence of the different actors involved in producing and deploying IoT applications is taken into account. This however will not be an easy task.

2 'IoT Ecosystem Study', IEEE Stndards Association (2014): http://standards.ieee.org/innovate/iot/study.html

Consider for instance the task of security by design as viewed by the software developer. To a large extent, the degree to which the product will need to be secured will be dependent on the operating environment in which it will run. In other words, when the target environment is not known, software developers have to deal with *threats* and not *risks*. One way to deal with this issue would be to implement a high level of security on all products as the default approach. Unfortunately however, this is likely to be very costly and may kill the business case for many IoT applications. If security is not to be a barrier for the deployment of emerging technologies, the concept of security by design will have to incorporate trade-offs such as these and 'duty of care' will also have to be applied with these considerations in mind.

Similar considerations apply to other parties involved in the supply and deployment of IoT applications. An integrator for instance should understand the mechanisms that are available for securing a particular device and should be skilled in configuring these mechanisms to meet the needs of different environments, but cannot be reasonably expected to understand the structure of the code. When incidents are a result of a combination of 'development' and 'integration' factors it will be difficult to assess where responsibilities lie – this is particularly true in highly distributed environments, where devices may not be synchronised and it may even be difficult to determine the order of events leading up to the incident.

Finally, it is worth noting that as computing systems become more powerful there is a tendency to give more control to the end user (in many cases the end user will be the owner and administrator of the device). The principle of duty of care should also be applied to the user. This means that end users should bear more responsibility for understanding and correctly using the devices they implement. Just as the safest cars cannot prevent a crash if the driver is not sufficiently careful, the security of IoT devices will depend to a certain extent on the way in which they are operated.

CONCLUSIONS

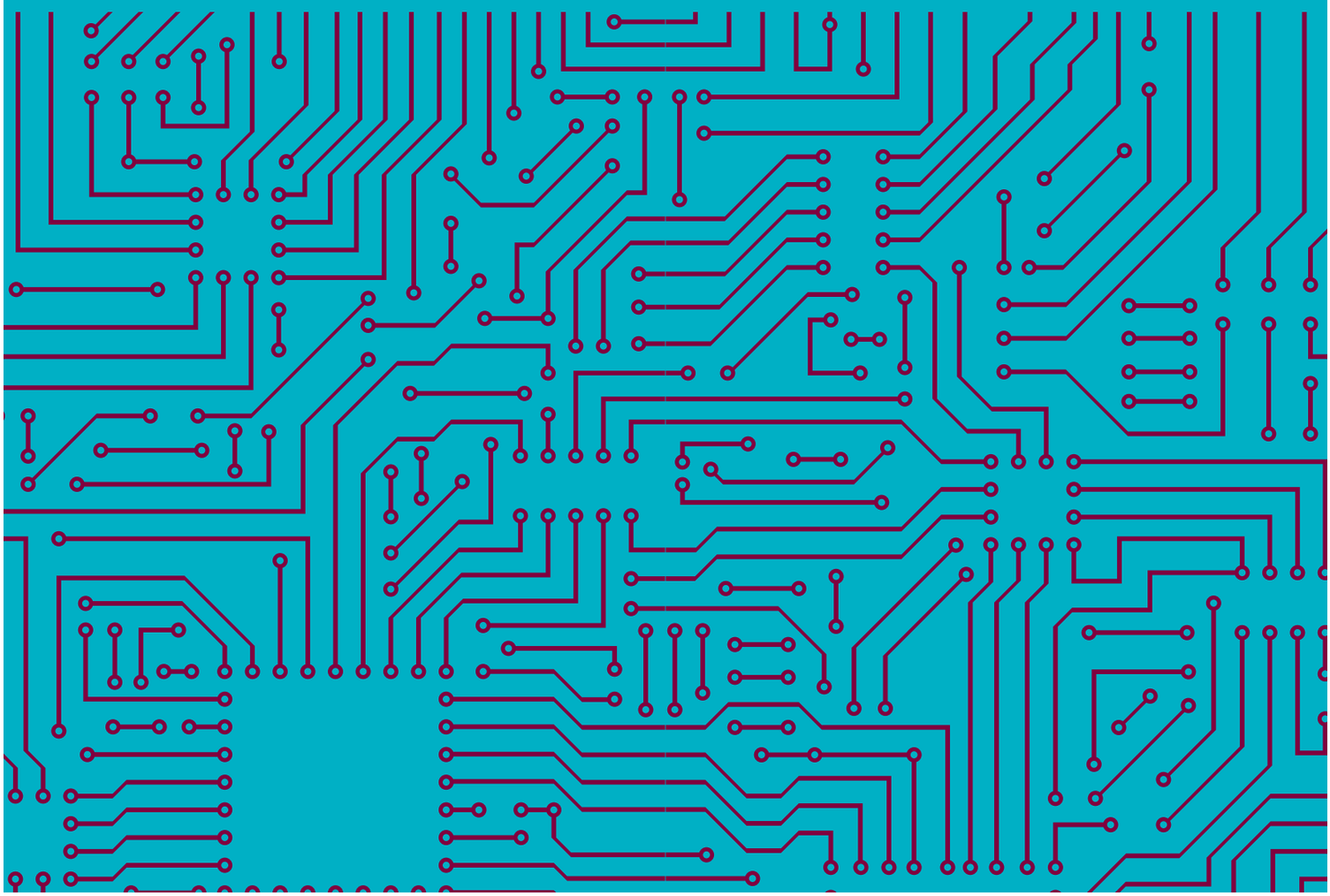
The Internet of Things presents some interesting challenges to developers and implementers where security is concerned. In many cases, the solutions to these challenges will involve assessing the right balance between competing factors, such as risk and cost.

The principle of duty of care can sensibly be applied in this area as long as due attention is given to the sphere of influence of the different parties involved in the final solution, which will be a combination of people, process and technology.

3 https://en.wikipedia.org/wiki/Duty_of_care

3 CYBERSECURITY AND THE INTERNET OF THINGS – A LAW ENFORCEMENT PERSPECTIVE[1,2]

Dr. Philipp Amann, MSc
Senior Strategic Analyst
Team Leader Strategy and Development
European Cybercrime Centre, Europol



INTRODUCTION

The Internet of Things (IoT) is characterized by a constantly growing network of connected devices, actuators and sensors that can interact with or collect data on their internal states or the external environment, using a variety of different protocols and standards. The IoT creates the ability for physical objects, which were previously often unconnected and without computing power, and people to remotely interact through the internet. It is one of the characteristics that make devices 'smart' as they become (more) context-aware.

The Internet of Things is also characterized by the convergence of people, processes, data, and objects by combining communications between machines, between people and machines and between people to deliver new or enhanced services and to provide improved contextual awareness and decision support.

Cloud Computing and Services provide the dynamic, scalable and ubiquitous infrastructure and services needed to support the storage and distributed processing of the data collected via the IoT. The ever-increasing amount of data that is being collected via the IoT – from different sources and on a variety of aspects, including data that was previously not or difficult to capture – links it to the concept of Big Data, which in essence is about new ways of analyzing, visualizing and leveraging la rge amounts of data in real-time or near real-time.

These concepts are a driving factor behind new types of 'critical infrastructure' such as smart cars, smart ships, smart homes, smart grids or smart cities.

However, the IoT plays a crucial role in more conventional types of critical infrastructure too as more and more smart sensors are being used in Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) control systems as well as Automatic Identification System (AIS) tracking systems.

RISKS AND CHALLENGES

The Internet of Things uses a variety of different software and hardware products as well as communication standards and connectivity protocols. Combined with the large and constantly increasing number of connected devices, this creates a broadened attack surface and increased number of attack vectors. In fact, the Open Web Application Security Project (OWASP) highlights several different attack surfaces such as a device's physical memory and interface (e.g. USB port), firmware, local data storage, update mechanism, network services, Cloud interface, mobile application and third-party APIs (application program interfaces).

1 2015 Internet Organised Crime Threat Assessment (IOCTA), https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015
2 2014 Internet Organised Crime Threat Assessment (IOCTA), https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

Basically, this means that any internet-facing device can become the target of an attack using a variety of different entry points.

The heterogeneity and complexity of the software and hardware ecosystem powering the IoT along with a lack of security and privacy by design creates substantial cybersecurity risks for industry, consumers and operators alike. Such environments are difficult to manage, control and safe-guard, considering also that many IoT devices have no built-in security features. In fact, due to the small size of some of these connected devices, resource limitations in terms of memory, battery and computing power are such that they are unable to perform cryptographic operations or scan for malware. In this regard, many of the so-called smart devices could actually be considered to be rather dumb when it comes to their lack of awareness to their risk posture.

As the IoT is more widely adopted and becomes increasingly part of production ecosystems one can also expect to see a higher degree of homogeneity and standardization when it comes to some of the hardware and software that is being used. As a consequence, the IoT runs the risk of failures that result from a single fault in software or hardware components used in smart devices, which present a mayor risk to cybersecurity. If such an exploitable failure is detected it can affect a potentially very large number of devices thereby creating a large number of potential victims. If there is even an option to fix such a vulnerability, this usually takes time, often years. Examples are smart TVs that may run operating systems used also in smartphones, which are often vulnerable to many of the same attacks, or home routers and IoT hubs.

A clear indicator of the growing adoption of the IoT is the rising number of smart 'things' such as smart homes, smart cars, smart medical devices and even smart weapons. This contributes to an increasing digitisation and online presence of personal and social lives, an increasing level of interconnectivity and automation, and an increasing amount of data that is being collected and analysed. This includes for instance facial and speech recognition features in smart devices or wearable technology that can process data. Apart from the aforementioned cybersecurity risks, this also creates a number of challenges in terms of identity, privacy and trust:

The data that is being collected and processed via the IoT creates new privacy issues as the combination of different categories of data can offer new insights. Since Big Data aids de-anonymisation – either through patterns and correlations that become visible in bigger data sets and/or the combination with other data sources – it becomes harder to protect privacy and personal data.

Because of the scale of the IoT, trust between different devices can be hard to engineer and expensive to guarantee. Yet, there is a need for strong and robust cross-platform authentication and identification services in order to restrict access to data and devices to authorized entities.

Moreover, the fact that smart devices are used to create contextual awareness and offer decision support makes them a target for data manipulation too.

Finally, large scale attacks against these new types of 'critical infrastructure' as well as existing infrastructures could have a significant impact in terms of safety, security, public health or the economy. Examples could include new forms of blackmailing and extortion schemes, hacked smart cars, medical devices or weaponized drones, data theft, attacks resulting in physical and mental harm, and new types of botnets. As with any cyber threat, such attack scenarios are not limited to a particular category of attackers or a particular set of motives.

LAW ENFORCEMENT CONSIDERATIONS

For law enforcement, the Internet of Things presents specific investigative challenges due to the diversity of hardware, software and communication standards and connectivity protocols being used. Some of the relevant data may be located in the Cloud, which will frequently require cross-border co-operation and legal assistance. In some instances, however, the amount of relevant data that can be extracted for investigative purposes may be minimal. Also, it can be expected that the IoT will further complicate the attribution of crimes, given the increased attack surface(s) and large number of attack vectors.

Extracting, identifying and combining the relevant evidence will routinely become a Big Data problem, requiring law enforcement to have the necessary skills, tools and expertise available.

An important application of Big Data in the area of law enforcement is predictive policing - the application of mainly quantitative analytical techniques to identify likely targets for intervention and to prevent crime, or solve past crimes by making statistical predictions. It is seen as a method that allows law enforcement to work more effectively and proactively with limited resources. The IoT can support predictive policing by providing the necessary data sets for the identification of patterns and correlations. The underlying models have a number of limitations such as the general inability to answer the question of causality. It is therefore important to use this concept carefully, proportionally and in line with relevant legislation and regulations.

As mentioned before, any smart device storing valuable data or providing crucial services can be the target of a cyber-attack. This can range from very small devices, to smart cars, to smart container ships, to smart cities.

Considering also the relevant findings and recommendations in Europol's EC3's 2014 and 2015 Internet Organised Crime Threat Assessment reports, this necessitates further attention and consideration by law enforcement as the IoT is increasingly becoming a reality and connected devices are regularly comprised. Specifically, this calls for a broader focus on potential targets, criminal modi operandi, and mitigating, preventive and investigative measures.

OPPORTUNITIES AND RECOMMENDATIONS

While the Internet of Things makes the protection of data, establishing trust and ensuring privacy and security more challenging, it can also help address the new challenges and threats in cyberspace, for instance in the form of data-driven security or behaviour-based security.

The IoT in combination with Big Data analytics, machine learning and Artificial Intelligence approaches can help improve cybersecurity through better threat detection and prediction, intelligence collection and analysis, and faster response. A combination of human-driven techniques, which typically rely on rules and may therefore miss any attacks that do not match the rules, and machine-learning approaches using anomaly detection, which tends to trigger false positives, may leverage the advantages of both domains.

Another potentially interesting approach to increasing cybersecurity for the IoT and to establishing trust and ensuring privacy in the decentralised network it creates is the use of the blockchain or Distributed Ledger Technology (DLT). DLT can potentially provide a framework to facilitate transaction processing and coordination among interacting IoT devices, allowing each to manage its roles and behavior and thereby making them (more) autonomous. It may also be applied to ensure that the operating system and firmware used in a smart component of critical infrastructure has not been tampered with.

For law enforcement in particular, the potential benefits include improved and more targeted analytical capabilities, an increased chance to find relevant evidence, improved triaging, the ability to create a denser timeline of events, and better support for the automated analysis of crime-relevant data, including speech, image and video recognition. In addition to the need to adhere to the principles of lawfulness and proportionality, it is of course of utmost importance to balance the potential benefits against the negatives that may result from reduced privacy and other unintended consequences.

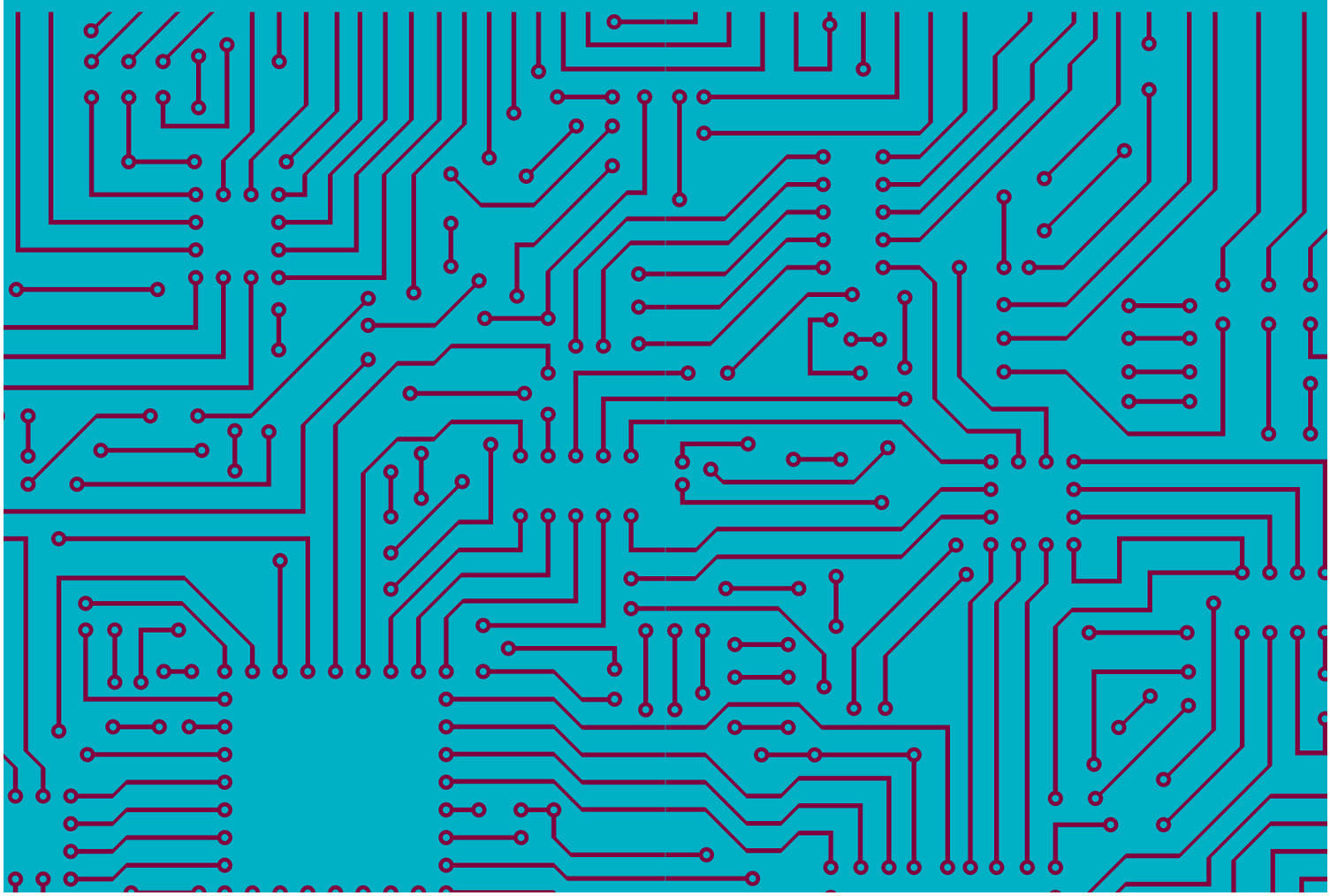
The complexity and resulting cybersecurity challenges in relation to the IoT ecosystem call for a holistic, smart and agile approach; the multi-faceted nature of the challenges and risks demands an equally faceted response by all relevant stakeholders with a view to ensuring cybersecurity. Consequently, cooperation and public private partnerships will play an increasingly important role – ideally, all IoT actors and relevant stakeholders should engage in discussions on IoT design choices and their implications.

Security-by-design and privacy-by-design should be the guiding principles when developing IoT devices and enabling services. This includes the need to only collect the minimum amount of data necessary, automatically protect personal data by using proactive security measures (e.g. end-to-end encryption) and means to make individuals less identifiable, implement data retention policies, ensure transparency, and provide opportunities to assess any analytical processing, to mention some.

The Internet of Things is no longer a futuristic concept but a well-established and constantly expanding model. It is therefore timely to hold a multi-stakeholder discussion on cybersecurity, putting it at the heart of the IoT.

4 THE INTERNET OF THINGS: A CYBERSECURITY STRATEGY PERSPECTIVE

Daniel Shepherd
Chief Marketing Officer, S21sec
Chairman, European Cyber Security Group (ECSG)



Yesterday´s definition of a nightmare: the spooky ghoul beneath the bed or in the wardrobe, grinning sharply as soon as the lights go out.

Today´s definition of a nightmare: lost phone, forgotten password, corrupted software, battery run down (again) and, more than anything else, a slow or (oh no!) a non-existent connection to the Internet.

The bottom-line is that we already live in a hyper-connected world and there is no turning back. We are hooked. We rely on connectivity for our day-to-day lives, both professionally and personally and we do not really know what to do with ourselves when that connection is down.

Yet Internet connectivity is not yet as pervasive as it will be. The concept of the Internet of Things (IoT) has been well documented: market commentators and technology companies alike are estimating at least 5x as many IoT connections by 2020 as mobile subscriptions and market revenues of more than US$ 5 trillion. These numbers surpass many times over the number of people that populate the world, but can easily be understood in the context of the diverse set of devices that are in scope: home appliances; vehicles; personal health and fitness devices; entertainment systems; energy meters; machinery; entire buildings; vending machines; and the list goes on, to include the human body.

While the phenomenon is today more pronounced in some areas and less so in others, the trend is clear: onwards and upwards. This form of progress is impossible to refute because it obeys two of the Internet´s value maxims: volume and variety. To monetise data, companies have to go beyond B2C; after all, the concept of share-of-wallet in the consumer space is becoming more challenging now that we the world faces up to the fact that we do not live in an economy with a Hollywood ending.

All these developments postulate amazing benefits for Society and Business.

A great example is healthcare. Many countries around the world are very concerned because people are generally living longer, consuming more and suffering from a growing number of acute and chronic ailments. These factors alone mean that healthcare provisioning is getting increasingly expensive. Add spiralling costs related to investments in innovation, hospital technology, rent per square meter and labour rates and a fundamental funding gap, it is easy to see how many national healthcare systems are struggling economically.

It is also easy then to understand the strong interest in the plethora of remote care, self-care and well-being technologies that are being commercialised. Even more profound work is being done to assist in the early diagnosis of predispositions to enable preventative care.

However, as the world pursues the fulfilment of ubiquitous connectivity and all of its promising benefits, we have already started to see the darker side of all this progress. For every innovation, there is someone that is able to demonstrate a risk: the car that can get

hacked; the health monitor that is vulnerable to data theft; machines that can be targeted and remotely controlled; or drones that are being diverted by drug cartels.

It is worth noting that the gunpowder line running between Benefit and Concern is getting shorter, such that we end up hearing the "kaboom" even before vulnerabilities are properly identified and documented, let alone patched, by the manufacturers. In part, this is because economic pressures mean that companies are launching products quickly to ensure time-to-market and thus time-to-revenue; in fact, in an IoT context, companies are working with applications and solutions in the field, while the associated guidelines and regulations have yet to be matured. However, the fact that progress requires openness, collaboration and standardization should not be overlooked. Unfortunately, these are very exploitable terms and the so-called Bad Guys, whether terrorists, activists, organized gangs, or petty criminals, can and will take advantage because they effectively lower the barriers to disruption.

Of course, in many ways these issues are not at all new. But what is new is that IoT essentially ups the ante. In an IoT world there is so much more to gain and thus lose than in yesterday´s world.

The cybersecurity industry has much to do in relation to IoT and the EU focus is crucial because the region is a central player both in terms of the source of demand and the ecosystem of players providing solutions. Here are just some of the initiatives that we should be putting in motion, with special consideration for how an EU structure could be leveraged to maximize reach.

- **Education**
  We must help educate the many companies involved in IoT (is there any that is not?) that their businesses and business models are changing. When banks started creating online platforms to allow customers to use the Internet to do what they used to do in-branch, they were doing more than create an additional customer touch point; they were entering a new digital market, with its tremendous potential for additional revenues and (potential) cost efficiencies, but also with its significant implications, from 24x7 customer support to a greater span of responsibility for securing the customer´s experience. With IoT, many companies will have to go through a similar sort of realization and internalization.

- **Duties of Care**
  The above point brings the topic of duties of care to the forefront because it fundamentally changes the scope of responsibility and accountability that any one organisation can be deemed to have in relation to it customers, or the individual citizen. For example, car manufacturers have traditionally been responsible for ensuring that drivers and passengers are enclosed in a safe environment when driving and that their physical safety has been taken into consideration at all stages of the product development process. However, cars already have the capacity to receive and store plenty of personal information from its owners. In this context, it can be clearly argued that the very same car manufacturers are accountable for the security of personal information that is received and transmitted between person, vehicle, filling station, home, office, mechanic, insurance company and more.

- **Cyber Security Business Model**
  In this sense, we must help organisations understand the types of security risks that their new business models are exposed to and support them in defining both risk mitigation and risk management approaches. While many organisations today can be quite disciplined and effective in a reactive mode, due to their hierarches and non-security related crisis management experience, this only goes to underline the potential of a proactive approach in security.

- **Security by Design**
  We can also do a lot to ensure that product development and product launch process are reviewed with security best practices in mind. In order to achieve "Secure by Design" in its truest sense, both the process and security domains need to map onto each other in terms of approach and methodology. Security needs to be understood to be a business domain, not an IT domain. And security needs to understand how the technical and business people really think. If we keep talking a different language and only do so sporadically or periodically, we will continue to let important security issues fall between two stools.

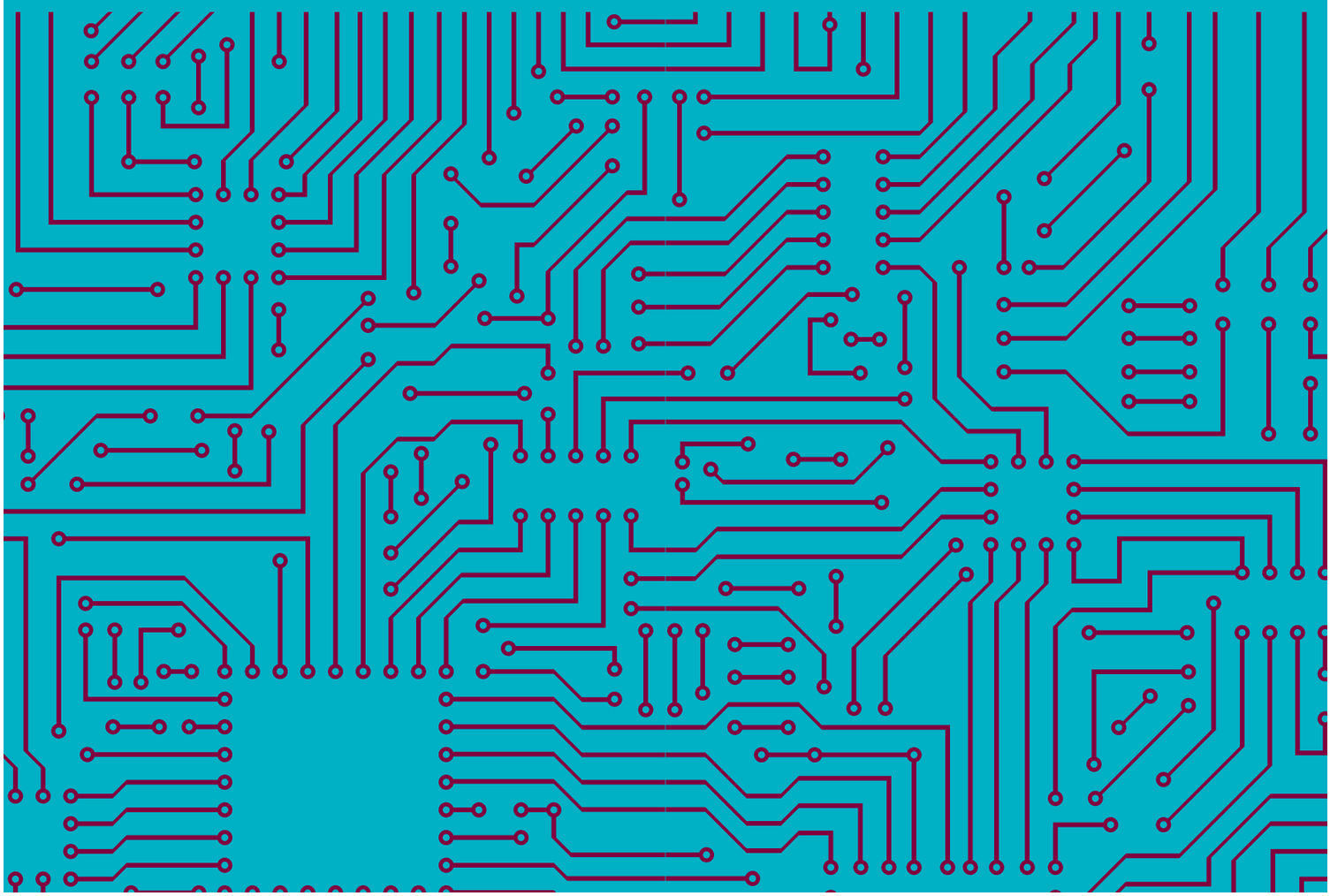
- **Trust Groups**
  Beyond policy and standards working groups, we have seen some very interesting developments in the formation of Trust Groups. In Trust Groups, the objective is to share, discuss and extract value on an on going basis from data and insights into developments, vulnerabilities, threats, risks, patches and solutions. The challenges around Trust Groups relate to competitive, economic, time and pride constraints that undermine the "greater than the sum of its parts" argument. While the theory sounds logical and appealing, most individuals and organizations still struggle with the idea that input and output are intrinsically connected. However, due to the cross-industry nature of IoT, these structures should receive a strong push.

- **Incident Response Capabilities**
  Furthermore, because, as we are all aware, incidents can and do happen despite all our various efforts, we need to significantly enhance our regional incident response capabilities. We continue to be too fragmented at a country-by-country and player-by-player level to really take advantage of the inherent scale that we have in the EU. Yet it is this type of scale that will be called upon in the event of an IoT-related breach.

The need for connectivity between humans is basic. In an IoT world, we are extending this logic to many things around us. Pursuing the next wave of growth, organisations globally are accelerating their IoT strategies and we are seeing exciting developments across most industries. While device connectivity is already a reality in some areas, the next 5 to 10 years will prove to be revolutionary in this context. As this wave continues to form, we, the cybersecurity industry, must play an active role to ensure that the promise of IoT is matched by its reality. The first step is to ensure we understand its implications and that we manage its risks proactively. While this is a global phenomenon, the EU has a fundamental duty, as expressed through its Core Values, to address the topic because of its key role as the source of both supply side players and a society that rightly demands and expects a resilient and secure environment.

5 INTEROPERABILITY, CYBERSECURITY, AND THE IOT

Ryan Budish
Senior Researcher
Berkman Center for Internet & Society
Harvard University



Berkman
The Berkman Center for Internet & Society
at Harvard University

INTRODUCTION

As the Internet of Things (or "IoT") expands, it is creating novel and complex cybersecurity challenges. Addressing those challenges requires application of frameworks and approaches that have not been typically employed in the cybersecurity space. In this short essay, I suggest that one useful framework is that of "interop" developed by Urs Gasser and John Palfrey.[1] The application of the interop framework to IoT cybersecurity leads to two observations: (1) the usefulness of any IoT ecosystem is often in direct tension with the ability to secure those IoT ecosystems; and (2) the challenges of addressing cybersecurity risks are magnified in the IoT as the inherent obstacles to addressing cybersecurity must be overcome not just once, but across every layer of interop.

UNDERSTANDING INTEROP

Interoperability (or "Interop") is a central, and often invisible, element of our highly interconnected modern society. Interop is operating silently in the background, every time someone makes a seamless international telephone call or accesses a website without having to think about things like signaling standards or Internet protocols. The fact that an e-mail, for example, can be read through proprietary software, in a browser, or a mobile device regardless of the computer, operating system, device manufacturer, or ISP is a tribute to interop.

At its most general level, interop is the ability to transfer and render useful data and other information across systems, applications, or components. But this occurs across complex and varying layers of interop. Specifically, the Gasser and Palfrey interop framework identifies four fundamental layers of interop: technological, data, human, institutional. Too often, people only think about interop as it relates to the exchange of data through technological means. And while those layers are critical for the IoT, so too are the human and institutional layers of interoperability.

Given the significance of each layer, it is important to consider each one briefly:

- **Technological:** The technological layer is the hardware and code that physically connects one system or device to another. This layer enables systems to share data with one another, often through an explicit, agreed-upon interface.

- **Data:** The data layer is the ability of physically interconnected systems to understand and make use of the bits passing between them. The data and technological layers are often considered together given their interdependence, but they are not synonymous.

1 Urs Gasser & John Palfrey, Interop (2012); Urs Gasser, GSR Discussion Paper: Interoperability in the Digital Ecosystem, ITU, June 2015, https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/Discussionpaper_interoperability.pdf.

The technological capacity to receive the raw bits is not the same as the ability to process those bits. When we consider cybersecurity risks, we often focus on the technological and data layers as they represent the vector by which technical exploits are deployed.

- **Human**: This layer is the ability for humans to understand and act on the data that is exchanged. Language and willingness to cooperate are two examples of human interoperability. If the individuals at the end points of a data exchange are unwilling or unable to understand each other and work together, interoperability may fail. In the context of cybersecurity, human interoperability is often a source of enormous risk, as attackers seek to exploit weaknesses in human behavior. It is simultaneously a key component of any attempt to address cybersecurity risks and investigate attacks, as both require significant coordination and cooperation.

- **Institutional**: The institutional layer is the ability of societal systems to engage effectively. Perhaps the most significant example of this layer is a legal arrangements. This, too, is critical in addressing cybersecurity risks. For example, institutional interoperability, through multilateral or multistakeholder organizations, may help establish norms for cybersecurity practices. Similarly, institutional interoperability, such as mutual legal assistance treaties, may facilitate the investigation of cybersecurity threats and attacks.

This high-level overview of interoperability makes it clear that interop plays an important role in how we think about cybersecurity. And this has important implications for cybersecurity in the IoT.

INTEROP AND THE IOT

Generally speaking, the Internet of Things (or "IoT"), represents a push to connect to the Internet an array of previously unconnected devices. Interoperability underlies and enables this explosion of the IoT. Take, for example, a jet engine that can signal from the air to ground teams a need for maintenance, or a pill bottle that can order a prescription refill. In order to do these things, IoT devices must be able to seamlessly interoperate with a variety of systems and networks in ways that are meaningful and secure.

The IoT, by leveraging interop and interconnectedness, most certainly has the potential to make daily life and industrial processes more convenient or efficient. But this increasing interconnectedness also poses cybersecurity risks, particularly when devices or systems are designed or implemented poorly. Each new device or network that is added to an interoperable system increases the opportunities for attackers to exploit the system.

THE TENSION BETWEEN IOT UTILITY AND SECURITY

The role of interop in cybersecurity and the IoT highlights the first observation: the usefulness of any IoT ecosystem is often in direct tension with the ability to secure those IoT ecosystems.

Take the example mentioned above of a pill bottle that can automatically refill prescriptions when the bottle is nearing empty. The bottle's usefulness increases with the number of doctors' and hospitals' systems that the bottle can interact with; a bottle that works with all of a patient's doctors is better than one that only works with one or two her doctors. Similarly, the usefulness of the bottle increases with the number of pharmacies that it interoperates with. However, each new hospital or pharmacy that the bottle interoperates with is another system that might have latent vulnerabilities, which creates a risk that sensitive data will be stolen. Moreover, the more systems that interoperate, the greater the risk that a single vulnerability in one system will enable data theft from other systems.

SECURING THE IOT

The Interop framework helps highlight a significant challenge in securing the IoT. As a recent white paper from the World Economic Forum's Global Agenda Council on Cybersecurity makes clear, "cultural and financial pressures encourage devaluing investments in cybersecurity."[2] These pressures, such as the need to be first-to-market and to maximize short-term returns for shareholders, make it difficult for companies to make the kind of long-term investments necessary for addressing cybersecurity issues. While the white paper identifies a variety of approaches for overcoming these obstacles, the obstacles remain entrenched and significant.

These obstacles, while a challenge across industries, are magnified in the IoT ecosystem. In highly interoperable systems, cybersecurity must be addressed at each layer of interop. And therefore, the inherent obstacles to addressing cybersecurity must be overcome not just once, but across every layer of interop. In other words, the social and economic barriers to addressing cybersecurity must be addressed at not only the technical and data layers, but at the human and institutional layers as well.

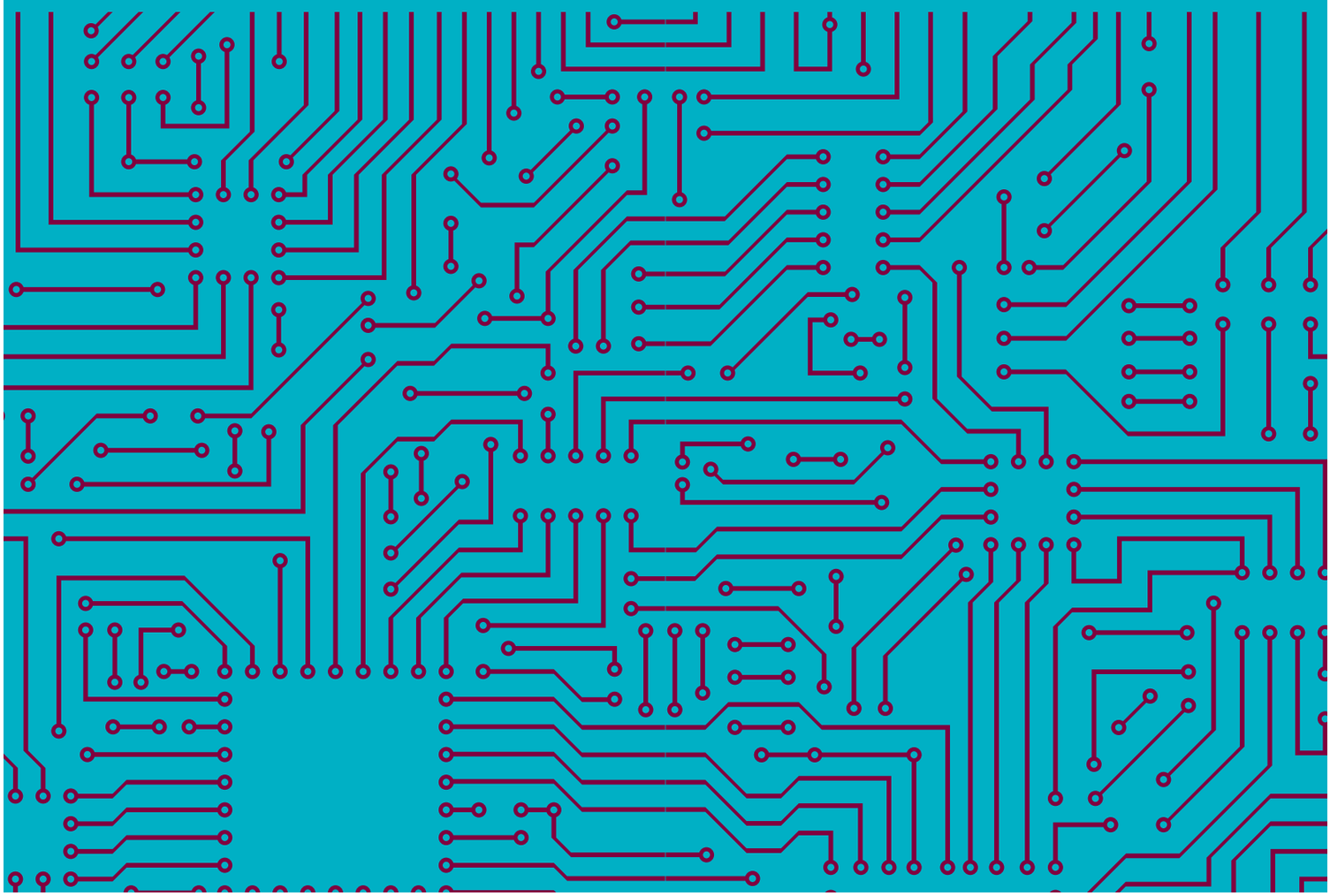
CONCLUSION

It would be easy, but inaccurate, to conclude that the only solution is to develop products that shun interoperability. Interoperability may increase the number of opportunities or vectors for cybersecurity attacks, or the potential fallout from such attacks, but it is not the cause of the security vulnerabilities themselves. Poorly designed systems, both interoperable and not, can be compromised. For that reason, it remains imperative to work to alter the underlying incentive structures that lead to inadequate investments in cybersecurity. This is important generally, and even more so for the IoT. Changing the incentive structures will require cooperation from both the public and private sectors across a variety of endeavors.

2 World Economic Forum, White Paper: Global Agenda Council on Cybersecurity, April 2016, at 4.

6 INTERNET OF THINGS

Leon Strous
President
International Federation for Information Processing (IFIP)



INTERNET OF THINGS

What developments do you see in the field of IoT?

The fast development of the Internet of Things is enabling the emergence of many new applications and the redesign of traditional systems towards more integrated services and effective operation. Some of the elements contributing to the wide potential of this area include: remote access / control, more effective monitoring and supervision thus allowing better performance, real-time access to data which supports timely decision making, wider systems integration, complemented with access to cloud-based resources, mobility without losing access to systems, access to large amounts of sensorial data, etc.

The very nature of the IoT, combining the physical and the cyber worlds, requires the combination of a set of competencies and hence interdisciplinary cooperation and coordination. In addition to the purely technological issues, there are other relevant aspects to be properly addressed in order to let the full potential of IoT be achieved. These include: legal and regulatory aspects, socio ethical aspects, and economical aspects. From a research perspective many topics and questions need to be investigated:

- **Characteristics of future IoT devices and IoT services**: What are the kinds of devices that we will have to manage in 5-10 years; What will be the peculiar issues that we will have to deal with in managing those devices; What can we learn from case studies of early prototype systems?

- **IoT methodologies, tools, and approaches**: What kind of monitoring information will we have to process; What will be the bandwidth and processing requirements; How autonomic can the IoT be and to what extend is explicit management still needed; What features (if any) should we start investigating; Can we utilize methodologies and tools currently being developed in other research areas?

- **Management protocols for the IoT**: What are the requirements for managing the IoT and related novel services; Can we use or adapt existing protocols to manage IoT devices or is a new set of protocols needed; Are generic IoT application protocols adaptable to address the management requirements; Are novel tools for designing application- or domain-specific protocols required; How can constrainedness of nodes and networks be dealt with; What are feasible security solutions for the management of IoT devices and services; How can a life-cycle be supported that may include the reselling of IoT devices?

- **Business models for IoT management**: Can we expect administrators to have system and network management skills; Can an operator managing a server also manage an ice cream machine? Are operators with domainspecific skills (and perhaps no system and network management skills) needed instead; What new business models can the availability of large-scale IoT management platforms open; Who will manage the devices that we buy? Should consumers manage Internet-enabled devices like light-bulbs? Or should the manufacturer manage these devices?

What economic opportunities brings IoT?

In many application domains IoT can bring big advantages in cost saving. Think about healthcare where the IoT with early warning and monitoring systems can allow people to live at home longer while still getting medical assistance when needed. Energy saving is another easy example. By monitoring and self-adjusting the use of energy in buildings, being homes, offices, schools, industrial facilities, can be controlled in a better way than currently often the case. Sensors in agriculture will facilitate better monitoring of (risks to) crops.

Can IoT be used strategically as a possible solution to major issues?

See the examples under economic opportunities. Major issues in the health care (cost), in food supply for the world, in environmental pollution issues can benefit from IoT opportunities.

What do you see as the security risks of IoT, in general and for your workfield?

There are the well-known and obvious privacy issues (big brother, loss of control of your life, ownership of data/information). There are risks in decision making processes due to errors in the functioning of the data collection and processing systems / inability to add professional interpretation and judgement of information. Such risks also exist currently in systems but in the context of the IoT, there may be less moments for people to react and correct.

Another risk concerns the issue of ownership. Devices / sub-systems typically have or at least should have an “owner”; therefore, in addition to the growing autonomy of such entities (which comes from the growing intelligence / cognitive capabilities), they also have to “obey” to their owners, which introduces a new dimension to the problem of designing such systems. When systems involve a large number of entities (hundreds? thousands? millions?), flat organizational structures are not appropriate. Therefore some “structural thinking” is necessary, leading to the organization of such entities in “communities” or “societies” (“ecosystems”). Important issues in these “communities” are the definition of “borders” / membership, roles, and evolution.

In organized communities – depending on their design / purpose – different behaviors can emerge. Some behaviors are consistent with the system’s purpose (healthy behaviors). But we can also have faulty / deviating behaviors. These are particularly critical as complexity increases and we become more dependent on such systems. Understanding (and detecting) faulty behaviors is thus critical. How do these behaviors propagate / extend over “different regions” of the communities? How do they evolve? How can systems adapt to faulty situations? Collaborative networks and collective adaptive systems principles are important here.

Faulty behaviors can have an endogenous source (component’s malfunctioning, interoperability “frictions”, non-collaborative behavior, etc.) or result from exogenous attacks (e.g. terrorist cyber-attacks). It is therefore necessary to develop adequate protection / recovery approaches and mechanisms. This involves distributed monitoring, (collective) diagnosis of detected faulty behaviors, and launching recovery / self-healing processes. Considering the complex nature of such systems, it is important to first elaborate some “health indicators”, including system’s trustworthiness indicators, system’s certification, etc. How much can we trust in systems that we do not fully understand and over which we do not have full control (as they are complex, evolving, components belonging to different owners, etc.)? Learning mechanisms should be an intrinsic functionality here.

What perspectives for the EU do you see to mitigate those risks?

The European Union / Commission should (continue to) encourage / support / facilitate research on all aspects of the IoT, emphasizing the interdisciplinary aspects. Similar, the EU/ EC could facilitate / guide interdisciplinary discussions on the risks and on ways to mitigate them, using the knowledge available at the various stakeholders. In such discussions stakeholders together should identify application areas where self-regulation / regulation can help mitigating risks.

It is essential to not only promote the economic opportunities and the advantages but also to educate / warn people / customers. Customers will love many applications of the IoT, but they are not aware of or don't want to see the risks, especially when they can get something "for free" or when an application makes life easy. A distinction can be made in different (types of) applications with different risks. Activating a car requires more security than a simple power switch for home usage turning on a lamp. Perhaps a security label, like used for energy efficiency, could inform the customers about the risks.

References?

The 13 Technical Committees and 130 Working Groups of IFIP cover a very wide range of topics in the ICT field. These groups represent a considerable research community, both from academia and from industry. For this contribution I have used (parts of) papers and calls for papers from conferences organized by various IFIP groups. The main reference is the paper "Contributing to the Internet of Things" by Luis M. Camarinha-Matos et al, in Technological Innovation for the Internet of Things, IFIP AICT Series 394, Springer, ISBN 978-3-642-37290-2. Other examples of papers used can be provided upon request.

DUTIES OF CARE

Which parties have a duty of care?

Being the global federation of professional ICT societies, IFIP is paying explicit attention to the professionalism of the ICT workforce. We consider this to be a key element in building trustworthy and reliable systems. Therefore, ensuring cyber security and cyber resilience is also a duty of care of **the individual ICT professional**, in all stages of a system lifecycle (design, development and operation). This means that most, if not all, types of ICT functions and jobs have to contribute to cyber security and cyber resilience.

Naturally we also support the view that companies and the management of these companies have a duty of care, as well as the individual user / consumer.

Where do these duties consist of?

ICT professionals should be trained / qualified in secure system design and development and have the right skills to securely operate and maintain such systems. They should adhere to a professional code of conduct that addresses issues like keeping the professional knowledge and skills up to date. They should resist commercial pressure to launch a product that does not meet the security requirements appropriate for that product. Companies should create conditions (in their culture and company / governance rules) to make this possible.

Users / consumers have a duty to educate themselves in order to be able to understand the risks of the systems they use and to take the measures they can take to safeguard the system and the data processed. Not performing such measures would make them responsible / liable for damage or make their potential claims to product liability invalid. One size does not fit all, a distinction has to be made in type of user/consumer and type of product/system.

What challenges do you see at this moment and in the future?

The main challenge will be to align requirements and frameworks, within the EU but also on a global scale.

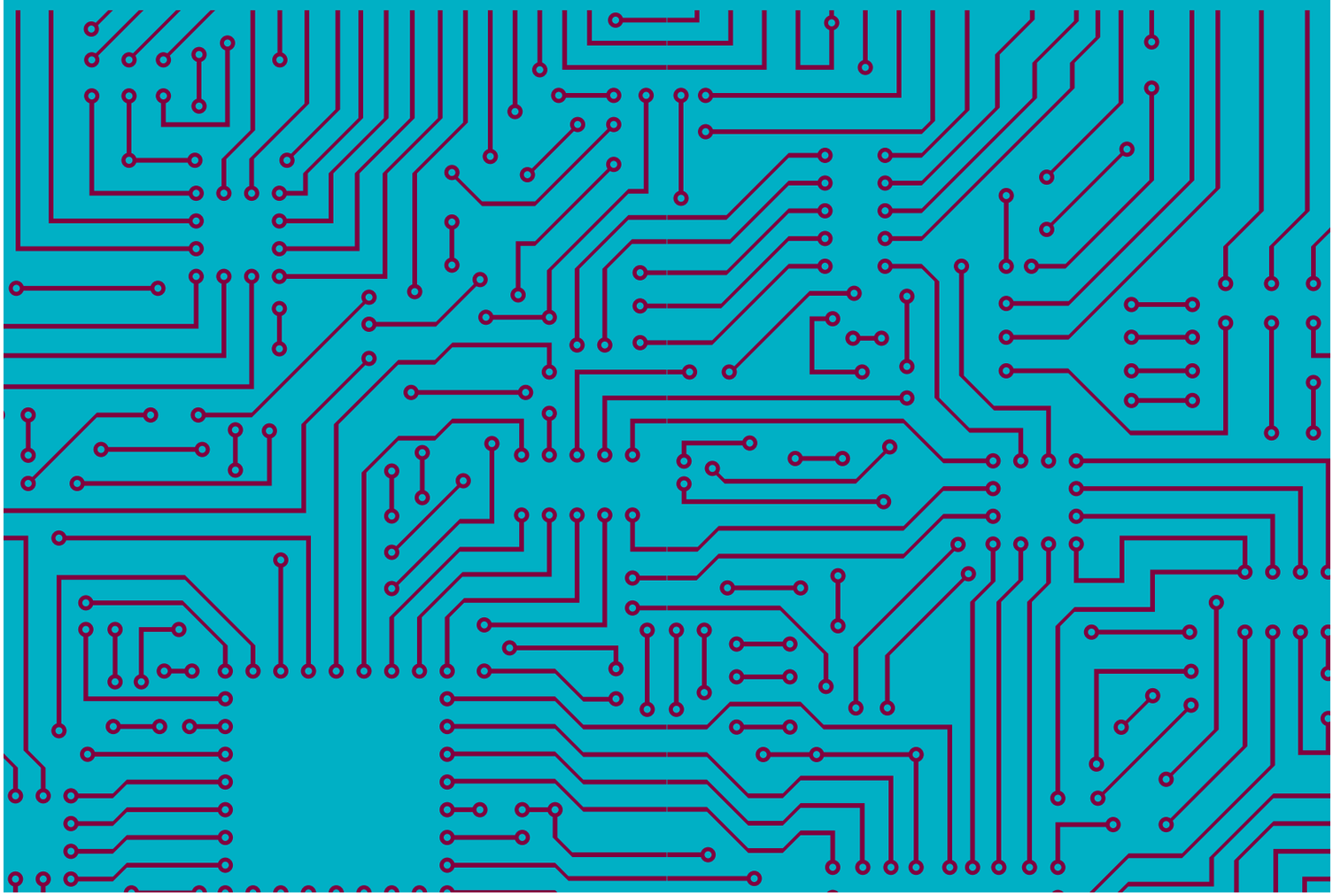
Should the EU harmonize the duties of care and provide a legal framework?

With respect to the individual ICT professional, it might be useful to consider frameworks comparable with those for chartered accountants or perhaps the medical profession. These frameworks should address the profession and professionalism. And the duty of care would be an element in such a framework since codes of conduct / codes of ethics are part of a profession. The EU could, as a starting point, encourage countries and professional societies to establish such frameworks and give guidance on the minimum elements in them. Since the development and production of IT systems and the threats to them are not limited to Europe, it is important to have a long term vision on a global requirement for the profession and the duty of care.

7 INTERNET SOCIETY PERSPECTIVE ON THE INTERNET OF THINGS

AN APPROACH TO TACKLING INTERNET SECURITY ISSUES

Internet Society



INTERNET SOCIETY PERSPECTIVE ON THE INTERNET OF THINGS

INTRODUCTION

This short paper presents a perspective of the Internet Society on some aspects of the Internet of Things (IoT) and the development of this ecosystem. It is produced with a question in mind - what possible action perspectives do you see for the EU to facilitate the chances of IoT? And what can be done to mitigate or reduce it to acceptable levels of security risks?

The Internet of Things is an emerging topic of technical, social, and economic significance. Projections for the impact of IoT on the Internet and the economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025.

The topic of the IoT is important to the Internet Society as it represents a growing aspect of how people and institutions are likely to interact with the Internet in their personal, social, and economic lives. An explosion of IoT applications could present a fundamental shift in how users engage with and are impacted by the Internet, raising new issues and different dimensions of existing challenges.

As such we have identified five areas we believe need to be addressed to fully realize the potential benefits of IoT for individuals, society, and the economy:

- Security
- Privacy
- Interoperability/Standards
- Regulatory, Legal and Rights Issues
- Emerging Economy and Development Issues

These aspects are explored in greater detail in a whitepaper released in October 2015 by the Internet Society: "An Overview – Understanding the Issues and Challenges of a More Connected World[1]". This paper provides a summary of the findings.

1 http://www.internetsociety.org/doc/iot-overview

SECURITY

While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be a fundamental priority. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Poorly secured IoT devices and services can serve as potential entry points for cyber attack and expose user data to theft by leaving data streams inadequately protected.

The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally. This challenge is amplified by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments.

As a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the Internet itself to potential harm. Accordingly, a collaborative approach to security will be needed to develop effective and appropriate solutions to IoT security challenges that are well suited to the scale and complexity of the issues.

PRIVACY

The full potential of the Internet of Things depends on strategies that respect individual privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users, but concerns about privacy and potential harms might hold back full adoption of the Internet of Things. This means that privacy rights and respect for user privacy expectations are integral to ensuring user trust and confidence in the Internet, connected devices, and related services.

Indeed, the Internet of Things is redefining the debate about privacy issues, as many implementations can dramatically change the ways personal data is collected, analyzed, used, and protected. For example, IoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to opt out of certain data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of users. While these are important challenges, they are not insurmountable. In order to realize the opportunities, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services.

INTEROPERABILITY / STANDARDS

A fragmented environment of proprietary IoT technical implementations will inhibit value for users and industry. While full interoperability across products and services is not always feasible or necessary, purchasers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, and concern over vendor lock-in.

In addition, poorly designed and configured IoT devices may have negative consequences for the networking resources they connect to and the broader Internet. Appropriate standards, reference models, and best practices also will help curb the proliferation of devices that may act in disrupted ways to the Internet. The use of generic, open, and widely available standards as technical building blocks for IoT devices and services (such as the Internet Protocol) will support greater user benefits, innovation, and economic opportunity.

LEGAL, REGULATORY, AND RIGHTS

The use of IoT devices raises many new regulatory and legal questions as well as amplifies existing legal issues around the Internet. The questions are wide in scope, and the rapid rate of change in IoT technology frequently outpaces the ability of the associated policy, legal, and regulatory structures to adapt.

One set of issues surrounds crossborder data flows, which occur when IoT devices collect data about people in one jurisdiction and transmit it to another jurisdiction with different data protection laws for processing. Further, data collected by IoT devices is sometimes susceptible to misuse, potentially causing discriminatory outcomes for some users. Other legal issues with IoT devices include the conflict between law enforcement surveillance and civil rights; data retention and destruction policies; and legal liability for unintended uses, security breaches or privacy lapses.

While the legal and regulatory challenges are broad and complex in scope, adopting the guiding Internet Society principles of promoting a user's ability to connect, speak, innovate, share, choose, and trust are core considerations for evolving IoT laws and regulations that enable user rights.

EMERGING ECONOMY AND DEVELOPMENT ISSUES

The Internet of Things holds significant promise for delivering social and economic benefits to emerging and developing economies. This includes areas such as sustainable agriculture, water quality and use, healthcare, industrialization, and environmental management, among others. As such, IoT holds promise as a tool in achieving the United Nations Sustainable Development Goals.

The broad scope of IoT challenges will not be unique to industrialized countries. Developing regions also will need to respond to realize the potential benefits of IoT. In addition, the unique needs and challenges of implementation in less-developed regions will need to be addressed, including infrastructure readiness, market and investment incentives, technical skill requirements, and policy resources.

The Internet of Things is happening now. It promises to offer a revolutionary, fully connected "smart" world as the relationships between objects, their environment, and people become more tightly intertwined. Yet the issues and challenges associated with IoT need to be considered and addressed in order for the potential benefits for individuals, society, and the economy to be realized.

The range of these challenges is considerable. As such, we believe it will take informed engagement, dialogue, and collaboration across a wide range of stakeholders to plot the most effective ways forward.

AN APPROACH TO TACKLING INTERNET SECURITY ISSUES

INTRODUCTION

Any cybersecurity framework needs to start with an understanding of the fundamental properties of the Internet (open standards, voluntary collaboration, reusable building blocks, integrity, permission-free innovation and global reach - "the Internet Invariants" [1], - and an appreciation of the complexity of the cybersecurity landscape. It should be premised on fostering trust and protecting opportunities for economic and social prosperity. Furthermore, real security on the Internet can only be realized within a broader context of trust and respect of fundamental human rights and values, such as privacy.

Achieving security objectives, while preserving these fundamental properties, rights and values is the real challenge of cybersecurity strategy. The design and implementation of security solutions should be undertaken with consideration as to the potential effect they might have these fundamentals.

Everyone has a collective responsibility for the security of the Internet: multistakeholder cross-border collaboration is an essential component.

Commercial competition, politics and personal motivation play a role in how well collaboration happens. But, as collaborative efforts have demonstrated, differences can be overcome to cooperate against a threat. Such voluntary as-needed "working for the benefit of everyone" collaboration is remarkable for its scalability and its ability to adapt to changing conditions and evolving threats, yielding unprecedented efficacy.

Informed by these reflections, we introduce the term "Collaborative Security" to describe our approach for tackling Internet security issues.

Collaborative Security[2] is an approach that is characterized by five key elements:

- **Fostering confidence and protecting opportunities**: The objective of security is to foster confidence in the Internet and to ensure the continued success of the Internet as a driver for economic and social innovation.

- **Collective Responsibility**: Internet participants share a responsibility towards the system as a whole.

  Fundamental Properties and Values: Security solutions should be compatible with fundamental human rights and preserve the fundamental properties of the Internet — the Internet Invariants.

- **Evolution and Consensus**: Effective security relies on agile evolutionary steps based on the expertise of a broad set of stakeholders.

- **Think Globally, act Locally**: It is through voluntary bottom-up self-organization that the most impactful solutions are likely to reached.

1 See "Internet Invariants: What Really Matters" http://www.internetsociety.org/internet-invariants-what-really-matters

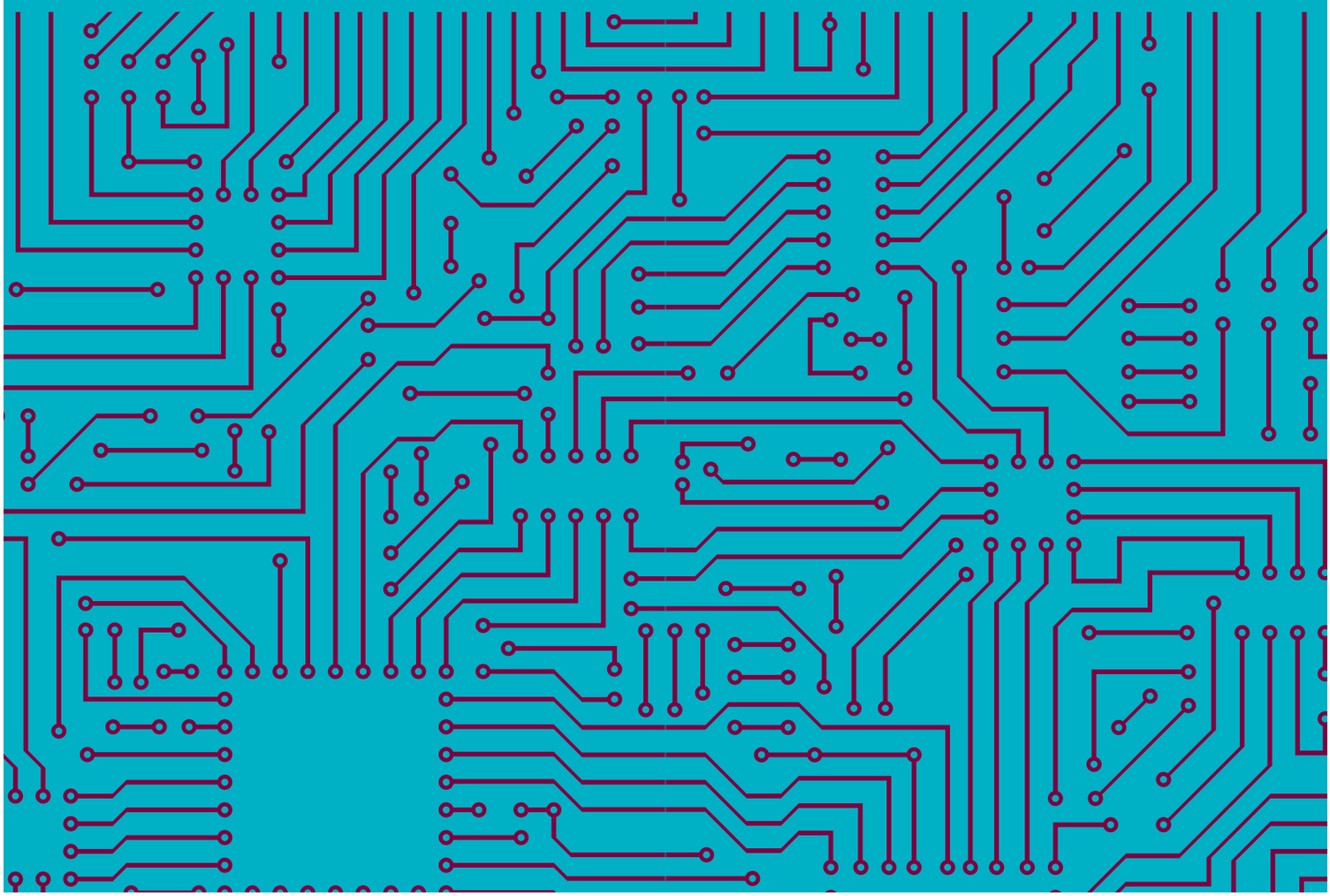
2 A more detailed description of the Collaborative Security approach is presented in the paper by the Internet Society "Collaborative Security: An approach to tackling Internet Security issues.", http://www.internetsociety.org/collaborativesecurity

ABOUT THE INTERNET SOCIETY

The Internet Society (http://www.internetsociety.org) is the trusted, independent source for Internet information and thought leadership from around the world. It is also the organizational home to the Internet Engineering Task Force (IETF). With its principled vision and substantial technological foundation, the Internet Society promotes open dialogue on Internet policy, technology, and future developments among users, companies, governments, and other organizations. Working with its members and Chapters around the world, the Internet Society enables the continued evolution and growth of the Internet for everyone.

8 CYBER SECURITY AND THE INTERNET OF THINGS

Koen Gijsbers
General Manager
NATO
Communications and Information Agency



Gartner predicts that the number of devices connected to the internet will increase by 35% per year in the coming years, with total numbers exceeding 20 billion by 2020. A future world where everything is connected and reporting information opens up many exciting possibilities – most of which have not been thought of as yet. The ability to combine data coming from different sources will allow the exploitation of connections not previously foreseen and should lead to more reliable decision making. However, this exponential growth presents also enormous challenges from a number of perspectives, not the least of which is cyber security. Can we evolve our cyber security posture at pace with this accelerating proliferation of devices?

We see that securing the Internet of Things will present a number of new and significant challenges:

1. **Trust**: Cyber security is normally considered along the three axes of: confidentiality, integrity, and availability of data. It is fair to say that the threat in the past has largely been focussed on the first and last of these. Attacks on confidentiality, trying to steal data such as military secrets or personal banking details etc., and attacks on availability, attempting to deny our ability to access data or deliver services via Distributed Denial of Service (DDoS) or virus attacks, have been the main worries in the traditional internet.

   IoT implementations will need to place much more emphasis on the third axis: data integrity. IoT sensors provide data, the purpose of which is ultimately to contribute to information used by a decision maker (human or machine) to make a decision and influence an outcome. Decision makers need to be able to trust the data they are presented with for making these decisions. If the adversaries can enter the network and manipulate the data, they can enter the 'decision loop' and might be able to cause poor decisions to be made or otherwise bias decisions in their own favour. For example, an adversary might attack sensors involved with building control systems, causing them to give false readings and thus perhaps causing operators (or automated systems) to take inappropriate actions such as turning up the temperature in a data centre causing expensive equipment damage and potentially data loss. In hospitals they might manipulate data provided by patient monitoring systems, causing inappropriate drugs to be administered or otherwise causing patients harm. On the battle field the consequences of falsified data can be nothing short of disastrous. If, for example, an adversary is able to alter location information, then he might be able to stimulate friendly fire incidents or deceive us regarding his true intent or abilities.

   We will need to develop solutions that increase the trust we have in our data. This might be by securing and authenticating the things and their data, by quickly and reliably detecting deception attempts and cleansing the data, or by developing techniques for reliable decision making in an environment where untrustworthy data is the norm.

2. **Cost and scalability**: While the cost of individual things is expected to be very low, currently the cost of securing them might be prohibitively high from either a financial and/or energy perspectives. In many instances, for example where unattended sensors and wearables are used, energy is limited so authenticating devices and encrypting data at the sensor may prove to be prohibitive as traditional public-key based techniques are generally computationally intensive and thus high consumers of scarce resources. At the same time management of symmetric keys across a network containing millions of heterogeneous devices might become too complex to be reliable.

   New and scalable techniques will need to be developed to deal with this if we are to have large penetration of IoT into high security environments.

3. **Dynamics**: Because in many situations devices can number in the thousands or millions and can be very mobile, it is anticipated that the network will be very dynamic, characterised by a constantly changing topology and composition, with devices constantly joining and leaving. Knowing the state of the network and being able to constantly update it and manage it may prove to be a challenge. Updating device software, for example, to provide patches against new vulnerabilities in a trusted way will also be challenging where we may have countless devices from countless different manufacturers deployed. Detecting and isolating compromised or faulty devices might also be difficult to achieve.

   It may be in some situations that not only individual devices join and leave the network, but entire clusters or subnets of users federate together to common purpose. How we trust each others' security in such federated environments, such as we might see in coalition operations, also becomes an issue. There are levels of the trust that may need to be established: do we trust the federated partner to join the network and not disrupt our network and data; do we trust them enough to use their data in our decision making; and finally do we trust them enough to share with them our data to be used in their decision making?

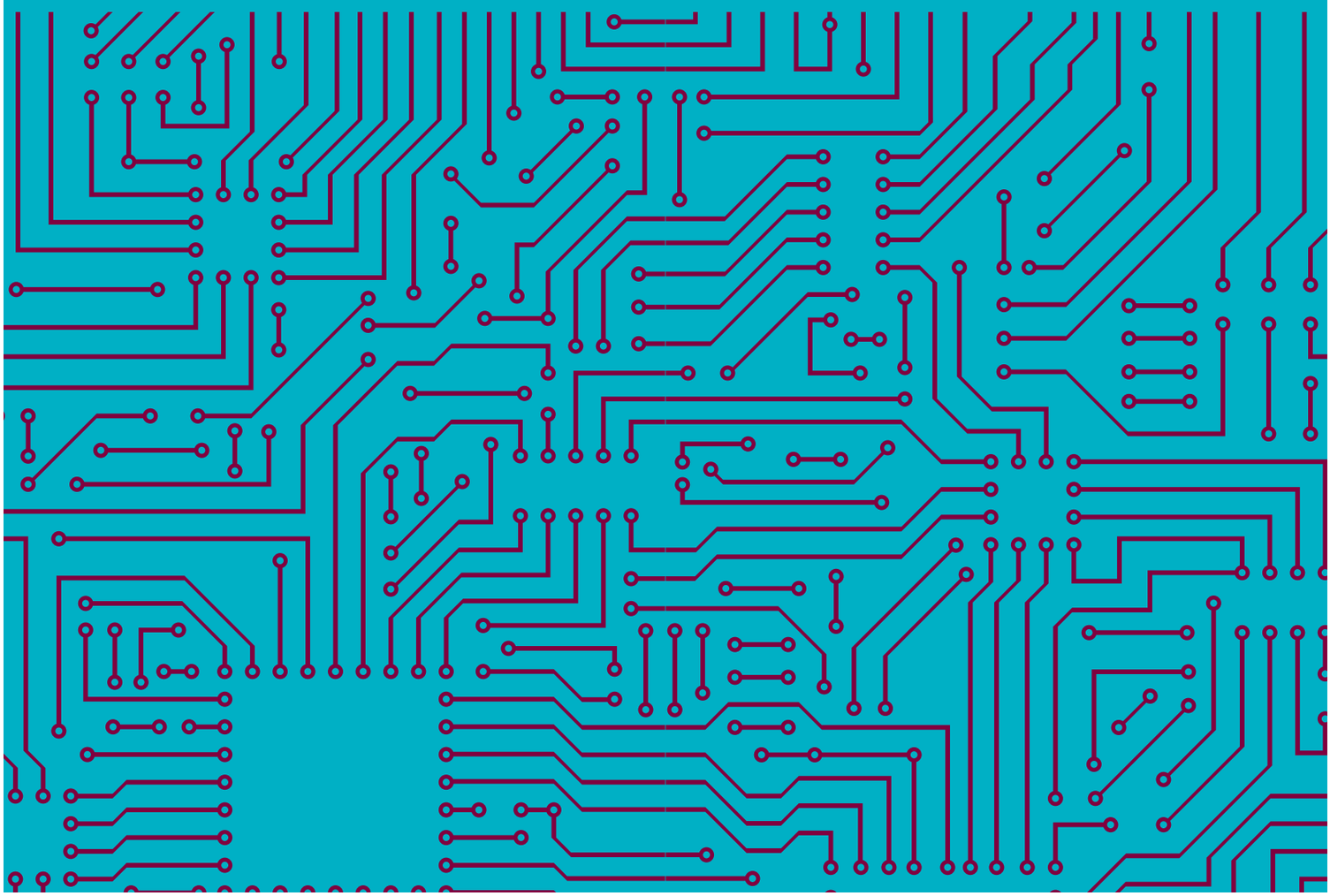
4. **Business Models**: Business models will be disrupted with smart objects perhaps being sold at a loss (or even given away) as companies will prefer to monetise data or data processing instead, leading to the so-called 'algorithmic economy'. As it is unlikely that any sector will be in a position to develop 100% of its own unique IoT devices and infrastructure, these business approaches raise the potential that data collected in high security environments, such as banking and military, may need to be sent to a commercial cloud in order to be processed into actionable information. Replicating the industrial capability for each type of device may simply be cost prohibitive. In the military this will also present challenges with bandwidth in tactical situations, where dismounted soldiers operate with limited or intermittent connectivity.

Security of IoT will quickly become everyone's problem; it is not something unique to the military. Whether the cyber attack is on a hospital, the banking sector, the military or private industry the consequences can be equally devastating to the entity or even the nation's security. Therefore, there is a strong need for all sectors to work together to solve some of the fundamental problems. There is a need for rapidly developing standards for low-overhead but high-robustness methods of authentication and security in order to increase the trust that can be placed in the data. Developing interface standards and agreeing architectures will facilitate the ability to rapidly deploy and integrate new types of devices. Developing management protocols that can be used across the industry to manage the IoT will be paramount. The community working these challenges needs to include both the sectors contemplating use of IoT solutions in their business, and also the manufacturers of the devices, components and infrastructure, as well as the system integrators that will deliver overall solutions. Funded innovation forums that bring together Government, military, industrial and academic players, should be established to facilitate this cooperation and demonstrate results according to accelerated timelines.

IoT presents us with enormous potential for disrupting each of our businesses, doing things that were simply never possible before, but it also provides us with huge challenges if we are to create this new world in a way that is secure from attack or unwanted exploitation. If we sit back and do not participate actively in shaping this IoT landscape, we will perhaps not be in a position to reap the promised rewards or may inadvertently expand the surface exposed to new and more threatening forms of cyber attack.

9 ADVANCING CYBERSECURITY IN THE INTERNET OF THINGS

Jochem de Groot
Manager Government Affairs
Microsoft



INTRODUCTION

Microsoft appreciates the opportunity to provide these comments to the Dutch Cyber Security Council on the cybersecurity issues posed by the growing connectivity of devices. The Internet of Things (IoT) represents an enormous opportunity to increase the level of participation and value of online activities. There will be an estimated 50 billion internet connected devices by the year 2020 potentially resulting in trillions of dollars added to the global economy. Through IoT, a much larger number of physical objects will be able to communicate and exchange data with other objects, with Web services, and with people. The majority of this communication will be between objects equipped with embedded sensors and actuators that can sense, measure, record, and/or act on aspects of their environment, and transmit that data autonomously – for further analysis or parsing against other data. Such detailed information about our environment and people has never before been available. This will provide a far more granular understanding of the interplay between many different factors, blurring the line between the physical and digital worlds. Therefore, IoT will revolutionize how individuals interact with their physical environment.

THE POTENTIAL IMPACT OF IOT

Today, people must master a multitude of devices to control and manage their environment. For example, thermometers must be set at appropriate temperatures for day and night; cars must be driven at what are considered safe speeds given existing traffic, weather conditions, and the need to arrive at a pre-determined destination at a given time; and so on. With the IoT, smart objects collect data and sense their environment, enabling services that are personalized to individuals' preferences and needs for the given context (e.g., home, work, social) – connecting them to appropriate content and expertise. These services bring people closer through shared experiences, enabling seamless and new ways to interact across the physical and virtual worlds. Physical objects move seamlessly between those worlds, adapting themselves appropriately to the different spaces, blending the two worlds to create a richer environment.

IoT will bring computing capabilities such as automation, analytics, and decision making to sectors including to manufacturing, energy, smart cities, healthcare, transportation, retail, and also governments. While many sectors have already been significantly transformed by computing, IoT represent a more ubiquitous and integral application of technology. We are only at the beginning of the development of the IoT. As the technologies continue to evolve, the dynamism, automation, and new knowledge that are enabled as a consequence render the world that we are moving into a promising future. Nevertheless, the full scope of the issues and opportunities is not yet well understood. There are still many unknown questions, let alone any pretension of answers. Therefore, developers and policy makers need to be educated on the impact and implications of IoT.

CYBERSECURITY IMPLICATIONS OF IOT

While the Internet of Things holds great promises for consumers, industry, and governments, the increasing connectivity does also pose challenges related to security and privacy that need to be addressed. To the extent that IoT is an extension of current platforms and networks, many of the same risks to confidentiality, integrity, and availability of data do apply. However, the heterogeneity, distribution, and global nature of IoT presents new challenges to security and privacy.

Microsoft and our partners have been working to make computing experiences more trustworthy for a very long period of time. The significant growth of connected devices and data flows combined with more sophisticated attacks and well-organized attackers are posing higher levels of complexity, which require robust cybersecurity investments and solutions.

In such a distributed ecosystem, it will be critical that participating stakeholders consider the following technical and public policy elements to enhance the security and resiliency of an IoT-enhanced world:

- **Secure by design, secure in development and secure in deployment (SD3)**: IoT devices and services should be designed and developed in manner that improves security and privacy during the lifecycle of the device by applying secure software development processes such as Microsoft's Security Development Lifecycle.

- **Secure communications**: Presumably, in the future many IoT devices will operate on the public Internet or on other networks where they may face a variety of threats to data confidentiality. IoT devices and services should utilize strong encryption techniques to protect data, and networks should use the latest communication protocols and up-to-date security architecture. On IoT devices that host third-party applications, the security of these communications needs to be addressed as well. Some more primitive IoT devices will lack the ability to perform encryption themselves. In such cases, one possible solution would be to design the device to allow its data to be encrypted by an intermediary gateway device on the local network before the data is sent over the Internet.

- **Manageability and security updates**: Many IoT devices will likely be built for single purpose applications and will have limited input/output capabilities to manage the device. IoT devices need to be designed to apply important functionality and security updates, preferably with the option of automatic updates requiring little or no administrator interaction. Devices should be designed to respond to security issues impacting devices, services, or applications. Awareness of the security or privacy issues related to other services and devices with dependencies should also be accounted for in update planning. IoT devices lacking the physical requirements for manageability and updates should be designed to allow security management by an intermediary gateway device on the local network before the data is sent over the Internet – as one possible solution.

- **Global Standards**: Internationally-developed standards based on a voluntary and market-led process with industry participation are best positioned to enable IoT adoption across the EU and integration with the global IT market. Standards can also help to improve the state of cybersecurity and promote innovation through commonly-understood practices and requirements.

- **Harmonization of Policies**: A single market following international standardization is necessary to ensure a consistent approach to IoT and cybersecurity. The development of national efforts that would lead to a further fragmentation should be avoided, as it could hinder IoT to enfold both its economic as well as social positive impact. We therefore urge the EU to harmonize this policy space and to help drive the Digital Single Market for IoT and cybersecurity.

It is critical that we work through issues in security early on to encourage an IoT built on trustworthy devices and services. The IoT is new and exciting, but we should not miss the opportunity to learn from our current and past investments in security. An analytical approach to the impact of our cybersecurity investments can help to maximize the value of IoT in Europe and around the world.

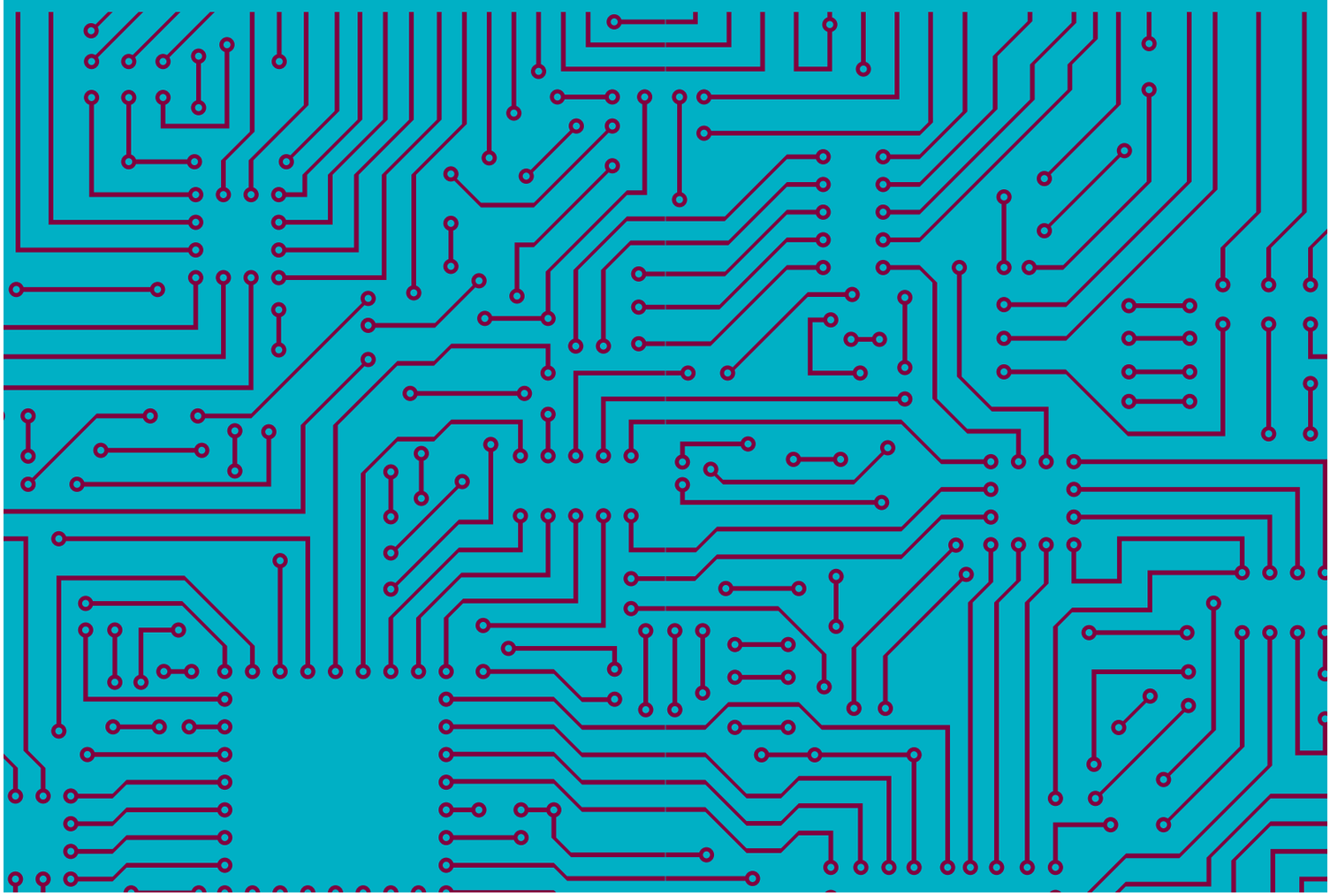
Microsoft looks forward to continue its cooperation with the Dutch Cyber Security Council, as well as the European Union, on IoT cybersecurity matters and other important technology policy issues.

10 TOWARDS HARMONISED DUTIES OF CARE AND DILIGENCE IN CYBERSECURITY

Radboud University

By Dr. Paul Verbruggen*
Dr. Pieter Wolters*
Prof. dr. Mireille Hildebrandt**
Prof. dr. Carla Sieburgh*
Prof. dr. Corjo Jansen*

* Business and Law Research Centre (OO&R)
Radboud University, Nijmegen, the Netherlands
http://www.ru.nl/law/research/business-law/
** Institute for Computing and Information Sciences (iCIS)
Radboud University, Nijmegen, the Netherlands
http://www.ru.nl/icis



Radboud University

CONTENTS

PREFACE

This White Paper was commissioned by the Dutch Cyber Security Council as part of the National Coordinator for Security and Counterterrorism, residing under the Ministry of Security and Justice. It provides a framework for discussion around the need to harmonise legal standards for duties of care and diligence in cybersecurity related to ICT goods and services, and offers proposals to better protect the interests of consumers of such goods and services.

The White Paper was drafted by dr. Paul Verbruggen, dr. Pieter Wolters, prof. dr. Mireille Hildebrandt, prof. dr. Carla Sieburgh, and prof. dr. Corjo Jansen.

We would like to acknowledge the comments and suggestions of the members of the supervising committee in preparing the White Paper: Liesbeth Holterman (Nederland ICT), Danny ter Laak (Parket-Generaal, Openbaar Ministerie), prof. dr. Lokke Moerel (Tilburg University, Morrison & Foerster LLP, member Cyber Security Council), Reinout Rinzema (Ventoux Law), Peter van Schelven (self-employed legal council), Ronald Verbeek (CIO Platform) and Maurice Wesseling (Consumentenbond).

The views expressed in this White Paper are those of the drafters only.

Nijmegen, May 2016.

EXECUTIVE SUMMARY

Information and communication technology (ICT) is ever more central to Europe's economic growth. However, as society becomes more and more dependent on ICT goods and services, the risks and costs of its disruption, failure or misuse increase. Consequently, **ensuring the confidentiality, integrity and availability of ICT (i.e. cybersecurity**) **constitutes a crucial pillar on which the use of ICT must be based in Europe and beyond**.

Yet, the question of who is responsible for ensuring cybersecurity is not easy to answer, in part due to the diversity among legal frameworks of EU Member States related to cybersecurity. **The Digital Single Market strategy launched by the European Commission in May 2015 offers a clear momentum to address, in a uniform and harmonised way, this legal fragmentation and resulting uncertainty.** This White Paper therefore offers a framework for discussion around the need to adopt harmonised duties of care and diligence for **cybersecurity in relation to ICT goods and services offered to consumers**. The paper does not address any sector-specific regulation adopted at EU or national level relating to cybersecurity, such as critical infrastructures, energy, health and finance. It further assumes the entry into force of the General Data Protection Regulation and the Network and Information Security Directive and does not offer suggestions on the topics covered by these legislative instruments.

The White Paper starts from the assumption that **any individual who has suffered a loss because of a lack of cybersecurity should have effective legal remedies against the actor responsible for providing such security.** In seeking to remedy these losses a consumer now encounters serious legal obstacles. It might first of all be difficult for a consumer to establish that the ICT provider owed a duty of care to him/her, what that duty implies given the circumstances, and whether the duty was in fact breached. While the fields of law applying to this context (sales, contract, unfair commercial practices, and tort law) offer various frameworks and concepts to provide answers to these pressing questions, they have so far only rarely been applied by courts in relation to cybersecurity issues. Consequently, there is **little legal certainty** as regards the question what actors in the ICT supply chain are required to do in terms of cybersecurity and, in turn, to what extent consumers can hold them to account for the lack of it. The question of who is responsible for the security of ICT goods and services is increasingly difficult to answer in the important development of the **Internet of Things** (IoT) as this development depends on the interconnection of multiple business actors in the provision of goods and services to consumers. Moreover, ICT providers typically use

extensive **exemption clauses** to limit or exclude their liability in contracts concluded with consumers. Enforcement by public enforcement authorities is typically not concerned with providing remedies to consumers who suffered damages because of a security breach.

Consequently, there are few regulatory incentives for business actors in the ICT supply chain to ensure the security of the ICT goods and services they provide to consumers. We contend that **a uniform legal benchmark requiring the use of appropriate technical and organisational measures (i.e. security by design)** by ICT providers when placing on the market goods or services will provide important new incentives for the ICT sector to ensure cybersecurity across the entire ICT supply chain and increase legal certainty for both business and consumers around duties of care and diligence in cybersecurity.

Below we identify a set of circumstances that must be considered significant when determining the relevant duty of care, after which we offer a number of recommendations. We use the term 'ICT goods and services' to collectively denote ICT systems, infrastructures, networks, hardware, firmware, software, applications and digital content. If more specific terminology applies, this will be specified. We kindly refer to the Glossary of terms annexed to this White Paper for the exact definitions used.

We recommend that **in assessing whether a duty of care and diligence has been breached in a specific case, the following circumstances should at least be taken into account**:

- The purposes for which similar ICT goods or services are normally used;
- The purpose for which the consumer requires the ICT goods and services, as communicated to the ICT provider;
- The legitimate expectations of the public at large;
- The presentation of or public statements about the goods and services by the ICT provider;
- Any foreseeable or irresponsible (mis)use by the consumer;
- The nature and severity of the risks poses by the ICT goods or services to consumers;
- The nature and severity of the damages involved;
- The state of scientific and technical knowledge at the time the ICT provider placed the ICT goods and services on the market;
- (Non-)compliance with accepted private industry standards.

This White Paper also offers the following **recommendations** concerning a specific set of topics **to harness the legal position of consumers** in the case of a lack of cybersecurity.

- ICT providers should be required to offer, in a clear and comprehensible way, information to consumers about their contractual obligations to ensure cybersecurity before they enter into a contract with consumers, including information about when, how, to what extent and for how long an ICT service provider or a producer or seller of goods with embedded ICT components, will provide updates or upgrades to consumers.
- Cybersecurity should be recognized as a main characteristic of ICT goods and services. As such, it should be part of a conformity assessment related to these goods and services.
- Sellers of consumer goods should not be able to contract out the confidentiality, integrity and availability of embedded ICT or digital content for the normal life-span of these goods. Also suppliers of digital content should not be able to contract out such matters in relation to this content for the duration of the related services contract.
- Consumers should have the right to be compensated for the damages they suffered due to any non-conformity with regard to the security of ICT goods and services. The recoverable damages should not be limited to material damages and should also include immaterial damages, in line with Article 77 of the General Data Protection Regulation.
- General terms and conditions related to consumer contracts of ICT goods and services must meet the requirements of fairness and transparency as laid down by the Unfair Contract Terms Directive. National courts, public enforcement authorities and consumer representative bodies should intervene proactively within the scope of their respective competences to better address the use of unfair terms by businesses in the ICT sector in consumer contracts.

- The material scope of the Product Liability Directive should be revised so as to include software. The 'development risk defence' as allowed under this Directive should not be interpreted extensively such as to exclude the liability of producers for the release, updating and upgrading of software that disregards known and knowable security vulnerabilities.
- Consumers should be able to recover from businesses liable under the Product Liability Directive damages to hardware devices or damage related to the loss of digital content. We propose to consider whether and to what extent consumers of software, whether or not embedded in a product, should have the right to claim material and immaterial damages from the producer based on the strict liability system as set out in this Directive.
- Businesses placing on the market ICT goods and services should be required to control, monitor and inspect these goods and services in terms of security vulnerabilities throughout the normal life-span of these products or for the duration of the related services contract.
- We recommend investigating whether and how existing EU legislative instruments intended to improve consumer access to justice (e.g. the Injunctions Directive, the ADR Directive and the ODR Regulation) may be applied effectively to provide consumer protection in relation to disputes with traders concerning cybersecurity.

1. INTRODUCTION

Information and communication technology (ICT) is ever more central to Europe's economic growth. It offers new opportunities to respond to business demands, consumer needs and pressing societal challenges. However, as society becomes more and more dependent on ICT goods and services (e.g. systems, infrastructures, networks, hardware, firmware, software and applications), the risks and costs of its disruption, failure or misuse increase. Consequently, ensuring the confidentiality, integrity and availability of ICT – discussed here as *cybersecurity* – constitutes a crucial pillar on which the use of ICT must be based in Europe and beyond.

The **aim** of this White Paper is to provide a *framework for discussion around the need to harmonise legal standards for duties of care and diligence concerning cybersecurity and offer proposals to better protect the interests of non-commercial end-users of ICT (i.e. consumers and data subjects) in terms of the confidentiality, integrity and availability of ICT goods and services, and data (including personal data) handled through them.* In practice, the costs of cyber *in*security are typically born by consumers and data subjects, rather than the business actors offering the ICT goods and services (i.e. *ICT providers*), including hardware producers, software and application developers, Internet service providers, telecom operators, digital content suppliers and retailers. Regardless of any responsibilities on the part of individual users, these users face numerous **hurdles to ensure effective remedies** against disruption, failure or misuse of ICT, including the compensation of damages sustained as a result thereof. This is in part due to legal uncertainty, as well as limited and diverse legal frameworks of the Member States.[1]

There is a clear **momentum** to address, in a uniform and harmonised way, this legal uncertainty and fragmentation. In May 2015, the European Commission launched an ambitious strategy for a *Digital Single Market*, which also fundamentally concerns cybersecurity.[2] Important new legislation is on its way in the areas of data protection and network and information security,[3] and new proposals have recently been submitted as part of this strategy to strengthen the protection of consumers of digital content (including

1 E. Tjong Tjin Tai e.a., 'Duties of Care and Diligence against Cybercrime', report for the Dutch National Coordinator for Security and Counterterrorism (March 2015), https://www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Duties%20of%20care%20and%20diligence%20against%20cybercrime%20(1).pdf (accessed 1 May 2016).

2 European Commission, 'A Digital Single Market Strategy for Europe' COM(2015) 192 final, p. 13.

3 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final, Brussels, 25.1.2012 (latest version as adopted by the European Parliament 15 December 2015) and the Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM (2013) 48 final, Brussels, 7.2.2013.

software) and in online sales contracts.[4] It is therefore timely to also **critically discuss the general legal framework in the European Union (EU) applying to the sale of goods and services by ICT providers to consumers**. This White Paper offers suggestions on how this framework can be amended to further harness the legal position of consumers in remedying a lack of cybersecurity, including the right to compensation of damages for the disruption, failure or misuse of ICT goods and services, including the personal data handled through them. The White Paper will not address any sector-specific regulation adopted at EU or national level relating to cybersecurity, such as critical infrastructures, energy, health and finance. The paper further assumes the entry into force of the General Data Protection Regulation and Network and Information Security Directive.[5] It therefore does not offer new suggestions on the topics covered by these legislative instruments.

2. PROBLEM ANALYSIS

The increasing dependence on ICT goods and services in today's society highlights the need to ensure their security. A lack of confidentiality, integrity and availability of ICT is likely to translate into direct or indirect, material or immaterial damages for businesses, consumers and data subjects concerned. **Any individual** who has suffered a loss because of the failure to deliver cybersecurity should have effective remedies against the responsible actor.

2.1 Legal uncertainty as regards duties of care

However, when seeking to remedy cyber insecurity, individual users frequently find themselves confronted with serious legal obstacles that prevent them from actually bringing a claim against the ICT provider in court. It might first of all be **difficult to establish whether a duty of care owed to the user, what the duty may imply given the context, and whether that duty was in fact breached**. An illustration is provided by a recent case in the Netherlands, which has received much attention from abroad.

Stagefright: Consumentenbond v. Samsung Electronics Benelux B.V.[6]

In July 2015 it was announced that Google's Android system was vulnerable to the so-called 'stagefright' bug, as a result of which smart phones operating on this system could be remotely accessed, allowing the attacker to read and delete data, and to spy on the user through operating the smart phone camera and microphone. In October 2015 a new version of the bug, stagefright 2.0, was publically announced.[7] Samsung's smart phones operate on the Android system and as a result some of the older models of its phones proved vulnerable. However, Samsung did not warn users of its smart phones about the bug, nor did it patch the security threat by providing updates or upgrades for its older models.

Therefore the Consumer Association in the Netherlands – *Consumentenbond* – decided to bring legal proceedings against Samsung requesting the court to provide interim injunctive relief. More specifically, Consumentenbond petitioned the court, amongst others, to require Samsung to (i) provide to the users of its vulnerable mobile phones information about the bug, (ii) provide security updates for Android bugs considered critical by Google for all smart phone models having this bug, and (iii) provide security updates for all smart phone models introduced in the Netherlands within the last two years and in the future. It based these claims on requirements under national laws of unfair commercial practices, sales, tort and data protection, which are all (some more than others) harmonised by EU law. According to Consumentenbond Samsung holds a

4 European Commission, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contract for the supply of digital content, COM(2015) 634 final, Brussels, 9.12.2015, and the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sale of goods, COM(2015) 635 final, Brussels, 9.12.2015.

5 See at note 3.

6 District Court of Amsterdam (President), Case C/13/600958 / KG ZA 16/51.

7 https://www.theguardian.com/technology/2015/jul/28/stagefright-android-vulnerability-heartbleed-mobile (accessed 1 May 2016).

market share of some 40% in the Dutch smart phone market, while over 80% of its smart phones are vulnerable to the stagefright bug.

The judge hearing the application for interim relief did not grant injunctive relief. The main reason for this decision was the finding that Consumentenbond had not provided sufficient evidence showing the urgency required for interim relief. Expert witnesses of Samsung testified that the stagefright bug does not constitute a security breach, but merely a weakness in Google's Android software. Misuse of that vulnerability would prove to be very complex, expensive and time consuming. As a result, a successful use of this weakness would be extremely limited. Documentary evidence provided by Consumentenbond did not disconfirm this, and neither could Consumentenbond furnish proof that a Samsung smart phone was hacked outside the testing environment. Furthermore, the interim relief requested was not considered appropriate as this would have considerable technical implications and costs for Samsung, whereas for the updating of their smart phones they would be dependent on Google's collaboration for they operate the Android system. With regard to the request to grant an order to provide information to smart phone users about the stagefright bug, the judge held that Samsung had already provided additional information on its website and that the question whether this information would be sufficient could not be answered based on the evidence provided by Consumentenbond.

Consumentenbond failed in its claims because it could not satisfy the specific requirements under national procedural law for summary proceedings. As a result, the judge did not consider the case in substance. Nevertheless, the case raises a number of very fundamental questions concerning the debate on duties of care and diligence in cybersecurity, including:

- Can a producer of smart devices be required to offer updates or upgrades for the software embedded in the device if that software proves to be vulnerable in terms of cybersecurity?
- Does such a duty exist independently of the fact that the vulnerable software is provided by a third party?
- In what time frame would such a duty to offer updates or upgrades exist? Would the producer be required to continue to provide updates or upgrades only shortly after the product is sold, for the normal life span of a product, or during its entire life cycle?
- Should the producer inform a consumer about what he/she can expect in terms of cybersecurity before a contract is concluded?
- Is the potential risk of disruption, failure or misuse of ICT sufficient to constitute a breach of contract even if the risk has not materialized in reality?

So far, questions such as these have hardly been addressed by courts in the Member States. While **the law as it stands offers various frameworks and concepts to provide answers to these questions, in particular in the fields of sales, contract, unfair commercial practices, and tort law**, few cases have come to the courts in which these frameworks and concepts could be applied and interpreted extensively to allow for remedies against insecure ICT goods or services. Consequently, there is little legal certainty as regards the question what actors in the ICT supply chain are required to do in terms of cybersecurity. This begs the political question of whether legislative intervention is needed at the European level in order to a lay down a clear and uniform legal framework regarding these duties of care and diligence.

2.2 Internet of Things

The discussion around the existence and scope of duties of care and diligence in cybersecurity is likely to gain further prominence in the light of the development of the Internet of Things (IoT). In this development, which has been recognized by the European Commission as a major catalyst for economic growth, innovation and digitalization in Europe,[8] **the question of who is responsible for the security of ICT goods and services is increasingly difficult to answer in the IoT** as it presupposes the interconnection of multiple business

8 COM(2015) 192 final, p. 14. See more generally, European Commission, Communication on 'Internet of Things – An action plan for Europe', COM(2009) 278 final, Brussels, 18.6.2009.

actors in the provision of goods and services to users. The functionality of the products or devices connected through the IoT is no longer determined by the hardware itself, but increasingly dependent on multiple service providers.[9] As the **complexity of the ICT supply chain** increases, also responsibilities for cybersecurity become more and more blurred and intransparent. Who can be held responsible for what exactly?

To answer this question one should look at the contracts that provide the legal infrastructure for the dense network of actors in the IoT. These contracts, which may be explicitly or implicitly linked, each involve their own set of rules and procedures determining the respective rights and obligations of the contracting parties. It is very difficult for consumers to understand the contracts they conclude, the documentation related to them (e.g. terms of service, privacy policies, etc), and the contracts between the business actors to which the consumer contracts are linked.[10] Moreover, the consumer contracts are typically **contracts of adhesion** ('take it or leave it'), locking users into long-term relationships with ICT providers through simple click wrap agreements. Users are bound by the services, their terms of service (and to some extent the privacy policies) by simply clicking an 'OK' or 'agree' button.

Cybersecurity is of eminent importance to the IoT since this novel ICT development does not only enable the collection of much more personal data, but also more intimate data in both intrusive and dynamic ways.[11] These data are no longer simply a by-product generated by the use of the device, but feed into the device and related services provided by and through it in order to, so it is claimed, enhance their functionality. We may expect that the business models in businesses in the IoT will be personal data-driven, as with current search engines, social media, advertising networks and data brokers. In the event of unwarranted disclosure of personal data (data breaches) we can thus expect a privacy and data protection impact. However, even without such breaches harm may be caused where the data are combined across different context and allowing for prohibited or undesirable discriminatory practices (e.g. regarding insurance pricing, credit rating or employability).[12] Furthermore, some of the devices in the IoT are designed with safety purposes in mind, such as door locks, smoke alarms and self-driving vehicles. Vulnerabilities in the cybersecurity of the ICT systems underpinning these devices may not just lead to the loss and misuse of personal data, but also to physical harm.[13] Thus, **cyber insecurity may translate into physical insecurity**. This, again, underlines the acute need to ensure cybersecurity in our society, now and in the future.

2.3 Exclusion of liabilities

Another important legal obstacle for consumers to obtain effective remedies against the failure to provide cybersecurity concerns the use of general terms and conditions through

9 This is already the case now for an ordinary smart phones, where security problems can relate to the hardware providers, the provider of the operating system, the firmware, various types of integrated software, telecom providers, and the providers of a plethora of apps (which may be part of the smartphone by default or downloaded by the end-user), while these phones can be bought from various types of (online) retailers or be part of a service contract with a telecom provider.

10 In assessing the contractual regime underpinning the use of the Nest thermostat, one of the popular home devices with Internet connectivity, Noto La Diega and Walden content that Nest users need to at least read thirteen different documents to have a full overview of their rights and obligations vis-à-vis sellers, services providers, licensors and other third parties concerned with the operation of the thermostat and related services. See: G. Noto La Diega and I. Walden, 'Contracting for the 'Internet of Things': Looking into the Nest', Queen Mary University of London, School of Law, Legal Studies Research Paper No. 219/2016, p. 3-4, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725913 (accessed 1 May 2016).

11 Consider the smart watch that collects data about the physical condition of its wearer (pulse, body temperature, physical exercise through GPS, etc.) throughout the day, on the workplace and even in bed.

12 For example, the US-based insurance company Oscar uses personal data generated by insurance takers to set insurance premiums. See https://www.hioscar.com/about/ (accessed 1 May 2016).

13 There are various reports of smart devices of which the security was compromised and could result in extensive physical harm for users and third parties. For example, iOS software in cars was reported to be hacked, making it possible for a hacker to have control over certain aspects of a car, including the possibility to start it remotely. See: http://blog.caranddriver.com/researcherbmw-mercedes-vulnerable-to-remote-unlocking-hack/ (accessed 1 May 2016). Another example is provided by the smoke alarms of Nest, the company that also produces smart thermostats, included the feature 'Wave', whereby one could switch the alarm off by waving the hands. This feature has been disabled since April 2013, since 'movements near Nest Protect that are not intended as a wave can be misinterpreted by the Nest Wave algorithm. If this occurs during a fire, this could delay the alarm going of'. See https://nest.com/support/article/Nest-Protect-Safety (accessed 1 May 2016).

which business actors impose far-reaching duties on consumers and make extensive restrictions as regards their liability. The **use of exemption clauses in contractual arrangements is widespread**.[14] Through these clauses businesses seek to exempt or severely limit their liability in relation to cybersecurity issues. One extreme example of this strategy is provided by the toy manufacturer Vtech in the aftermath of a hack which left millions of user accounts of children exposed.

VTech

In November 2015, the online Learning Lodge Portal of the Hong Kong based toy manufacturer VTech was hacked, leaving some 4.8 million unique email addresses and personal data relating to hundreds of thousands of children (names, genders, birthdates, postal addresses, user names, passwords, etc) exposed.15 According to one influential observer, VTech 'allowed itself to be hacked' because it 'continued to run a service with such egregious security flaws (...)'.[16]

In response to this major security breach, VTech amended its Terms & Conditions of the Learning Lodge Portal. It now includes an extensive exemption clause that reads:

'YOU ACKNOWLEDGE AND AGREE THAT YOU ASSUME FULL RESPONSIBILITY FOR YOUR USE OF THE SITE AND ANY SOFTWARE OR FIRMWARE DOWNLOADED THEREFROM. YOU ACKNOWLEDGE AND AGREE THAT ANY INFORMATION YOU SEND OR RECEIVE DURING YOUR USE OF THE SITE MAY NOT BE SECURE AND MAY BE INTERCEPTED OR LATER ACQUIRED BY UNAUTHORIZED PARTIES (emphasis added).'[17]

This clause implies a full disclaimer as to the duty to provide cybersecurity on the part of VTech. It is highly doubtful whether this clause will hold in court proceedings.[18] While this is an extreme example, many actors in the ICT sector use such extensive exemption clauses for direct or indirect, material or immaterial damages caused by their devices and services. Rather common is the use of a clause phrased along the lines of 'any exclusions, disclaimers or limitation of liability provisions will apply to the extent permitted by local laws'. In the United Kingdom, however, the Competition and Markets Authority, which is the national public enforcement authority in the field of consumer protection, has stated that such wide exclusion clauses are both unfair and lack transparency.[19] This would entail that such clauses are inapplicable, meaning that companies relying on these clauses can be held liable for damages caused. The problem is that **consumers are frequently not aware of their rights** and we do not expect the liable parties to remind them of their rights.

14 The European Commission recognizes the widespread use of exemption clauses in cloud services: '(...) contracts often exclude, or severely limit, the contractual liability of the cloud provider if the data is no longer available or is unusable, or they make it difficult to terminate the contract. This means that that data is effectively not portable.' Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Digital Single Market Strategy for Europe' COM(2015) 192 final, Brussels, 6 May 2015, p. 14.

15 http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids (accessed 1 May 2016).

16 http://www.troyhunt.com/2016/02/no-vtech-cannot-simply-absolve-itself.html (accessed 1 May 2016).

17 VTech Electronics Europe plc, 'Terms and Conditions' Learning Lodge Support (update 24 December 2015), http://contentcdn.vtechda.com/data/console/GB/1668/SystemUpgrade/FirmwareUpdateTnC_GBeng_V2_20160120-170000.txt (accessed 1 May 2016).

18 In December 2015 a class-action lawsuit was filed against VTech Electronics North America and VTech Holdings Limited before the U.S. District Court for the Northern District of Illinois. See: https://www.bigclassaction.com/lawsuit/vtech-data-breach-class-action-lawsuit.php (accessed 1 May 2016).

19 Competition and Markets Authority, 'Unfair contract terms guidance. Guidance on the unfair terms provisions in the Consumer Rights Act 2015',31 July 2015 (CMA37), at para. 2.54-2.55, available at: https://www.gov.uk/government/ uploads/system/uploads/attachment_data/file/450440/Unfair_Terms_Main_Guidance.pdf (accessed 1 May 2016).

More generally, there is a **tendency in the private sector to deny any responsibility** whenever a weakness in the security of their network, infrastructure or services is exposed. Companies tend to freeze and entrench themselves in legal discourses on liability, rather than assuming responsibility (*not* liability) to improve and remedy the signalled shortcomings. A typical response by industry is provided by the example of the Volkswagen Group, whose encrypted electronic car keys proved rather easy to crack.

Volkswagen Group

In 2013, a research team of Radboud University (Nijmegen, the Netherlands) and the University of Birmingham (UK) publicly announced that they had dismantled the so-called 'Megamos Crypto transponder'.[20] This type of transponder is a passive RFID tag which is embedded in the key of the cars and is widely used in the automotive industry as an electronic vehicle immobilizer. The 'obvious' security gaps uncovered by the researchers could lead the dark minded to wirelessly lock pick cars.

In response the Volkswagen Group, who had used the specific transponder in millions of its cars, brought interim proceedings against the research team before the High Court of Justice in London, requesting a prohibitive injunction preventing the authors, their institutions, and anyone who assisted them, from publishing key sections of the paper. The High Court allowed the injunction for it found that the researchers had misused confidential information in software similar to that used by Volkswagen for its car keys (i.e. the Megamos Crypto algorithm), while Volkswagen cars depend on the secrecy of that information. As a result, the study could not be published containing the disputed algorithm.

Accordingly, rather than acknowledging the weaknesses exposed by researchers and improving electronic car key safety, the hardware producer's knee-jerk response was to file interim proceedings against them. Car owners with these specific keys are left to wonder about the security of their car locks, while the producer does not initiate any action (e.g. a product recall) to resolve the security issue. The spokesperson of the Dutch automotive industry suggested car owners to get a steering-column lock.[21] Similar responses to deny all responsibility to provide better solutions to security threats have been observed in relation to home wireless routers, which prove to be vulnerable for hackers by simply trying the default login password of the routers.[22] Importantly, the example of Volkswagen also shows that **manufacturers of products with significant embedded ICT components deny responsibility for failures of this software as if it is not an inherent part of the product they produced**. Instead, they point to the developer of the ICT involved. With modern products becoming more and more software-driven, it should be questioned whether this position is tenable under the law and whether producers can be held liable for damages caused by insecure ICT integrated in their products.

2.4 Public enforcement action

Enforcement by public authorities is typically not concerned with providing remedies to consumers who have suffered damages because of a security breach. These authorities have powers to impose penalties, but not to compensate damages suffered. These need to be compensated through civil court proceedings. More generally, **few public authorities in the field of competition, trade and consumer law have developed a mature policy strategy concerning cybersecurity.** Enforcement action is either pursued through individual court proceedings or, more likely, collective actions. Public enforcement action is principally concerned with the managing, monitoring and controlling of security breaches concerning personal data, typically in response to notifications by targeted data controllers and processors. Data protection authorities and supervisory bodies in the field of telecom are the

20 R. Verdult, F.D. Garcia & B. Ege, 'Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer', in: USENIX, *Supplement to the Proceedings of the 22nd USENIX Security Symposium*, Washington, DC: USENIX 2013, https://www.usenix.org/sites/default/files/sec15_supplement.pdf (accessed 1 May 2016).

21 Harald Bresser, spokesperson RAI Automobielindustrie, http://nos.nl/nieuwsuur/artikel/2051484-miljoenen-auto-s-te-hacken-door-gebrekkige-beveiliging-chip-autosleutel.html (accessed 1 May 2016).

22 A. Greenberg, '"Millions" of Home Routers Vulnerable to Web Hack', 3 July 2010, http://www.forbes.com/sites/firewall/2010/07/13/millions-of-home-routers-vulnerable-to-web-hack/#43ca6249a68c (accessed 1 May 2016).

central public actors here.[23] Budgetary restraints require these authorities to take focused action only, at times leading to sub-optimal outcomes in terms of protection. 'Rogue traders' and 'cowboys' may take advantage of the absence of any market access controls, and may offer digital services (applications) with very few security measures in place, or worse, with no security at all. As long as public authorities cannot keep these players from offering their services on the digital market place (e.g. through the introduction of approval or licensing systems), individual rights to ensure compensation for damages caused by insecure ICT must be available to complement public enforcement action.

2.5 Incentives to ensure cybersecurity

Combined with factors such as the **high costs of litigation** and the applicability of **foreign systems of law** under the rules of private international law, these circumstances are likely to lead end-users of ICT goods and services, in particular consumers, to abstain from pursuing their claims. Consequently, there are very few legal incentives for the private sector to ensure the security of the ICT goods and services they provide to users, both businesses and consumers. Economic incentives tend to be lacking as well, due to the **absence of information about and transparency of** cybersecurity issues at the consumer's end, limiting their ability to choose between different service providers based on how they provide the appropriate cybersecurity. The **costs of switching** to another service provider may also be high given the long-term service agreements into which consumers are enrolled through click-wrap contracts, thus limiting the ability of consumers to respond to cyber insecurity by choosing another provider.[24] As there are **few regulatory and market incentives** for actors in the ICT supply chain to ensure cybersecurity, legislative intervention by the EU is desirable.

3. NEED FOR HARMONISATION

Cybersecurity constitutes a crucial pillar on which the responsible use of ICT must be based. Users of ICT systems depend on the security of these systems to engage in economic transactions (online sale of goods and services), politics (voting machines, e-voting) and social life (social media). **A lack of cybersecurity will translate into distrust** of important aspects of daily life.

The European Commission recognizes the salience of cybersecurity for economic growth in Europe in its Digital Single Market strategy adopted in 2015. In its strategy it places great emphasis on the security in digital services and in the handling of personal data for public trust in online activities and the digital economy in general. More specifically, it holds:

> "Specific gaps still exist in the fast moving area of technologies and solutions for online network security. A more joined-up approach is therefore needed to step up the supply of more secure solutions by EU industry and to stimulate their take-up by enterprises, public authorities, and citizens."[25]

Harmonising legal duties of care and diligence in cybersecurity will help to further strengthen public trust in ICT goods and services. Harmonisation will also address important aspects of the problems highlighted above. It will first of all increase **legal certainty** for both consumers and businesses. All actors will be able to rely on a uniform legal framework based on clearly defined legal concepts regulating central aspects of cybersecurity across the EU. The laws stipulating duties of care and diligence in cybersecurity are currently only in part harmonised. While the General Data Protection Regulation will provide a new uniform standard for data protection in Europe,[26] including rules for the recovery of damages by individuals suffering damages because of a violation of the Regulation, the general legal

23 Tjong Tjin Tai e.a. 2015 (note 1), p. 141-142, 144.

24 See in the domain of cloud computing the discussion paper by Expert Group on Cloud Computing Contracts, 'Switching – Data portability upon switching' (January 2014) http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_topic_4_switching_en.pdf (accessed 1 May 2016).

25 European Commission, 'A Digital Single Market Strategy for Europe' COM(2015) 192 final, p. 13.

26 See note 3.

framework concerned with the compensation of damages caused by a lack of cybersecurity beyond data protection differs strongly among Member States. A **uniform legal benchmark requiring the use of appropriate technical and organisational measures (i.e. security by design) proportionate to the cybersecurity risks posed by goods or services sold by ICT providers to consumers** will further the free movement of these goods and services in the EU internal market, reduce unfair competition between businesses based in different jurisdictions, and may help to protect users against the loss of personal data, digital content, and even physical health.

We anticipate that removing the current barriers stemming from the fragmentation of the legal framework discussed above, will strengthen the legal position of consumers to recover damages, thus stimulating the private sector to ensure higher levels of confidentiality, integrity and availability of ICT. A demand for a high level of cybersecurity will also foster technological development and innovation in that field, offering industry the chance to roll out effective security solutions worldwide. Increased cybersecurity will bolster Europe's economic growth, whilst also providing secure ways to collect and process personal data to help address pressing societal challenges, including aging, environmental degradation and organised crime.

4. TOPICS FOR HARMONISATION

This White Paper presents a specified set of topics suitable for harmonisation with a view to harness the legal position of consumers in recovering damages sustained due to a lack of cybersecurity. The topics have been selected upon thorough analysis of the existing legal framework, its application in practice, and through repeated engagement with the ICT sector, concerned NGOs and government authorities.

The measures proposed here extend beyond national approaches to market economies and related public and private ordering. In general, complex policy objectives require the capacities of both public and private actors to address challenges in delivering these objectives. Also for the policy area of cybersecurity, it has been stressed on several occasions that such security can only be attained by a combination of public and private law measures.[27]

4.1 Pre-contractual information duties

Consumers need reliable and comprehensible information to make a well-informed decision when entering into a contract for the provision of ICT goods and services. Such **transparency enables efficient economic transactions.** There are several instruments of secondary EU legislation in which businesses are required to disclosure the main characteristics of ICT goods or services before a contract is enter into by the consumer,[28] yet cybersecurity has not been identified as such a main characteristic.

It is suggested that where ICT goods and services are concerned these legislative measures should be read as including the obligation for businesses to inform consumers in a clear, meaningful and comprehensive way about their obligations under the contract to ensure the confidentiality, integrity and availability of the ICT involved. **Information about when,**

27 OECD, '*Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (OECD, Paris 2012), available at: http://oe.cd/cybersecurity-strategies (accessed 1 May 2016), p. 13, 15, 31 and 32, the EU Cybersecurity strategy JOIN(2013) 1 final, Directive 2013/40/EU (Recital 23), and the White House Summit on Cybersecurity and Consumer Protection, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit (accessed 1 May 2016).

28 Generally these pre-contractual information duties concern the main characteristics of the service, identity of the trader, price, arrangements for payment, delivery, and performance, right to withdrawal, duration of the contract, and out-of-court complaint and redress mechanisms. See for example Articles 5 and 6 Directive 2000/31/EC **of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market** (E-commerce Directive), OJ L 178, 17.07.2000, p. 1-16, Article 22 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, OJ L 376, 27.12.2006, p. 36-68 and Article 5 and 6 Directive 2011/83/EC of the European Parliament and of the Council on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ *L* 304, 22.11.2011, p. 64-88 (Consumer Rights Directive).

how, to what extent and for how long a business will provide the consumer with updates or upgrades of the ICT goods or services must be offered. Cybersecurity should be regarded as a key characteristic of these goods and services and, accordingly, accurate information about it should be provided to consumers. If the updates or upgrades are only available upon additional payment or via **additional service contracts** (including maintenance or end-user license agreements - EULAs), this should also be disclosed. Accordingly, consumers are enabled to make a more informed and efficient transactional decision.

Furthermore, the Unfair Commercial Practices Directive lays down rules for businesses when engaging in commercial practices vis-à-vis consumers.[29] It prohibits commercial communications, including advertising and marketing, by a business (the 'trader') related to the promotion, sale or supply of a product to consumers that are unfair. The Directive holds that a commercial practice is unfair if it is contrary to requirements of professional diligence and it materially distorts or is likely to materially distort the ability of the average consumer to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken otherwise.[30]

We need to investigate **to what extent the omission of information about the obligations of the business under the contract as regards the provision of updates or upgrades can be considered an unfair commercial practice**, in particular in case of an invitation from the business to purchase ICT goods or services. Such information should be regarded as material for consumers to make an efficient transnational decision, for example, in relation to software that has proven vulnerable to specific cybersecurity risks but is still offered to consumers. According to Article 7(1) of the Directive a commercial practice shall be regarded as misleading and unfair if it does not provide the substantive information that an average consumer requires to take an informed transactional decision, thus potentially causing the consumer to conclude a contract it would not have concluded otherwise. Following Article 7(2), the same is true where the trader provides the required information in an unclear, unintelligible, ambiguous or untimely manner. Where the trader invites the consumer to purchase its ICT goods or services the duty to provide such information is even more stringent, arguably including the duty to disclose information regarding cybersecurity.

Having regard to the complexity of the ICT supply chain, in particular in the IoT, we also suggest studying in further detail in what way and to what extent accurate **information about who is responsible for ensuring cybersecurity for each of the relevant parts of this supply chain** can be provided to the consumer in a clear, meaningful and comprehensible way. From a consumer law perspective knowing who is responsible for the security of ICT goods or services is necessary for consumers to know who to hold liability in case of a security breach. From the perspective of data protection law, controllers have a duty to inform individuals about who is the processor or sub-processor of the personal data processed by such goods and services.[31]

29 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, p. 22-39.

30 Article 5(1) read in conjunction with 5(2) and 2(2) Directive 2005/29/EC.

31 Articles 28-30 General Data Protection Regulation. See more generally: Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', 264/10/EN, WP 169, Opinion of 16 February 2010.

RECOMMENDATION 1 – ICT providers should be required to offer consumers, in a clear and comprehensible way, information about their contractual obligations to ensure cybersecurity before they enter into a contract with consumers, including information about when, how, to what extent and for how long a business will provide updates or upgrades of ICT goods and services to consumers.

4.2 Conformity

Conformity in sales law traditionally concerns the question of whether supplied goods (i.e. tangible products) comply with the quantity, quality and description required by the contract.[32] Conformity is typically presumed if the goods are fit for the purposes for which goods of the same description would ordinarily be used, possess the qualities of goods which the seller has held out to the buyer as a sample or model, or are fit for any particular purpose for which the buyer requires the goods and which he had made known to the seller at the time of the conclusion of the contract.[33] General contract law and services law similarly require ICT service providers to provide services in accordance with the conditions stipulated by contract and in a way that can reasonably be expected of them.[34]

Cybersecurity (including security of personal data) is only rarely stipulated as one of the qualities of supplied ICT goods and services. Contracts related to the sale of 'smart' goods (i.e. goods embedded with ICT, software and/or network connectivity) or the provision of ICT services do not generally include obligations about the security of the networks and infrastructures used or the personal data collected through them. As the example of VTech discussed above showed, contracts are used to play down user expectations as to the security of the product and to limited or exclude any liability for damages caused by security breaches. Here, mandatory rules from the fields of telecommunications law and data protection law do not seem to be integrated (sufficiently) in the contracts underpinning the supply ICT goods and services. Given the forthcoming General Data Protection Regulation we may expect data protection by design to become a legal duty whenever goods or services are sold that involve the processing of personal data. **Integration of for example obligations of security by design into contracts could provide important additional incentives for compliance**, in particular in business-to-business relationships. Public enforcement authorities may also help to ensure such integration in contracts.

In the Digital Single Market as envisaged by the European Commission, a central role has been given to trust and security in ICT goods and services and in the handling of personal data. In line with this, **cybersecurity should be recognized as a principle quality attribute of ICT goods and services.** Such recognition should not be limited to business-to-consumer relationships, but also extend to business-to-business relationships in order to ensure that duties of care in cybersecurity translate into legal duties throughout the entire ICT supply chain.

32 In the Netherlands the rules governing the sale of tangible goods has recently also been applied (by analogy) to standard software provided upon payment through a tangible medium or downloaded from the internet and of which the use is not limited in time. Cf. Supreme Court, 27 April 2012, *NJ* 2012/293 (*Beeldbrigade*). This implies that Dutch sales law, including the rules on conformity, burden of proof and prescription, also apply to such standard software. This position is exceptional in the EU, however. Member States typically define the provision of standard software as a service or licence contract. The leading case under English law is *St Albans City and District Council v. International Computers Ltd* [1997] FSR 251, which still requires software to be transferred through a tangible medium in order to fall within the scope of sales law.

33 See for example Article 35 United Nations Convention on Contracts for the International Sale of Goods and Article 2 Directive 1999/44/EC of the European Parliament and of the Council on certain aspects of the sale of consumer goods and associated guarantees, OJ L 171, 7.7.1999, p. 12-16.

34 Importantly, articles 12-15 of the E-commerce Directive (Directive 2000/31/EC) exempt ISPs from liability with regard to data stored or transmitted by them on the condition that they did not have knowledge of or control over such data. They are not liable to the extent that their conduct is 'of a mere technical, automatic and passive nature' (cf. CJEU Joined Cases C-236/08 to C-238/08, *Google v Louis Vuitton* [2010] ECR I-02417, para. 120). This exemption is remains in place after the entry in force of the General Data Protection Regulation (see Article 2(4)). However, if ISPs are controllers or processors of personal data, the rules of this Regulation do apply, including the right to compensation of data subjects.

4.2.1 Conformity in present and future EU consumer law

The understanding of cybersecurity as a fundamental quality of ICT goods only in part resonates in the current EU legal framework on sales law. The principle legislative instrument applying here, the Consumer Sales Directive, does not mention the issue of cybersecurity in the sale of consumer goods.[35]

In December 2015 two legislative proposals were presented by the European Commission as part of its Digital Single Market Strategy to further harmonise the field of sales law: (i) a proposal for a Directive on certain aspects concerning contract for the supply of digital content (**Digital Content Directive**),[36] and (ii) a proposal for a Directive on certain aspects concerning contracts for the online and other distance sale of goods (**Online Sales Directive**).[37] Both proposals introduce fully harmonised rules that aim to ensure a high and uniform level of consumer protection across the EU. Importantly, the Digital Content Directive currently explicitly excludes the IoT from its scope of application.[38] It is suggested that **these proposals do not sufficiently take into consideration the importance of cybersecurity**, now and in the future, in the provision of ICT goods and services, and more generally, the Digital Single Market.

There are several reasons to argue for this. When exploring the contents of the Digital Content Directive, it should first be welcomed that the proposed regime on conformity of digital content involves the matter of security of related ICT services. Article 6, paragraph 2 of the proposal reads:

> (...) the digital content shall be fit for the purposes for which digital content of the same description would normally be used including its functionality, interoperability and other performance features such as accessibility, continuity and security, taking into account:
>
> (a) whether the digital content is supplied in exchange for a price or other counter-performance than money;
>
> (b) where relevant, any existing international technical standards or, in the absence of such technical standards, applicable industry codes of conduct and good practices; and
>
> (c) any public statement made by or on behalf of the supplier or other persons in earlier links of the chain of transactions unless the supplier shows that
>
> (i) he was not, and could not reasonably have been, aware of the statement in question;
>
> (ii) by the time of conclusion of the contract the statement had been corrected;
>
> (iii) the decision to acquire the digital content could not have been influenced by the statement.

35 Article 2 Directive 1999/44/EC.

36 European Commission, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contract for the supply of digital content, COM(2015) 634 final, Brussels, 9.12.2015. Article 2 defines digital content as 'data which are produced and supplied in digital form, including computer software, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or by other means. It also includes services allowing for the creation, processing and storage of data in digital form (e.g. cloud computing) and for the sharing of such data with other users of the service.

37 European Commission, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sale of goods, COM(2015) 635 final, Brussels, 9.12.2015.

38 Recital 17 Digital Content Directive.

However, this objective approach to conformity is disowned by the Directive as it allows the digital content provider under Article 6, paragraph 1 to define in the contract – and more likely in the general terms and conditions under it – what the consumer may expect in terms of the quantity, quality, duration and version of the content, as well as its functionality, interoperability, accessibility, continuity and security. Also the extent to which the consumer may expect updating of the digital content – presumably including patches and upgrades in the light of discovered software bugs and security breaches – can be defined in the contract. Accordingly, **digital content providers can subjectively determine by contractual arrangements what conformity means** and thus what expectations consumers may have in terms of the security of the digital content provided to them. As Beale notes, this phrasing is 'quite unnecessary' and 'potentially dangerous to consumers'.[39]

The Online Sales Directive, in contrast, does not allow for such a subjective approach to conformity. Much like the Consumer Sales Directive, it defines conformity of goods in Article 5 in objective terms, namely as being fit for all the purposes for which goods of the same description would ordinarily be used, including all accessories and instructions the consumer may expect to receive, and possessing the qualities and performance capabilities which are normal in goods of the same type and which the consumer may expect given the nature of the goods and taking into account any public statement made by or on behalf of the seller.

The **lack of consideration of cybersecurity as a matter of conformity of sales is problematic**, not only for sales falling within the scope of the Online Sales Directive, but also for the face-to-face sales contracts concluded between traders and consumers in physical establishments (e.g. in shops) as covered now by the Consumer Sales Directive. This is so because now already and even more so in the near future a substantial part of sales will concern goods with significant ICT components. In the case of smart goods and connected devices in the IoT the functionality of these tangible goods is substantially (if not predominantly) defined by related and linked service contracts. More specifically, the use of smart or connected devices typically involves the following contracts:

- A sales contract through which ownership of a tangible good (incl. hardware) is acquired;
- An end user license agreement (EULA) to use the software embedded in the device;
- Service contracts for software maintenance;
- Service contracts for the provision of digital infrastructure, content or services;
- Service contracts (user agreements) for the processing or exploitation of user data.[40]

This underlines that smart goods and connected devices being sold in stores, online or through other distance means will generally bring with them the provision of ICT services as an inherent part of their functionality. Due to this **hybrid character of smart products**, security of integrated and related digital content (e.g. data, software, applications) should be part of any applicable conformity assessment. From the perspective of the promotion of a Digital Single Market in which European businesses and consumers can trust on the accessibility, continuity and security of ICT services, the absence of these matters in rules determining the conformity assessment is an undesirable flaw. The proposals for the Digital Content Directive and Online Sales Directive offer an excellent opportunity to also review the Consumer Sales Directive and explicitly include cyber security in the requirements of conformity.

Furthermore, as the two proposals now stand, there is a very **static separation between the material scope of both Directives**. The purchase of smart goods and connected devices online or by other distance means falls within the ambit of the Online Sales Directive only,

39 H. Beale, 'Scope of application and general approach of the new rules for contracts in the digital environment', briefing paper for the European Parliament, PE 536.493 (February 2016), p. 21, http://www.europarl.europa.eu/committees/nl/ events-workshops.html?id=20160217CHE00181 (accessed 1 May 2016).

40 This list is likely to be extended in the context of devices used in the Internet of Things. In assessing the contractual regime underpinning the use of the Nest thermostat, Noto La Diega and Walden (note 10) content that Nest users need to at least read thirteen different documents to have a full overview of their rights and obligations vis-à-vis sellers, services providers, licensors and other third parties concerned with the operation of the thermostat and related services.

as if they were 'traditional' tangible goods. Where digital content is *embedded* in these products, it would seem to follow from Recital 13 of the proposed Directive that it applies 'where the digital content is embedded in such a way that its functions are subordinate to the main functionalities of the goods and it operates as an integral part of the goods.' Recital 11 of the Digital Content Directive reads the exact opposite and excludes digital content embedded in goods from its material scope. If consumers download new digital content onto these goods, however, the Digital Content Directive does seem to apply.

This static separation is not **tenable in practice**, in particular in the light of the hybrid character of smart goods and connected devices in the IoT. For example, if the digital content (e.g. software or applications) embedded in a smart phone sold online proves vulnerable for security breaches, but the content in this phone was in part updated under a service contract the owner signed with a third party, which Directive would apply? As Wendehorst has aptly noted, it is '**hardly possible to draw a clear line** between the supply of goods *with embedded* digital content and the supply of goods *and* of digital content'.[41]

Furthermore, it is debatable what is meant by 'the main functionalities of the goods' under Recital 11 of the Digital Content Directive and Recital 13 of the Online Sales Directive. Consider the example of smart thermostats, of which the key functionality can be said to be the control of household heating systems. However, through in-build sensors, related software and applications for remote control (e.g. through smart phones, tablets, and smart watches), and interconnections with other household devices (such as door locks, lights, electricity sockets, sprinklers, fire alarms and home security systems) their function changes into something much wider, namely a control system for energy use and home security that might autonomously control the functionality of household appliances based on user-generated data. Knowing which Directive applies in the event of a security breach in this complex, yet increasingly real-life situation is important since the current proposals provide different rules on conformity, remedies against non-conformity and termination of contracts. To overcome potential difficulties in determining the scope of application it has already been suggested to adopt a single piece of secondary EU legislation covering all types of online and digital content contracts.[42]

What appears crucial in a review of the scope of the Digital Content Directive, the Online Sales Directive, and even the existing Consumer Sales Directive, is the **need to better integrate features of accessibility, continuity and security in the conformity assessment**. This could be done by including the principles of **privacy by design and privacy by default** as laid down in Article 23 of the General Data Protection Regulation as additional criteria for establishing conformity.[43] To define conformity in this context, regard may also be had to **accepted industry standards** laying down best practices among commercial entities, including ISO 27000-series on information security management.[44]

It is also recommended that this **conformity assessment is extended to devices operating in the IoT and the digital content provided through them**. As noted, the Digital Content Directive explicitly excludes the IoT from its scope of application, but this exclusion carries with it the danger that it would leave a potentially huge market largely unregulated in such a way that the full harmonisation objective of the current proposal would be undermined. In its Digital Single Market strategy the European Commission contends that:

41 Ch. Wendehorst, 'Sales of goods and supply of digital content – Two worlds apart? Why the law on sale of goods needs to respond better to the challenges of the digital age', briefing paper for the European Parliament, PE 556.928 (February 2016), p. 8, http://www.europarl.europa.eu/committees/nl/events-workshops.html?id=20160217CHE00181 (accessed 1 May 2016). See in the same vein, V. Mak, 'The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content' briefing paper for the European Parliament, PE 536.494 (February 2016), p. 8-9, http://www.europarl.europa.eu/ committees/nl/events-workshops.html?id=20160217CHE00181 (accessed 1 May 2016).

42 Mak 2016 (note 41), p. 9-10.

43 Wendehorst (note 41), p. 14-15.

44 ISO, 'ISO/IEC 27001 – Information security management', http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (accessed 1 May 2016).

'A fragmented market does not provide sufficient scale for cloud computing, Big Data, data-driven science and the Internet of Things to reach their full potential in Europe. To benefit fully from the potential of digital and data technologies, we will need to remove a series of technical and legislative barriers. (...) Legal certainty as to the allocation of liability (other than personal data related) is important for the roll-out of the Internet of Things.'[45]

A security breach in the IoT context may enable the unwanted access to all parts of the network. The Article 29 Working Party also notes that devices operating in the IoT are also difficult to secure, both for technical and commercial reasons.[46] Therefore, the current proposals should be revised taking into close consideration the development of the IoT and the cybersecurity issues triggered by it.

RECOMMENDATION 2 – Cybersecurity should be recognized as a main characteristic of ICT goods and services. As such, it should be part of a conformity assessment related to these goods and services. To determine the conformity of these goods and the appropriate level of security for them, regard must at least be had to the purposes for which goods and services of the same description would ordinarily be used, the particular purpose for which the goods and services are required by consumers and the security risks these goods and services pose to consumers.

RECOMMENDATION 3 – Sellers of consumer goods should not be able to contract out the confidentiality, integrity and availability of related ICT for the normal life-span of these goods. Similarly, suppliers of digital content should not be able to contract out such matters of cybersecurity for the content supplied for the duration of the related services contract.

4.2.2 Burden of proof

To further strengthen the position of consumers in relation to providers of ICT goods and services, the two proposed Directives includes rules on the **burden of proof** as regards conformity with the underlying contracts. Article 9(1) of the Digital Content Directive places the burden on the supplier, requiring it to show that the content was in conformity at the time of supply. This would also imply that the supplier carries the burden to prove that a security problem (e.g. exploits, malware, attacks, ID theft or fraud) was caused by the own fault of the consumer, e.g. irresponsible password use. In any event, the consumer does not carry the burden to prove that the digital content supplied to him/her was already non-conforming at the time of supply. The Online Sales Directive also suggests a reversal of the burden of proof with respect to conformity. Article 8(3) of the proposal holds that any lack of conformity with the contract is presumed to have existed at the time of acquiring the goods or the dispatch to a carrier chosen by the consumer. This reversal is limited to a period of two year, however. The Digital Content Directive, in contrast, does not place a time limit on its reversal of the burden of proof.

The suggested reversals of the burden of proof with respect to conformity **strengthen the legal position of consumers in important ways**. Provided that cyber security becomes an inherent part of the conformity assessment related to ICT goods and services the proposals should be welcomed. This is particularly so for reasons of cybersecurity since a security vulnerability may be

45 COM(2015) 192 final, p. 14.

46 It holds that: 'As their components use wireless communications infrastructures and are characterised by limited resources in terms of energy and computing power, devices are vulnerable to physical attacks, eavesdropping or proxy attacks. Most common technologies currently in use – i.e. KPI infrastructures – are not easily ported on IoT devices since most of the devices do not have the computing power needed to cope with the required processing tasks. Article 29 Working Party, 'Opinion 8/2014 on the recent developments on the Internet of Things' 14/EN, WP 223, Opinion of 16 September 2014.

difficult for individual consumers to discover given the potentially secretive and hidden nature of such vulnerabilities, let alone attacks or breaches. In that regard, it might be considered to extend the time limit under the Online Sales Directive for goods with embedded ICT components that were not in conformity with accepted principles of cybersecurity. This may already be read into the exception Article 8(3) of the Directive provides.[47]

RECOMMENDATION 4 – It should be considered whether time limits as regards the reversal of the burden of proof for conformity could be extended where it is difficult for individual consumers to discover security vulnerabilities.

4.2.3 Relationship with data protection law, including the right to damages

It also needs consideration that the **two proposed Directives do not provide for an explicit link with data protection law**. As noted, the Directives do not consider basic principles of data protection law, including privacy by design and default as criteria for conformity of supplied digital content and goods sold online or by other distance means. More generally, data protection laws grant rights to consumers with the view to protect their personal data and privacy (e.g. rights to withdraw consent, to information and access to data, rectification and erasure of data, data portability) and impose duties of care on controllers and processors of personal data in the handling of these data. These rights and obligations may directly affect contractual relationships between consumers and businesses.[48] For example, the exercise by a consumer of his/her right to withdraw consent to the processing of personal data under Article 7(3) General Data Protection Regulation may impact on the provision of services under a service contract for the supply of digital content. Similarly, termination of a contract for the supply of digital content would seem to imply the deletion of personal data collected under that contract. These are important questions that need to be addressed, also from the perspective of cybersecurity. The Digital Content Directive and Online Sales Directives do not provide any answers, however.

The lack of coordination between consumer sales law and data protection law also emerges in relation to the **right to damages**. Article 77 of the General Data Protection Regulation provides consumers (data subjects) with a right to compensation from the controller or processor for the material and immaterial damages they have suffered as a result of an infringement of the rules laid down by the Regulation.[49] The Online Sales Directive does not provide for a right to damages. Article 14 of the Digital Content Directive gives consumers the right to compensation of 'any economic damage to the digital environment of the consumer caused by a lack of conformity with the contract or a failure to supply digital content'.

However, this article limits the right to compensation for non-conformity to economic damages to the digital environment of the consumer. Damage to the digital content itself (e.g. unavailability, disruption or the loss of data) is not compensated under this provision and neither are consequential losses other than damage to the consumer's digital environment. Accordingly, damages suffered because of bugs in the digital content that enabled hackers to access the consumer's computer, steal (personal) data, access his/her bank account, and fully clear it, are not recoverable under the proposed Directive.[50] Even if the stolen data do not represent any economic value (e.g. family pictures, personal notes), its unavailability, disruption or loss should be compensated by allowing claims for immaterial damages congruent with the sentimental and moral value of the data, or the degree of distress and anxiety caused by the security breach, as already recognized in certain Member States and the forthcoming General Data Protection Regulation. As noted, the insecurity of software might

47 Article 8(3) Online Sales Directive provides that the two limit of two year does not apply if it 'is incompatible with the nature of the lack of conformity'.

48 Mak 2016 (note 41), p. 9.

49 Under English law, it was recently recognized that the immaterial (non-pecuniary) damages suffered by individuals as a result of the collection of personal data contrary to privacy laws can be recovered under tort law. See Vidal-Hall v. Google, [2014] EWHC 13 (QB) as upheld by Google v. Vidal-Hall [2015] EWCA Civ 311.

50 Cf Mak 2016 (note 41), p. 27.

in some instances even lead to physical insecurity and physical harm (and potentially death). Damages related to physical harm and death also seem to be excluded, however.

What is more, Article 14(2) Digital Content Directive enables Member States to lay down detailed rules on the exercise of the right to damages. The discretion provided to Member States when designing a regime for compensation might effectively undermine the objective of the Directive to provide full harmonisation measures as regards the supply of digital content to consumers.[51] In the light of the full harmonisation aim, one may also wonder whether Member States are at all allowed to provide for the right to be compensated for additional damages, as this would certainly provide more protection to consumers than the level of protection offered by the Directive itself. In line with this, some authors have noted that the removal of the consumer's right to seek compensation for other damages is to be considered wrong.[52]

Accordingly, there seems to be an **apparent mismatch between the Digital Content Directive, Online Sales Directive and General Data Protection Regulation** with regard to the scope of the right to damages. Given that many types of damages fall outside the scope of the right to damages as warranted by the Directive, the recovery of these damages is governed by non-mandatory national private laws. Consequently, it is likely that businesses will seek to exclude liability for these damage types through contractual arrangements with consumers. To the extent that suppliers of digital content can be seen as controller or processors of personal data, this would be manifestly contrary to the directly binding provisions of Article 77 GDPR. Accordingly, it is suggested that the rights to damages for consumers under the Digital Content Directive is amended along the lines of Article 77 GDPR to provide the consumer a stronger legal position to recover the damages suffered as a result of insecure digital content. Enabling the compensation of the full amount of damages suffered, strengthens the motivation for consumers to seek compensation from businesses, which may in turn **incentivize individual business and the industry at large to enhance their efforts to ensure cybersecurity**.

RECOMMENDATION 5 – Consumers should have the right to be compensated for the damages they suffered due to an established non-conformity with regard to cyber-security of ICT goods and services.

RECOMMENDATION 6 – The recoverable damages caused by such a non-conformity should not be limited to material damages only and should also include immaterial damages, in line with Article 77 of the General Data Protection Regulation.

4.3 Unfair terms

Upon concluding contracts related to ICT goods and services, consumers typically agree to the general terms and conditions of business as part of a contract. Frequently, these terms and conditions include far reaching duties and restrictions for consumers. Empirical research shows that standard form contracts and related terms and conditions are hardly ever read, in particular in online environments.[53] This creates the risk that businesses use these general terms to minimize expectations regarding cybersecurity and write off any corresponding liability. Recent studies on standard contract terms used by major online service providers and mobile applications such as Dropbox, Google, Facebook, LinkedIn, Instagram, Snapchat and Twitter demonstrate that these providers use terms that would not meet the fairness test under the Unfair Contract Terms Directive.[54] These terms include:

51 Mak 2016 (note 41), p. 27.

52 Beale 2016 (note 39), p. 24.

53 In a study by researchers at New York University the Internet browsing behaviour of 48,154 monthly visitors to the websites of 90 online software companies was tracked to study the extent to which potential buyers accessed the end-user license agreement linked to the software. The study found only one or two consumers out of every 1000 accessed the agreement. Those who did access the agreement do not read more than only a small portion. See: Y. Bakos, F. Marotta-Wurgler and D. Trossen, 'Does anyone read the fine print? Consumer Attention to Standard-Form Contracts' *Journal of Legal Studies* (2014) 43(1), p. 1-35.

54 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *OJ* 1993 L 95, p. 29.

- The unilateral change of contractual obligations and the services that are provided under a contract with the user;
- The unilateral termination of the contract by the service provider;
- The exclusion or limitation of liability; and
- The choice of jurisdiction, including arbitration clauses.[55]

It must be recognized that **general terms and conditions related to consumer contracts for ICT goods and services should meet the fairness and transparency tests** laid down by the Unfair Contract Terms Directive. Unilateral changes as regards the level of cybersecurity provided under the contract should not be allowed without reasonable notice to the consumer. Liability exemption clauses should be closely scrutinize d as regards unfairness within the meaning of this Directive if they effectively bar consumers from obtaining compensation for the damages they suffered because of a lack of security.[56] Clauses phrased along the lines of 'any exclusions, disclaimers or limitation of liability provisions will apply to the extent permitted by local laws' may be considered to lack transparency (and thus be unfair), as the Competition and Markets Authority in the United Kingdom currently does.[57] Also clauses excluding the jurisdiction of the courts in which the consumer resides and imposing mandatory arbitration should be examined as regards their fairness. The Unfair Contract Terms Directive creates the presumption that arbitration clauses in consumer contracts are unfair and, therefore, invalid.[58] Case law of the Court of Justice of the European Union has consistently held that such clauses are to the detriment of consumers and should be considered unfair.[59]

Finally, it is well recognized that litigation by individual consumers against users of general terms and conditions is underdeveloped. In response to this stance and to ensure a high level of consumer protection across Europe, the Court of Justice has on the national courts of the Member States the obligation to apply the unfairness test under the Unfair Contract Terms Directive *ex officio*. This obligation involves the **duty of a national court to assess of its own motion whether a contractual term falling within the scope of the Directive is unfair**, thus compensating for the imbalance which exists between the consumer and the seller or supplier in drafting and negotiating the contract.[60] In the event that claims are brought to court, either by individual consumers or their representative organisations through collective action, these courts should investigate the fairness of the general contract terms used in the related consumer contracts.

Public enforcement authorities in the field of consumer protection and consumer representative bodies also have a role to play here. It is suggested that they **should proactively address the use of unfair terms** by businesses in consumer contracts relating to ICT goods and services. While public authorities may develop enforcement strategies to target such usage in the ICT sector, consumer representative bodies may initiate complementary collective action against businesses before a court to require the cessation or prohibition of the use of unfair terms.

55 See: M. Loos and J. Luziak, 'Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers', *Journal on Consumer Policy* (2016) 39(1), 63-90 and Forbrukerrådet (Norwegian Consumer Association), 'Appfail. Threats to Consumers in Mobile Apps' (March 2016), http://fbrno.climg.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf (accessed 1 May 2016).

56 The Annex to Directive 93/13/EEC contains an indicative and non-exhaustive list of the terms which may be regarded as unfair. Point 1(b) relates to exemption clauses as it concerns terms that have the objective of 'inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations'.

57 Competition and Markets Authority 2015 (n 19), at para. 2.54-2.55.

58 Point 1(q) of the Annex to Directive 93/13/EEC.

59 See for example CJEU Case C-168/07, *Mostaza Claro v. Centro Movil Milenium SL* [2006] ECR I-10421 and Case C-40/08, CJEU *Asturcom Telecomunicaciones SL v. Rodriguez Nogueira* [2009] ERC I-9579.

60 See most recently CJEU Case C-377/14, Radlinger v. Finway, ECLI:EU:C:2016:283 (decision of 21 April 2016), paras. 52-53.

RECOMMENDATION 7 – General terms and conditions related to consumer contracts of ICT goods and services must meet the requirements of fairness and transparency as laid down by the Unfair Contract Terms Directive. National courts, public enforcement authorities and consumer representative bodies should intervene proactively within the scope of their respective competences to better address the use of unfair terms by businesses in the ICT sector in consumer contracts.

4.4 Liability in the ICT supply chain

So far this White Paper has addressed the duties of care and diligence as regards cybersecurity arising under contractual arrangements between businesses and consumers relating the ICT goods and services. However, the ICT supply chain involves a much **wider range of actors concerned with the delivery of secure ICT**. To give an example, the seller of smart goods with embedded software is to some extent dependent on the care taken by the software developer for the security of that software. There might be good reasons why consumers suffering damages because of a lack of cybersecurity would want to hold liable these third parties for damages rather than their respective contracting parties.[61]

However, the current legal framework applying to the extra-contractual liability of third parties for damages caused by a lack of cybersecurity fails to provide sufficient incentives for the ICT sector to secure higher levels of cybersecurity.[62] More specifically, **the conditions governing the extra-contractual liability of these actors (including tort, laws of delict or unlawful act, and product liability) have proven difficult to satisfy** for consumers in order to compensate the damages caused by a security breach. Under these liability regimes the burden of proof concerning the existence of a duty of care, the breach of that duty, and the causal link between that breach and damages suffered typically lies with the claimant. Furthermore, the widespread use of liability exemption clauses may also limit the extent to which damages can be claimed. Whereas the Product Liability Directive has established a fully harmonised strict liability regime for producers as regards damages caused by defective products,[63] it is unclear to what extent this regime applies to faulty software as such, or to software embedded in products.[64]

4.4.1 Product liability

To further strengthen the duty of care as regards cybersecurity in the ICT sector, and provide better possibilities for end-users sustaining damages because of a lack of such security, it is suggested to **extend the strict liability regime for damages caused by defective products laid down by the Product Liability Directive to software**. Such extension appears to be in line with the position of the European Commission in the late 1980s.[65] Accordingly, the concept of 'product' as set out in Article 2 of this Directive should be read to include software, irrespective of whether it is provided by downloading or streaming, or on a tangible medium or by other means.[66] Updates and upgrades of software should also considered part of the definition of product. Products with embedded software would logically qualify under this definition as well if that software proves vulnerable in terms of cybersecurity.

61 These reasons involve practical reasons (e.g. if the contracting parties turn out to provide fewer possibilities to recover all damages, for example because of a lack of financial means or insolvency), but also legal concerns (e.g. the applicability of liability exemption clauses).

62 Tjong Tjin Tai e.a. 2015 (note 1), p 135-136.

63 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29), last amended by Directive 1999/34/EC of the European Parliament and of the Council (OJ L 141, 4 Jun. 1999, p 20).

64 Tjong Tjin Tai e.a. 2015 (note 1), p. 54 and 84.

65 Lord Arthur Cockfield, then vice-President of the European Commission and Commissioner for Internal Market, Taxes and Customs, noted in his written response on behalf of the Commission to question raised by Mr. Gijs de Vries (LDR-NL) whether the Product Liability Directive also covers computer software that the Directive indeed 'applies to software in the same way (...) that it applies to handicraft and artistic products'. Response to written question No. 706/88, *OJ* C 114, 8.5.1989, p. 42. The Court of Justice of the EU has not had the opportunity to rule on the matter as a case concerning insecurity digital content or products with embedded digital content has not been presented to it so far.

66 Cf. Article 2(1) Digital Content Directive.

The inclusion of software within the material scope of the Product Liability Directive offers **important advantages to consumers who want to obtain compensation for damages caused by insecure software.** The Product Liability Directive establishes a regime of strict liability for specific damages caused by a defect in a product that was placed on the market by the producer. Article 4 of the Directive requires a claimant to prove the damage, the defect and the causal relationship between defect and damage. Fault on the part of the producer does not need to be established. With the extended scope of the Directive as proposed here, the developer of software or applications that place these 'products' on the market can also be held liable as a 'producer'. Furthermore, Article 3(1) may also provide that where a business only supplies a specific part of the software (e.g. the source code of software, which is then moderated by another actor), it can nonetheless be held liable as a producer of a 'component part' of the product.[67] Article 3(2) may enable that if the software developer cannot be identified, which might be a real risk for consumers in IoT environments, the supplier of the software shall be treated as its producer, unless he informs the consumer, within a reasonable time, of the identity of the software developer or of the person who supplied him with the software. Accordingly, **the multi-layered concept of producer as presented by the Directive would closely fit with characteristics of the ICT supply chain,** in which almost all goods and services are composite 'products'.[68] The Directive notes that if two or more producers are liable under its regime, they are jointly and severally liable.[69]

Article 6 of the Product Liability Directive holds that a product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account. **Software with security vulnerabilities should be considered defective**.[70] Producers should take into account any foreseeable irresponsible use of software, for example by implementing smart solutions as regards cybersecurity based on security by design (e.g. no default passwords and the automated implementation of crucial security updates or upgrades). The defect does not need to materialise in reality: **the risk of a defect or 'potential for failure' has been considered sufficient to prove the defectiveness of the product**.[71] In the case of a security vulnerability this implies that potential attacks causing damages to the consumer are not required to establish liability on the part of the producer. The costs 'necessary to overcome the defect in the product in question' may in that case be compensated to the extent that they fall within the scope of Directive.[72]

Article 9 of the Product Liability Directive stipulates that damages caused by death or by personal injury can be compensated, as well as damage to, or destruction of any item of property other than the defective product itself and used by the injured person for private use and consumption, with a lower threshold of € 500. This concept of damages is rather restricted and consequential losses other than medical costs (e.g. pure economic losses, loss of income, and damage to the product itself) cannot be compensated. This significantly limits the potential for consumers to recover their damages from producers and, in turn, the practical importance of the Product Liability Directive.[73]

67 This implies that only those actors putting into circulation software, applications or components thereof can be held liable under the regime. Individual developers working under the supervision of these actors (e.g. employees) will not be liable vis-à-vis consumers. Also component producers will be able to escape liability where they show that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the final producer of the product (cf. Article 7(f) Product Liability Directive).

68 Noto La Diega and Walden (note 10), p. 23.

69 Article 5 Product Liability Directive.

70 This is in line with what has been argued above (paragraph 4.2.1) in relation to conformity in sales law.

71 CJEU Joined Cases C-503/13 and C-504/13, *Boston Scientific Medizintechnik GmbH* v. *AOK Sachsen-Anhalt and Betriebskrankenkasse RWE*, ECLI:EU:C:2015:148 (decision of 5 March 2015), paras. 40-42.

72 Ibid., para. 54.

73 See in general B. van Leeuwen and P. Verbruggen, 'Resuscitating EU Product Liability Law? Contemplating the Effects of Boston Scientific Medizintechnik (Joined Cases C-503 and 504/13)', 23(5) *European Review of Private Law* **2015, 899-915.**

To further enhance the legal position of consumers of software it may **be considered whether these end-users should be allowed to claim a broader set of damages from the producer based on the strict liability system as set out in the Product Liability Directive** in case of a lack of cybersecurity. Introducing a right for consumers to recover both material and immaterial damages under this Directive would be congruent with developments in the field of data protection law, in which Article 77 of the forthcoming General Data Protection Regulation will allow data subject to claim from controllers or processors such damages.

Article 9 of the Directive already enables compensation of damages caused by personal injury. Where software insecurity translates into physical insecurity and thus causes harm, which is more likely to occur where household appliances are connected in the IoT,[74] that harm may be compensated under the Directive. **Damages to items of property should be read to include also damage to hardware devices or damage or loss of digital content stored** on the consumer's devices or via cloud computing services. Damages should also include the necessary costs incurred by a consumer to prevent the risk caused by the defective product (e.g. a potential intrusion in the consumer's digital environment) from happening. These costs might include the price of related to necessary updates or upgrades to patch the security vulnerability and the costs related to restoring and retrieving any lost data.

Another additional advantage of bringing software within the scope of the Directive is that **producers are prohibited to limit or exempt their liability arising from the Directive to consumers**.[75] Currently, producers frequently exclude their liability for damages caused by the software embedded in their products.[76] Such limitations or exemptions would no longer be allowed in relation to the liability for damages sustained by consumers and covered by the Directive.

We anticipated that the inclusion of software in the material scope of the Product Liability Directive creates spin-off effects for more general regimes governing extra-contractual liability (tort and delict law) such that concepts developed under the Directive translate into and influence concepts used to establish liability under these regimes (e.g. the concept of product, the duty of care of producers, and burden of proof for *culpa*), as it has done in the past.[77]

RECOMMENDATION 8 – The material scope of the Product Liability Directive should be revised so as to include software.

RECOMMENDATION 9 – Damages to items of property for personal use should be interpreted to include also damage to hardware devices or damage to or loss of digital content. It may be considered whether and to what extent consumers of software, regardless of whether it is embedded in a product, may be enabled to claim both material and immaterial damages from the producer based on the strict liability system as set out in this Directive.

4.4.2 Development risk defence

Importantly, the producer escapes all liability arising from the Product Liability Directive if he proves that 'the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered.'[78] This so-called **development risk defence offers businesses in the ICT sector**,

74 See note 11.

75 Article 12 Product Liability Directive.

76 Noto La Diega and Walden cite a 'limited warranty' clause used by Nest Labs Europe Ltd in relation to Nest products, which states that the warranty 'does not cover consumable parts, including batteries, unless damage is due to defects in materials or workmanship of the Product, or software (even if packaged or sold with the Product)'. See Noto La Diega and Walden (note 10), p. 23.

77 See in general Van Leeuwen & Verbruggen 2015 (note 76).

78 Article 7(e) Product Liability Directive.

in which technologic knowledge is highly fluid and rapidly evolving, **a very significant instrument to fend off liability claims** related to insecure software. As the ICT industry would typically contend, there is no such thing as 'bug free' software. Accordingly, it might argue that software developers who did not discover any serious vulnerability at the time of the release of its product would be able to take advantage of the defence.

While Member States are allowed to exclude the development risk defence under the Directive, only Luxembourg and Finland have used this possibility.[79] To strengthen the position of consumers in recovering damages sustained due to a lack of cybersecurity, **the European legislature and the individual Member States should critically consider the application of this defence in relation to defective software**. While it should be acknowledged technological development in the ICT sector is fast, the release of software that disregards known and knowable vulnerabilities in terms of cybersecurity should preclude the producer from relying on the development risk defence. This should also apply to updates and upgrades of software which do not sufficiently take into account observed security threats. The defence should be interpreted restrictively.[80] Allowing for an extensive interpretation of the defence would not seem to be in line with the high level of protection offered in the domain of data protection law through the forthcoming General Data Protection Regulation, which requires controllers and processors of personal data to implement appropriate technical and organisational measures to secure personal data.

RECOMMENDATION 10 – To the extent that software falls within the material scope of the Product Liability Directive, the development risk defence allowed under the Directive should not be interpreted extensively such to exclude the liability of producers for a release of software (including updates or upgrades of it) that disregards known and knowable security vulnerabilities.

4.4.3 Product surveillance and recall

Product safety laws impose duties on producers to control, inspect and monitor the quality of the products they place on the market. In general, they need to be informed of the risks these products might pose to consumers and must be able to take appropriate action necessary to avoid these risks, including the communication of adequate and effective warnings and the organisation of product recall from distributors and consumers. Also distributors of products are obliged to act with due care to help to ensure compliance with the safety requirements, in particular by not supplying products which they know or should have presumed, on the basis of the information in their possession and as professionals, do not comply with those requirements.[81]

Where producers place on the market ICT goods and services, it should be considered whether general duties of product safety law concerning product surveillance may also apply to these goods and services. This could imply that producers of such goods and services are required to monitor these products in terms of security vulnerabilities through surveillance and testing mechanisms during normal life-span of these products. **Where vulnerabilities are discovered, they could be required to issue notifications and warnings to consumers, and in cases of high risk, a product recall.** If this concerns products with network connectivity, a notice, warning or recall could effectively and efficiently be organised through pop-up messages or screen alerts. Furthermore, they could be blocked or frozen in order to patch the vulnerabilities and restore the security of the goods and services. The risk of incurring liability for damages arising under the Product Liability Directive may provide additional incentives to issue effective warnings and organise recalls.

79 Article 15(1)(b) Product Liability Directive.

80 See also Case C-300/95, *Commission v. United Kingdom* [1997] ECR 1997, p. I-02649, paras. 26-29.

81 Article 5(1) and (2) Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4). Article 17 Directive 2001/95/EC notes that it shall be without prejudice to the Product Liability Directive.

RECOMMENDATION 11 – Businesses placing on the market ICT goods and services should be required to control, monitor and inspect these goods and services in terms of security vulnerabilities throughout the normal life-span of these products or for the duration of the related services contract.

4.5 Enforcement

It has been noted above that individuals typically lack the information, legal expertise and financial resources necessary to initiate proceedings against actors in the ICT supply chain and be successful. Courts, public enforcement authorities and consumer representatives can complement the actions of individual consumers to enforce their rights in important ways, as already observed in the case of unfair contract terms. Collective action by consumers or their representative bodies would appear more effective than individual action,[82] although its success is not guaranteed.[83] Some ICT providers have been noted to develop strategies to forestall class actions.[84]

Collective action has only in part been harmonised in the EU. The Injunctions Directive provides rules for consumer representative bodies and public enforcement authorities to bring collective actions against traders for the cessation or prohibition of infringements of consumer rights.[85] The Directive does not provide for harmonisation as regards the collective recovery of mass damages. It should be investigated whether and how the Injunctions Directive can assist consumer representative bodies and public enforcement authorities in the protection of consumer interests related to cybersecurity.

We suggest conducting a similar investigation for the recently adopted Alternative Dispute Resolution (ADR) Directive and the Online Dispute Resolution (ODR) Regulation.[86] These legislative instruments both aim to provide to consumers easy and low-cost dispute resolution in order to find out-of-court solutions to their disputes with traders arising from cross-border (online) transactions. In the absence of these solutions, such disputes currently are often left unresolved.

Public enforcement authorities in the fields of data protection law and telecommunications law have developed national and cross-border policies relating to cybersecurity. It is suggested that also national public authorities in the **field of competition, trade and consumer law need to (further) develop policies on cybersecurity, preferably in coordination with other competent national authorities.** Campaigns to raise awareness amongst consumers as regards risks of cybersecurity may already address a number of important issues and have been applied

82 Tjong Tjin Tai e.a. 2015 (note 1), p. 139-155.

83 In the US, a number of class actions involving security breaches have been filed. See for a list of these class actions: www.lawyersandsettlements.com/lawsuits-filed/internet-technology-lawsuits/ (accessed 1 May 2016). It is unclear how successful these class actions are in providing consumers with remedies. There are few final court decisions and the settlements themselves are not disclosed. Moreover, Settlements may not necessarily resolve security threats, as the settlement in the class action brought against Sony for the major security breach of its Playstation Network in 2011 shows (see: https://www.bigclassaction.com/lawsuit/sony-employee-data-breach-class-action-lawsuit.php, accessed 1 May 2016).

84 In response to a class action filed against Dropbox for its authentication bug before the US District Court, Northern District of California (*Christina Wong, et al. v. DropBox, Inc.*, Case. No. CV-11-3092), the California-based company amended its Terms of Services requiring users in the US to sign up to mandatory arbitration and a prohibiting them to initiate class actions. See: http://www.computerworld.com/article/2487987/cloud-computing/update--dropbox-changes-its-terms-of-service-to-stop-class-action-lawsuits.html and Dropbox Inc., 'Dropbox Terms of Service' (Version of November 4, 2015) https://www.dropbox.com/terms?view_en#terms (both accessed 1 May 2016).

85 Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (Codified version), *OJ* L 110, 1.5.2009, p. 30-36. The consumer rights that can be protected through the harmonised collective action concern the rights granted under the Directives on consumer rights, consumer credit, package travel, unfair commercial practices, unfair terms in consumer contracts and consumer sales.

86 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes (Directive on consumer ADR) OJ L 165, 18.6.2013, p. 63-79 and Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), OJ L 165, 18.6.2013, p. 1-12.

successfully in the past.[87] Such campaigns may be organised together with relevant business organisations and consumer representative bodies to strengthen their legitimacy base and effectiveness.[88]

RECOMMENDATION 12 – It should be investigated whether and how existing EU legislative instruments intended to improve consumer access to justice might be applied effectively to provide consumer protection in relation to disputes with traders concerning cybersecurity.

RECOMMENDATION 13 – Public enforcement authorities should complement enforcement activities taken by individual consumers and consumer representative bodies, for example by developing awareness raising campaigns as regards cybersecurity risks.

5. APPROACHES TO HARMONISATION

There is a wide array of techniques to achieve harmonisation as regards duties of care and diligence in cybersecurity, ranging from bottom-up 'spontaneous' harmonisation at the national levels to top-down legislative intervention through Regulations adopted by the EU legislature. Each of these approaches has its relative advantages and disadvantages. Generally, the harmonisation of consumer rights in the EU is orchestrated through the adoption of Directives, aiming to establish a minimum or maximum harmonised level of protection by the laws of the Member States. Regulations are not typically used as legislative instruments if consumer rights are established or harmonised. However, where harmonisation specifically concerns procedures for the enforcement of consumer rights, Regulations might be used as legislative instruments.

Having regard to the topics discussed in this White Paper, however, **it is unrealistic to expect that all these topics can be harmonised by adopting one single legislative measure with a single approach to harmonisation for cybersecurity.** In fact, several recommendations offered here do not require any legislative action at the EU or national level, but simply different action under the existing legal framework. It is therefore proposed that, to the extent possible, **the amendments suggested here should be incorporated in the existing legislative frameworks or proposals for legislation**, each having its own approach to harmonisation.

It must be noted, however, that in these legislative frameworks and proposals due regard must be had to private, **industry standards for cyber security**. These rules might be technical standards or industry codes of conduct and good practices, concerning technical aspects of cybersecurity, but also organisational (or management) requirements to ensure the confidentiality, integrity and availability of ICT goods and services. **If adopted at the international level, such as the ISO 27000-series, and widely implemented in the entire ICT supply chain through the use of contractual arrangements or procurement policies, these private standards may offer additional harmonisation effects in the ICT sector.** Such effects might further be bolstered by incorporating such standards in relevant legal frameworks concerning the assessment of the existence, scope and violation of duties of care and diligence in cyber security.

87 See for example the campaign 'Updates in, hackers out' organised by the Dutch Authority for Consumers and Markets in 2014 to raise awareness amongst Dutch consumers about the importance of up-to-date software. See https://www.consuwijzer.nl/thema/veilig-internetten-updates-binnen-hackers-buiten (accessed 1 May 2016).

88 See for example the campaign 'Alert Online' supported by government bodies and representatives from business and society in the Netherlands. The campaign sets the goal 'to encourage greater awareness of cyber security in government and the business community, as well as among consumers in general.' See on this background of this campaign: https://www.alertonline.nl/over_alert_online/About-Alert-Online/ (accessed 1 May 2016).

6. CONCLUSION

This White Paper has sought to provide a framework for discussion around the need to harmonise legal standards for duties of care and diligence concerning cybersecurity and offer proposals to better protect the interests of consumers and data subjects in terms of the confidentiality, integrity and availability of ICT goods and services. Acknowledging that the policy field of cyber security is wide, diverse and only in part regulated and harmonised, the White Paper has focused on the general EU legal framework applying to commercial transactions between ICT providers and consumers with respect to ICT goods and services. Various elements of this legal framework have been critically discussed as regards the scope of protection offered by them to consumers and, accordingly, suggestions were offered for improvement.

It needs to be stressed once more that **the exact scope of the duty of care and diligence that an ICT provider owes to a consumer as regards cybersecurity of ICT goods or services, if any, ultimately depends on the set of circumstances of a particular case.** It is not possible (or desirable) to define in detail the duties of care and diligence ICT providers owe to consumers in their commercial dealings. Such specified rules do not match with the wide diversity of cybersecurity threats (e.g. vulnerabilities, exploits, malware, attacks, ID theft and fraud), or with the constitutive elements of cybersecurity (i.e. confidentiality, integrity and availability). Moreover, specified rules would run the risk of becoming impracticable and obsolete soon after their enactment given the rapid technological developments in the ICT sector.

Therefore, we suggest to rely on accepted and tested **open norms** in the domain of European private law (including the concepts of 'conformity', 'unfairness', 'defectiveness'), and to interpret these norms to accommodate concerns of cybersecurity in relation to ICT goods and services provided by businesses to consumers. In assessing whether a duty of care and diligence has been breached in a specific case, the following circumstances should at least be taken into account:

- The purposes for which goods or services of the same description as sold by the ICT provider to the consumer would ordinarily be used;
- The purpose for which the consumer requires the goods and services, as communicated to the ICT provider;
- The legitimate expectations of the public at large;
- The presentation of or public statements about the goods and services by the ICT provider;
- Any foreseeable irresponsible (mis)use by the consumer;
- The nature and severity of the risks poses by the ICT goods or services to consumers;
- The nature and severity of the damages involved;
- The state of scientific and technical knowledge at the time the ICT provider started to offer the goods or services to consumers;
- (Non-)compliance with accepted private industry standards.

Accordingly, duties of care and diligence in cybersecurity can be differentiated in relation to the type of cybersecurity threat, the ICT provider, and the goods or services involved. Such **a principle-based approach corresponds with the regulatory approach taken under the General Data Protection Regulation and the Network and Information Security Directive**, which require controllers and processors of personal data and operators of networks and information systems to have in place appropriate technical and organisational measures to manage the risks posed to the security of these data and networks and information systems.

ANNEX: GLOSSARY OF TERMS

Application – A specific form of software designed to run on hardware and perform tasks for the benefit of the user.

Consumer – Any natural person who is acting for purposes which are outside his trade, business, craft or profession.

Controller – The natural or legal person, public authority, agency or other body which, alone or jointly with others, who determines the purposes and means of the processing of personal data.

Cybersecurity – The situation in which ICT and all of its relevant components are safe from threats to its confidentiality, integrity or availability and to the data (including personal data) handled through it.

Data subject – A natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Digital content – Data which are produced and supplied in digital form (including computer software, applications, games, music, videos or texts), irrespective of whether they are accessed through downloading or streaming, from a tangible medium or by other means. Digital content also includes services allowing for the creation, processing and storage of data in digital form and for the sharing of such data with other users of the service.

Duty of care and diligence – The legal obligation to act with due care or use professional diligence towards the legitimate interests of others.

General contract terms – A contractual term which has not been individually negotiated and has been set by a trader with the view to be used in multiple contracts.

Hardware – The collection of physical elements that constitutes an ICT system.

Hacker – A persons who seeks and exploits vulnerabilities in ICT systems or services in a malicious manner or for personal gain.

Information and Communication Technologies (ICT) – Technologies that enable users to access, store, transmit, and change information.

ICT goods and services – Goods and services based on ICT, including systems, infrastructures, networks, hardware, firmware, software, applications and digital content.

ICT providers – Business actors offering on the market ICT goods and services.

Internet of Things – The infrastructure in which devices ('things') are designed to record, process, store and transfer data (including personal data) and interact with other devices or systems using network capabilities in order to deliver services or digital content based on the collection and further combination of these data.

Internet service providers (ISPs) – For-profit or not-for-profit actors that store and transmit Internet traffic, data and online content, including hosting providers, access providers and other content and service providers (including search engines, trading platforms, social media).

Personal data – Any information relating to an identified or identifiable natural person, that is, the data subject.

Personal data breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing – Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor – A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Software – Set of information and instructions that enable the operation of hardware, including application software, system software, and malicious software (malware).

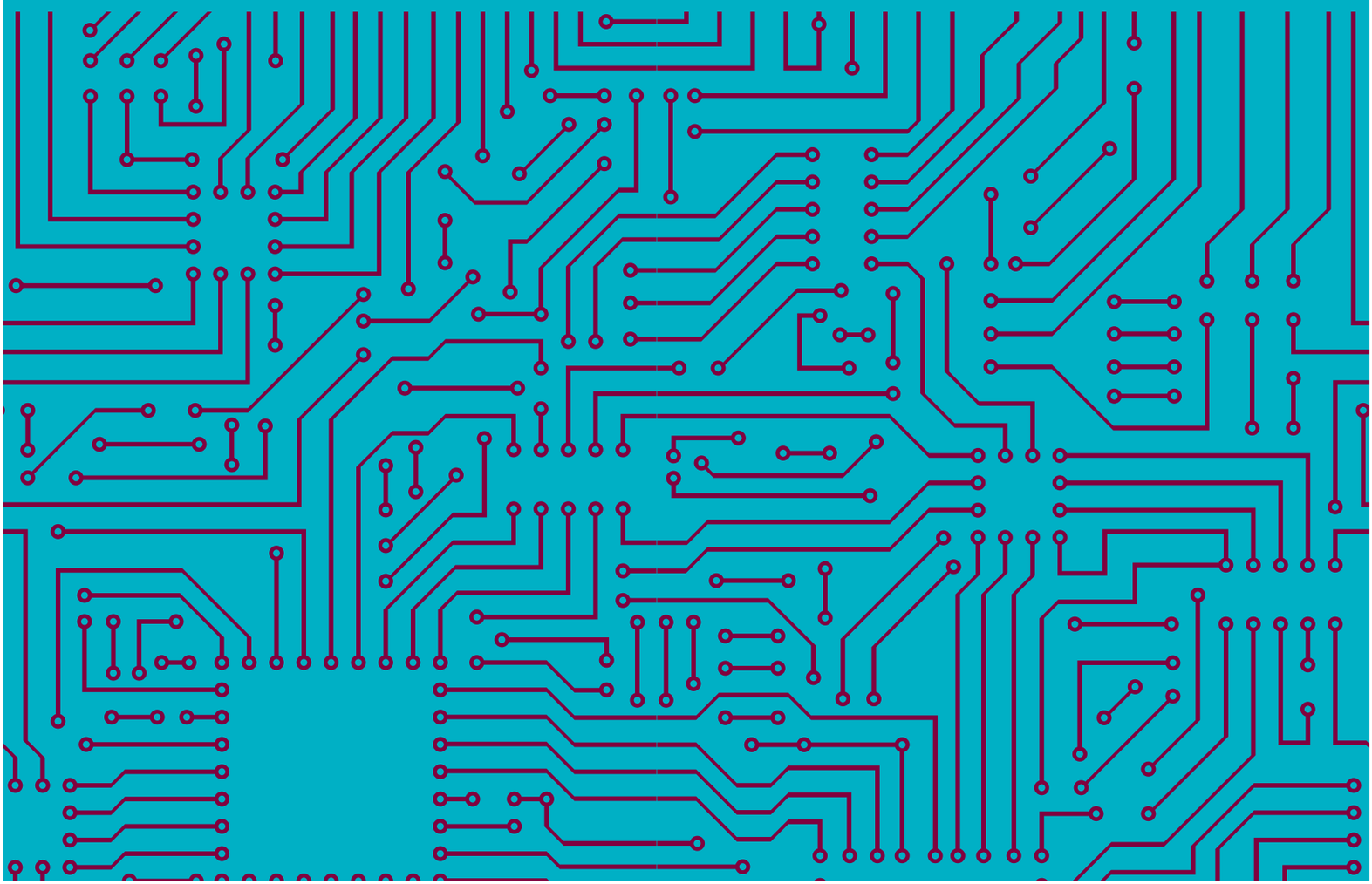
Security by design – The situation in which ICT goods and services have been designed to provide the appropriate technical and organisational measures to ensure cybersecurity, given the ordinary use of these systems and services and the foreseeable risks they pose to users.

Trader – Any natural person or any legal person who is acting for purposes relating to his trade, business, craft or profession and any other person acting in the name or on behalf of a trader.

Vulnerability – A characteristic of ICT goods or serviced that enable their unauthorized disruption, failure or misuse.

11 GLOBAL AGENDA COUNCIL ON CYBERSECURITY

Danil Kerimi
Head of Digital
Economy and Technology Policy,
ICT Industries
World Economic Forum USA



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

CONTENTS

EXECUTIVE SUMMARY

Fuelled by billions of users and endless new internet of things devices, we are in the midst of an explosion of hyperconnectivity. This means attackers can now disrupt more people through more devices, and each year there are more breaches, more affected companies and users, and more damage. It is increasingly clear that no one is immune from cyberattacks.

For this reason, it is imperative that the public and private sectors balance and prioritize the limited resources available to address cybersecurity challenges. Too often, cultural and financial pressures encourage devaluing investments in cybersecurity. Before those pressures can change, the public and private sectors must better understand the tensions that make it difficult to fully embrace cybersecurity best practices, as well as the obstacles to effective collaboration.

What the Private Sector Should Know About Public Sector Tensions:

Among the many significant challenges that can make it difficult for the public sector to effectively address cybersecurity issues, there are three particularly important hurdles:

1 *International fragmentation:* Differences in approaches to cybersecurity, data jurisdiction and legal enforcement (not to mention culture, language and politics) across jurisdictional and territorial boundaries can make it hard to effectively prevent, investigate and prosecute cyberattacks.

2 *International norm-setting:* International political differences and country-specific agendas can make it difficult to develop consensus norms regarding cybersecurity let alone enforce those norms consistently and effectively.

3 *Roles with respect to the private sector:* The varying and sometimes confrontational roles that the public sector must play, spanning regulator to information sharer and collaborator, can create tensions with the private sector that can be counterproductive to trust and cooperation.

What the Public Sector Should Know About Private Sector Tensions:

Similarly, there are many significant challenges that can make it difficult for the private sector to effectively address cybersecurity issues, including two particularly important obstacles:

1 *Misalignment of incentives for cybersecurity best practices:* Companies often fail to take basic steps to protect their systems and their users because companies are placed in the difficult position of balancing the market pressures of rapid innovation against sustained investments in cybersecurity, which may raise costs or delay delivery of products to market.

2 *Ecosystem complexities:* Today's software and hardware environments are increasingly complex ecosystems populated by a network of interacting devices, networks, people and organizations. This means cybersecurity solutions often require the voluntary engagement, cooperation and investments of many independent entities, while the incentives and mechanisms for taking such actions are distributed inconsistently across the ecosystem.

Additionally, there are obstacles that impede public-private sector collaboration on cybersecurity issues, including trust deficits between the government and private sector, the challenge of maximizing the effectiveness of government interventions while balancing security objectives with fast-paced innovation, and the weakness of existing information-sharing frameworks.

Securing the Future

These powerful tensions within the ecosystem make it clear that systemic changes are necessary to realign approaches to cybersecurity. Although there is no quick fix, there are steps that organizations can take immediately to begin to address cybersecurity challenges. These include:

1 *Adopting best practices and cyber hygiene*: An important first step is developing policies and procedures that include regularly validating approved hardware and authorized software, establishing security system configurations, timely patching of applications and operating systems, controlling and auditing user privileges and educating users.

2 *Improved authentication*: Organizations must move beyond insecure passwords to mechanisms such as two-factor authentication and continuous authentication technology, which will become increasingly important as more devices connect to our networks.

3 *Preparing for attacks*: It is critical that organizations take steps to prepare for eventual attacks, including enhancing forensic capabilities, developing business continuity plans and developing plans for regaining user trust.

The public and private sectors acting alone cannot overcome the culture and incentives that make cybersecurity so difficult today. To address these systemic challenges, the public and private sectors must come together in several ways, including:

1 *Blended governance approaches*: The public and private sectors must explore new ways of collaboration that would leverage the perspectives of governments, companies, civil society and academia.

2 *Careful government interventions*: The public and private sectors must collaboratively construct effective regulations and frameworks that address cybersecurity needs without hampering innovation or diminishing trust.

3 *Independent security organizations*: Independent organizations can reward implementation of best practices and create high-information consumers.

4 *Holistic cybersecurity education*: More holistic educational programmes can provide cybersecurity professionals with a range of necessary skills beyond the purely technical.

There is no silver bullet for cybersecurity, but that does not mean the problems are intractable. Instead, it means that careful collaboration between the public and private sectors is necessary to address these complex challenges in an ongoing and comprehensive manner.

1. INTRODUCTION

The Global Agenda Council on Cybersecurity, one of the World Economic Forum's 80 Global Agenda Councils, was formed to explore and develop practical solutions to the challenging questions on changing cybersecurity trends and emerging new challenges. Cybersecurity can no longer be left to IT departments and security groups within companies. It is an issue that requires engagement at the highest levels of both industry and government.

The council's members include cybersecurity experts, policy-makers, business executives, civil society representatives and academics. Over the course of several meetings, these experts have identified and debated some of the central issues, challenges and opportunities relating to cybersecurity. This report synthesizes several of the ideas expressed at these meetings.

Cybersecurity has already become a critical issue across business, industry, government and civil society; it will only grow more urgent as the online world becomes a central and underlying component of the physical world. As of the end of 2015, 3.2 billion people are connected to the internet in some form, including 2 billion from developing countries. And this is growing at a rapid pace. From 2000 to 2015, the global internet penetration rate grew from 6.5% to 43%.[1] Those people, and the many more who join each year, rely on the internet for their jobs, commerce, culture and communications. And they are connected by more than just PCs and mobile devices; increasingly, everyday products and core infrastructure – including refrigerators, thermostats, the electrical grid and aircraft engines – rely on embedded computers and network connections. As society and industry become more dependent on these internet-connected devices, the significance of cybersecurity increases as well.

The public and private sectors each face difficult and unique challenges in balancing their varied roles and responsibilities, and prioritizing their limited financial, time and human resources. Too often, members of the public sector fail to appreciate the complexity of the challenges that the private sector faces and vice versa. These misunderstandings can inhibit effective collaboration and partnerships. This report tries to break through those barriers to build a foundation in which collaboration can thrive.

There are no easy solutions, but the good news is that there are things the private sector can do right now to address these cybersecurity challenges. By following and implementing cyber hygiene and best practices, companies can make an immediate and positive difference. However, without cooperation between the public and private sectors, such measures will be inadequate. The private sector on its own cannot create a culture that emphasizes security practices, realign financial incentives that reward speed over security, or mend trust deficits with the public sector. But together with the public sector, these challenges can be addressed. Through the use of new multistakeholder processes, as part of blended governance frameworks, public-private partnerships can begin to change the culture and incentives of security best practices, create frameworks for collaboratively constructing effective cybersecurity regulations and tools without hampering innovation or diminishing trust, and support the creation of independent security organizations that enable well-informed consumers.

The World Economic Forum possesses a unique ability to focus the attention of decision-makers at the highest levels of both the public and private sectors, and to harness their energies in devising creative and effective solutions. In that way, the Forum is the ideal institution to address cybersecurity issues. The Global Agenda Council on Cybersecurity, as well as the Forum's Future of the Internet Initiative's Cyber Crime project, present unique opportunities for exploring innovative solutions to a complex and ever-evolving problem. As described below, advancing cybersecurity will require multistakeholder collaboration and international cooperation. The World Economic Forum's Global Agenda Council on Cybersecurity is proud to be a contributor to that effort.

1 ICT Data and Statistics Division, International Telecommunications Union, "ICT Facts and Figures: The World in 2015." 2015. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

2. EMERGING TRENDS

Many public and private sector decision-makers intuitively appreciate that cybersecurity is an important consideration. But less clear are the tectonic shifts pushing the issue to the fore. Although there are many factors that contribute to cybersecurity's increasing saliency, three are worth identifying here: (1) the shift toward cloud services and more devices' built-in Internet connectivity; (2) the increased prevalence, severity, and fallout from data breaches, and (3) the inability of security to keep pace with technological development.

A. Increased Reliance on Internet-Connected Devices and Services

Key takeaway: The internet of things and cloud computing are creating new opportunities for vulnerabilities and crime while simultaneously expanding the potential devastation of such attacks.

Decreasing costs of hardware, software and internet connections, combined with greater bandwidth capacity, are enabling companies to put internet connections into previously unconnected devices,[2] while making users more reliant on data centres and cloud computing.[3] Taken together, these two trends have enabled rapid changes in the capabilities of software, products and services. But they have also opened new opportunities for crime and espionage, and simultaneously expanded the potential devastation of such attacks.

Cheaper and faster technology is making cloud computing increasingly technically and economically viable. The cost of digital storage has plunged from $300,000 per gigabyte of data in 1981 to $0.03 per gigabyte in 2014.[4] Files that would have taken days to download over a 28.8 kbps dial-up connection can be transferred in minutes or seconds over today's broadband connections. These changes have enabled an array of new services that move many aspects of computing, including data storage and analysis, to remote systems that provide access and computational power to users on an as-needed and aggregated basis. Companies are no longer required to build their own network infrastructure; companies can instead use infinitely scalable cloud computing to rent remote storage and processing capabilities and easily scale up their resources as they grow. In fact, major internet companies such as Dropbox, Netflix and Pinterest do just that – they have built entire platforms on server infrastructure rented from other companies. Consumers benefit from cloud computing as well, using online services to store, access, synchronize and share files, photos and other digital assets.

As cloud computing has become more common, the centralization of services and the explosion of internet of things (IoT) devices has created a hyperconnectivity that creates new challenges for cybersecurity:

1 *Centralization of services*: Cloud computing has unburdened smaller companies from the need to invest in infrastructure, which has decentralized and democratized opportunities for smaller companies to deploy innovative services. But this has also led to centralization at the infrastructure level on to a handful of platforms. Only a few companies have the resources to build and deploy the massive data centres necessary for modern internet services. For that reason, a large portion of internet data and traffic is managed by a concentrated pool of companies including Amazon, Microsoft, Google, Rackspace and IBM. This centralization presents both challenges and opportunities; these large data centres are often better equipped to maintain their services to defend against attacks than the average small company but they also present more tempting targets for attackers.

2 Koomey, Jonathan. "The Computing Trend That Will Change Everything." *MIT Technology Review*, 9 April 2012. http://www.technologyreview.com/news/427444/the-computing-trend-that-will-change-everything/; Goldman Sachs, "The Internet of Things: Making Sense of the Next Mega-trend." Global Investment Research, 3 September 2014. http://www.goldmansachs.com/our-thinking/ages/Internet-of-things/iot-report.pdf.

3 Armbrust, Michael et al., "Above the Clouds: A Berkeley View of Cloud Computing," *University of California, Berkeley*, 10 February 2009. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf; Naone, Erica. "Conjuring Clouds." MIT Technology Review, 23 June 2009. http://www.technologyreview.com/article/413981/conjuring-clouds/.

4 Komorowski, Matt. "A History of Storage Cost (Update)." *Mkomo*, 9 March 2014. Web. 25 November 2015. http://www.mkomo.com/cost-per-gigabyte-update.

2 *Expansion of connected devices:* The transfer of services and data to the cloud has also enabled the rapid adoption of interconnected devices, including both mobile devices and IoT. Increasingly, individuals are relying on mobile devices for internet connectivity. Mobile broadband (i.e., 3G and 4G connections) penetration has reached 47% worldwide and is estimated to grow to 70% by 2020,[5] enabling new online services such as mobile banking in sub-Saharan Africa.[6] Additionally, the cloud has enabled an array of internet-connected physical objects (IoT) ranging from critical infrastructure to personal devices. These objects have the ability to generate data through a variety of sensors and then process and store that data in the cloud. Some estimate that by 2020, there will be 25 billion connected "things" in use,[7] most with durability, latency, enrolment, vulnerability, authentication and privacy challenges.

3 Taken together, this hyperconnectivity of services and products has greatly increased the ability of attackers to reach more users through more devices. Every new connected device introduces another potential entry point to the network, increasing the overall attack surface. Cloud computing and IoT are forecast to create unprecedented opportunities for improving lives and enabling innovation. Unfortunately, they also invite a new set of cybersecurity challenges.

4 Cloud computing service providers' incentives may not always align with greater investments in cybersecurity, or they may simply lack the necessary expertise. Many companies that have marketed conventional industrial machines or non-computerized appliances or services are now grappling with complex security issues. For example, car manufacturers, consumer appliance manufacturers, livery services and industrial equipment manufacturers are facing many of the same challenges that have traditionally been considered "computer" problems. The universe of devices connected to the internet is vast, and developers and manufacturers bring different corporate cultures, experiences and expertise when designing the security of their products. And for some, that experience and expertise is limited.

B. Breaches and Vulnerabilities Are Increasing in Frequency and Severity

Key takeaway: Attacks are inevitable. Over the past year, major entities from nearly every sector have suffered significant attacks and the commoditization of exploits and vulnerabilities will only enable more attacks.

The number and severity of breaches continue to rise. According to one report, there were 1,540 breach incidents in 2014, affecting over 1 billion records – a dramatic increase from 1,056 incidents affecting 575 million records in 2013.[8] Cybersecurity is a challenge for entities both large and small, sophisticated and not. A recent study conducted for the UK government found that 90% of large businesses and 74% of small businesses had suffered a data breach over the past year, both increases over the previous year.[9]

Over the past couple of years, breaches have affected some of the most important industries worldwide – including finance, healthcare, entertainment – and governments. In mid-2014, a small team of criminals infiltrated JP Morgan Chase's computer system to steal the personal information of 83 million individuals and small businesses as part of a securities fraud scheme.[10] In early 2015, attackers used a variety of exploits to steal 80 million social security records and other personal data from the US health insurance company Anthem.

5 ICT Data and Statistics Division, "ICT Facts and Figures"; GSM Association, "The Mobile Economy Series 2015." 2015. http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf.

6 Id.

7 Gartner. Gartner Symposium/ITxpo. "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015." N.p., 11 November 2014. http://www.gartner.com/newsroom/id/2905717.

8 Gemalto. "2014 Year of Mega Breaches & Identity Theft." February 2015. http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf.

9 United Kingdom, Her Majesty's Government. "Information Security Breaches Survey 2015," 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432413/bis-15-303_information_security_breaches_survey_2015-executive-eummary.pdf.

10 Hackett, Robert. "Arrests Made in Connection with JPMorgan Hack, Report Says." *Technology*. Fortune, 21 July 2015. Web. 25 November 2015. http://fortune.com/2015/07/21/arrests-jpmorgan-chase-hack/.

And in October 2015, police arrested two teenagers for stealing bank and personal information of up to 4 million customers from the UK telecoms company TalkTalk.[11]

Government systems have also been the target of attacks. For example, in January 2014 it was revealed that an employee of the Korea Credit Bureau had stolen the personal credit card data of 20 million South Koreans and sold the information to marketing firms.[12] In June 2015, the United States Office of Personnel Management discovered a year-long intrusion into its systems. The attack compromised the records of over 21 million current and former US government employees, including social security numbers, sensitive background-check records and even fingerprints.[13] While the attacks were originally believed to have originated from nation-state sponsored adversaries, the Chinese government recently arrested several criminal hackers who allegedly conducted the attack.[14]

Sony Pictures suffered a crippling attack in late 2014, suspected to be the work of hackers tied to a nation-state government. The hackers, allegedly motivated by the pending release of the Sony film, *The Interview*, stole and then released large files including unreleased movies and scripts, internal financial reports, employee health information, and a trove of publicly embarrassing internal emails. The attack crippled Sony's systems, including: "The telephone directory vanished. Voicemail was offline. Computers became bricks. Internet access on the lot was shuttered. The cafeteria became cash-only. Contracts – and the templates those contracts were based on – disappeared."[15]

These examples make apparent that there is no single cybersecurity threat or adversary. Instead, threats take many forms. Attackers can be nation-states or affiliated hacking groups; they can be criminals, or a disgruntled employee. Attackers can be motivated by political or commercial gain. They can take advantage of human mistakes, technical vulnerabilities, or a combination of these. They can use any of the high-profile vulnerabilities that have been found in popular user software such as Flash, critical security protocol toolkits like OpenSSL (e.g., Heartbleed), and mobile device operating systems like Android (e.g., Stagefright).

It is difficult to measure the costs of such attacks. Many estimates exist, and while the exact amounts may not be accurate or useful, they underscore the potential severity. For example, IBM and the Ponemon Institute estimate that the average consolidated cost of a data breach is $3.79 million.[16] By contrast, the 2014 Verizon Breach Investigation Report suggests a range of costs, depending on the number of stolen records; while a breach of 100 records is estimated to cost a company anywhere from $1,000 to over $500,000, a breach of 100 million records could cost between $400,000 to just under $200 million.[17] Highly regulated industries, such as healthcare, education and finance, may have even higher data breach costs.

Not only is no one immune from these high-cost attacks, but it is becoming easier to obtain the tools necessary to perpetrate them. Lucrative grey and black marketplaces for selling hacking tools, software vulnerabilities and exploits – particularly coveted zero-day exploits – facilitate and enable attacks. The increasing availability of the tools required for a successful cyberattack

11 "Second teenager arrested over TalkTalk data breach." *The Guardian*, 30 October 2015. http://www.theguardian.com/business/2015/oct/30/second-teenager-arrested-over-talktalk-data-breach.

12 "Credit Card Details on 20 Million South Koreans Stolen - BBC News." *BBC News*. N.p., 20 January 2014. http://www.bbc.com/news/technology-25808189.

13 US Office of Personnel Management. "Cybersecurity Incidents." Cybersecurity Resource Center. June 2015. https://www.opm.gov/cybersecurity/cybersecurity-incidents.

14 The identities, and whether the hackers were connected to the Chinese government, is still unclear. Nakashima, Ellen. "Chinese government has arrested hackers it says breached OPM database." *Washington Post.* 2 December 2015. https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

15 Hess, Amanda. "Inside the Sony Hack." Slate, 22 November 2015 http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.

16 Ponemon Institute LLC. "2015 Cost of Data Breach Study: Global Analysis." May 2015. http://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF.

17 Verizon. "2015 Data Breach Investigations Report." April 2015. http://www.verizonenterprise.com/DBIR/.

has increased both the number and sophistication of attacks,[18] and developments like machine learning, which will lead to attacks that rapidly evolve, will only increase sophistication of attacks in the future. Cyber criminals have evolved from discrete, ad hoc networks of individuals to a highly organized system of financially driven criminal enterprises around the globe. And this commoditization of cyber offensive tools will continue to enable the growth of cyberattacks.

C. Business and Technology Developments Outpace Security Improvements

Key takeaway: The speed and pace at which new products and services are being developed outpaces the ability and/or willingness of companies to address cybersecurity risks.

The growing threat of attacks is compounded by the fact that the speed and pace of development for new products and services outpace companies' abilities to respond to cybersecurity threats. For many companies, security considerations are secondary as they balance the market pressure for rapid innovation against investments in cybersecurity. Emphasizing cybersecurity may not lead to immediate or measurable impacts on earnings or might delay bringing products to market. For that reason, it is easy for executives and board members to view investments in cybersecurity as a waste of money or, worse, a waste of critical time. Even seemingly small tasks such as rolling out and installing updates and patches can take a long time. In some cases, patches may break core product functionality or prove too expensive and might be forgone entirely. The 2015 Verizon Breach Investigation Report, for example, noted that "99.9% of the exploited vulnerabilities had been compromised more than a year after" the vulnerability had first been publicly disclosed and a patch made available. More often than not, critical product updates remain unapplied well after vulnerabilities have been discovered.[19]

The pace of technical development also makes it hard for institutions and individuals to make informed purchasing decisions. The technical complexity of cybersecurity is only one piece of that information gap. Some of the same factors that enable the fast pace of innovation also create barriers to informed purchasing with respect to cybersecurity, including:

- *Lower barriers to market entry:* Developing new online tools and services might have previously required companies to invest heavily in capital expenditures, including servers and other network infrastructure. Now companies can rent infinitely scalable architecture, lowering the initial investment costs and making it easier for anyone to enter the market, no matter what their competence.

- *Ease of becoming a developer:* Big software companies like Microsoft and Google have extensive hiring, training and quality-assurance programmes, which can help ensure (although by no means guarantee) that end products reflect expertise in cybersecurity. Now, however, app stores like those found on the Android and iOS ecosystems have lowered the bar for becoming a developer and distributor. These developers may have neither the knowledge and experience to address cybersecurity issues nor the resources to respond to issues when they arise.

- *Fewer signalling devices and less accountability:* With new market entrants emerging daily, it is harder for consumers to rely on brand name as a proxy for quality. Where a brand name company might face market pressures to address cybersecurity lapses in its products, there is no guarantee that a new start-up will even exist in six months, let alone respond to issues. This can make it harder for consumers to identify quality apps and hold developers accountable when issues arise.[20]

Collectively, these changes in the marketplace can increase the cybersecurity risks faced by consumers and users of products and services by making it harder for them to properly assess the associated risk of new tools and services.

18 Ablon, Lillian et al. "Markets for Cybercrime Tools and Stolen Data." *RAND Corporation*. 2014. https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

19 Id.

20 McGoogan, Cara. "Instagram Scam App Stole Passwords from Users." *Wired UK*. 11 November 2015. http://www.wired.co.uk/news/archive/2015-11/11/malware-infected-instagent-pulled-from-app-store.

3. CURRENT TENSIONS AND CONSIDERATIONS

These emerging trends create a complicated and quickly evolving cybersecurity landscape. Both governments and companies struggle with unique challenges as they try to *balance and prioritize resources and responsibilities*. Too often, for the public and private sectors, security is an afterthought. Simple steps, like cyber hygiene and adopting best practices, remain undone because of cultural and financial pressures that allocate financial, time and human resources to other priorities. While the public and private sectors could begin to address these challenges together, often they fail to appreciate the difficult tensions they each face. Before the public and private sectors can effectively collaborate on cybersecurity, they must better understand the tensions and considerations that shape their respective approaches to cybersecurity.

A. What the Private Sector Should Know About Public Sector Tensions

Key takeaway: The public sector must simultaneously play a multitude of roles with respect to cybersecurity, which can create conflicts, confusion and distrust. Governments face significant challenges as they attempt to balance those roles while navigating complex relationships with national, regional and global stakeholders.

It is important for the private sector to keep in mind that any single government or agency can be playing one or many roles in the cybersecurity ecosystem. And in playing each of these roles, the government may have different, or even competing, interests and objectives. These roles can include:

- *Governments as defenders* – governments strive to protect their citizens from harm, which may include promoting cybersecurity best practices, aggregating intelligence, or even engaging in offensive operations that weaken the cybersecurity of other countries.
- *Governments as users* – governments rely on effective cybersecurity to defend their own systems.
- G*overnments as regulators* – acting through their legislative, judicial, regulatory branches, governments regulate to implement policy through the rule of law.
- *Governments as stakeholders* – acting through a variety of bilateral and multilateral negotiations and agreements, governments establish international law or norms to govern cybersecurity.
- *Governments as coordinators* – governments coordinating public and private initiatives, through standard-setting processes, and by facilitating the sharing of information between private and public stakeholders.
- *Governments as promoters* – governments actively promoting cybersecurity and the local companies that enable it through endorsement, funding and incubation programmes.
- *Governments as researchers* – governments conducting or funding research on technical or societal issues related to cybersecurity.
- *Governments as service providers* – governments providing cybersecurity (or information relating to it) for use by other government agencies or the public.
- *Governments as educators* – governments educating both citizens and the private sector about the importance of and approaches to cybersecurity.[21]

21 See Gasser, Urs and David R. O'Brien. "Governments and Cloud Computing: Roles, Approaches, and Policy Considerations." *Berkman Center for Internet & Society*, 17 March 2014. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410270.

In playing these various roles, each important in their own way, governments are continually switching from one role to the next, as they rebalance, reprioritize and reshape their objectives. This can create shifting, challenging and even confusing relationships with stakeholders and the private sector. For example, in the course of responding to and investigating cybersecurity incidents, governments must balance cross-border cooperation while resolving conflicting national laws and jurisdictional claims, and protecting their own national interests. At the international level, governments must balance multilateral cooperation with unilateral action as they encounter a messy and evolving set of global norms. And in the course of pursuing national security, governments struggle to find the right balance of cooperation and coordination with the private sector, as well as the right balance between government's offensive and defensive roles.

1. International Fragmentation

Key takeaway: Fragmentation, both legal and technical, has complicated government efforts at responding to, investigating and prosecuting cybersecurity incidents. Outdated and inadequate bilateral and multilateral mechanisms have necessitated striking a difficult balance between cooperation and confrontation at the international level.

Government efforts at addressing cybersecurity are often complicated by the legal and technical fragmentation of the internet. The internet is not an international network, but a transnational one. For that reason, responding to and investigating cybersecurity incidents requires, among other things, coordination across territorial and jurisdictional boundaries. However, legal fragmentation has been a significant obstacle to international cooperation. This legal fragmentation emerges from differences across jurisdictional and territorial boundaries in approaches to cybersecurity, along with differences in culture, language and politics.

In cybersecurity investigations, governments must carefully balance claims of "data sovereignty", which refers to the tricky questions relating to assertions of jurisdiction over data as it is stored within, and transits across, national boundaries. Any country physically involved in the processing, storage or transmission (origination, destination, or intermediary) of data could be said to have a jurisdictional claim over data. Governments must carefully navigate these complex, and often competing, set of assertions in order to obtain data necessary to an investigation.

When governments try to resolve these jurisdictional questions, it can lead to tensions with other nations and with private sector companies. For example, in December 2013, as part of a federal narcotics investigation, the United States government was trying to obtain access to a particular customer's emails that were stored at a Microsoft data centre in Dublin, Ireland. One option for the US government would have been to exercise the Mutual Legal Assistance Treaty (MLAT) process, a system of bilateral and multilateral agreements by which nation states commit to assisting one another in criminal investigations and prosecutions. In complex international investigations into cybersecurity incidents, such cross-national cooperation is often necessary and is an increasingly important part of investigations. According to estimates from the US Department of Justice, over the past decade the number of MLAT requests to the US increased by 60%, with computer records requests increasing tenfold.[22]

However, as a mechanism for addressing cybersecurity, the MLAT process has, in practice, proven difficult and frustrating for law enforcement. Many of the MLAT agreements were drafted before the globalization of data and, as a result, investigators are often waiting months for responses to MLAT requests. Cybersecurity incidents require quick responses because digital evidence can quickly disappear, which makes it difficult for governments to rely on MLATs in these circumstances. For those reasons, in the Dublin case the US government instead served a warrant on Microsoft, claiming that the US had jurisdiction

22 US Department of Justice, "Mutual Legal Assistance Treaty Process Reform." *FY 2015 Budget Request*. 2015 http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

over the data because Microsoft is a US company. Microsoft opposed the warrant, asserting that the US government's jurisdiction did not reach data stored exclusively in another country. This is just one example of the difficult choices governments must make in balancing cooperation and confrontation in cybersecurity investigations.

Additionally, governments face a feedback loop that encourages greater levels of fragmentation. Governments often invoke the challenges of addressing cybersecurity issues as a reason for *increasing fragmentation*, which, in turn, only makes it harder to address cybersecurity. Several countries, including China,[23] Russia[24] and Brazil,[25] have proposed or enacted data localization laws to stop one kind of cybersecurity threat (nation-state surveillance) even though it may complicate addressing other cybersecurity threats.

Similarly, in response to concerns about US surveillance, the European Court of Justice struck down the "Safe Harbor" data-transfer provision of the 1995 Data Protection Directive in October 2015. The Safe Harbor rule had permitted companies outside the EU to store and process the data of Europeans, as long as they self-certified their ability to adequately protect that data. In response to the court's decision, the EU and US announced a new framework for transatlantic data flow. This new agreement – the EU-US Privacy Shield – includes a requirement that American companies wishing to import data from Europe meet new obligations on how personal data is processed and individual rights are guaranteed. In addition, the EU-US Privacy Shield includes limitations, safeguards and oversight mechanisms protecting the rights of EU citizens during US government law enforcement and national security investigations. The EU-US Privacy Shield also provides for mechanisms for EU citizens to seek redress for violations of the agreement and for annual reviews of the agreement.[26] Although the EU-US Privacy Shield must still be adopted, the entire affair highlights the risk of greater fragmentation through conflicts over data sovereignty.

2. National Security and International Norms

Key takeaway: The development of norms can lag substantially behind technological developments. And even when norms are established, they can be applied inconsistently.

It is important for the private sector to keep in mind that governments operate in an international arena where they are continually constrained by norms of behavior. These norms can be an effective way to counteract fragmentation through shared understandings and agreements for addressing cybersecurity challenges. Through mechanisms, ranging from legal treaties to non-binding statements, informal customs and principles, governments have increasingly sought to establish international norms and agreements on investigations into cybercrimes and acceptable practices relating to cyber activities. However, the development of norms also poses challenges for governments as they must often act to address new cybersecurity threats well before norms are established and must carefully choose when to adhere to norms and when those norms interfere with their national laws and interests.

There have been several recent, and largely successful, attempts at addressing aspects of cybersecurity through norms. However, these efforts also highlight many of the challenges for governments. For example, in 2001, the Council of Europe adopted the Budapest Convention on Cybercrime. The convention aimed to facilitate detection, investigation and prosecution domestically and internationally by increasing international cooperation.

23 Wong, Gillian. "China to Get Tough on Cybersecurity." *Wall Street Journal*, 9 July 2015. http://www.wsj.com/articles/china-to-get-tough-on-cybersecurity-1436419416.

24 Gulyaeva, Natalia and Maria Sedykh. "Russia Enacts Data Localization Requirement; New Rules Restricting Online Content Come into Effect." *Chronicle of Data Protection*, 18 July 2014. http://www.hldataprotection.com/2014/07/articles/international-eu-privacy/russia-enacts-new-online-data-laws

25 Toor, Amar. "Will the Global NSA Backlash Break the Internet?" *The Verge*, 8 November 2013. Web. 25 November 2015. http://www.theverge.com/2013/11/8/5080554/nsa-backlash-brazil-germany-raises-fears-of-Internet-balkanization.

26 European Commission, "Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-US Privacy Shield" 29 February 2016. http://europa.eu/rapid/press-release_IP-16-433_en.htm?locale=en; European Commission, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield" 2 February 2016. http://europa.eu/rapid/press-release_IP-16-216_en.htm.

The Budapest Convention currently has 54 signatories, with 47 of those having ratified the convention. While considered a success in many respects, it also demonstrates some of the challenges of norm-setting, including:

- *Delays*: Nearly half of the ratifying countries took a decade or longer to complete ratification.
- *Lack of Uniformity:* The Budapest Convention, while not limited to European countries, remains a primarily European agreement, with many significant stakeholders around the world actively in opposition.
- *Narrow scope:* The convention, by design, only touches on a small aspect of cybersecurity; attempts to expand the convention to other topics have so far had only limited success.
- *Conflicts of laws:* Several countries have struggled with fully implementing the convention due to constitutional or statutory conflicts, particularly those relating to different conceptions of privacy and free speech.
- *Slow to update:* Nearly 15 years old, the convention has been criticized for not keeping pace with technological change and evolving needs.[27]

A more recent effort at international cooperation and norm setting is the United Nation's 2014-2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of National Security (UNGGE), composed of representatives from 20 nations. The UNGGE released a report in July 2015, which built on previous efforts from 2010 and 2013. The report detailed existing and potential threats to information security, the possible cooperative measures to address them, including norms, rules or principles of responsible behaviour for states, and suggested various confidence-building measures to strengthen telecommunication and global information system security. That experts from 20 nations developed a consensus report on cybersecurity represents a positive turn towards establishing norms with respect to cyberspace. And although questions remain about the ultimate enforceability of the agreement, it remains a positive sign for the development of cybersecurity norms.

3. Cooperation with the Private Sector

Key takeaway: The public sector faces a difficult challenge of balancing the need to access information for investigations with the security of communications, privacy rights and commercial interests.

Governments play many roles and sometimes these roles can conflict, creating confusion and challenges for the private sector. Nowhere is that tension more apparent than the current global debates about the proper limits of governmental authority in accessing digital communications. Within the past year, conflicts over the use of encryption in communication devices and services have taken centre stage, often throwing into tension governments' roles as defenders, promoters, users and regulators. This debate has focused on both encryption of the devices that prevent anyone other than the owner from reading data stored on the device, and end-to-end encryption of communications. End-to-end encryption refers to the exchange of data over a communication channel that is completely encrypted from the sender to the intended receiver, meaning that anyone intercepting or passing the data, including service providers, law enforcement and intelligence agencies, cannot access the contents of the communication.

Over the past two years, several companies announced the availability of device and end-to-end encryption in their products. In 2014, Apple announced that iOS 8's iMessage would

27 Vatis, Michael A. "The Council of Europe Convention on Cybercrime," *National Academy of Sciences*, 2010. https://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf.

encrypt communications end-to-end and that iPhones would be encrypted by default.[28] Shortly after, Google followed suit by announcing that Android Lollipop would encrypt user data in certain messaging applications by default.[29] In November 2014, popular instant messaging service WhatsApp, currently owned by Facebook, announced it would support an end-to-end encryption protocol called TextSecure.[30] In March 2015, Yahoo introduced an extension that encrypted messages in Yahoo Mail.[31]

This trend towards greater encryption in consumer-grade software and devices has created a difficult challenge for governments, which must balance national security and law enforcement demands for additional information and the need for security in devices to prevent crime and fraud. Around the world, states have taken different regulatory approaches to this challenge. In the United Kingdom, for example, proposed legislation could potentially ban the use of the end-to-end communications in applications including WhatsApp, iMessage and Snapchat.[32] Similarly, the use of encryption in consumer messaging applications continues to be hotly debated in places like the US and France, particularly after the coordinated attacks in Paris in November 2015 and increased attention to the threat from groups such as ISIS.[33]

B. What the Public Sector Should Know About Private Sector Tensions

It is important for the public sector to understand that the private sector often fails to adequately address cybersecurity not because of a lack of solutions. In many cases, implementing those solutions may come at the cost of added expenses, reduced shareholder gains, delayed product releases, or impaired user experiences. There is no shortage of accepted best practices that companies could implement that would reduce the risk of attacks and the harms that would come from those attacks. For example, there are best practices relating to general corporate security, including the Center for Internet Security's (CIS) set of Critical Security Controls for effective cyber defence.[34] And there are best practices relating to network security management, including the ISO 27001, the International Organization of Standardization's (ISO) exhaustive set of security standards

28 Sanger, David. "Signaling Post-Snowden Era, New iPhone Locks Out NSA," *The New York Times*, 26 September 2014. http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html.

29 Timberg, Craig. "Newest Androids will join iPhones in offering default encryption, blocking police," *The Washington Post*, 18 September 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

30 Greenberg, Andy. "Whatsapp Just Switched on End-to-End Encryption for Hundreds of Millions of Users," *Wired*, 18 November 2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

31 Stamos, Alex. "User-Focused Security: End-to-End Encryption Extension for Yahoo Mail," *Yahoo Blog*, 15 March 2015, http://yahoo.tumblr.com/post/113708033335/user-focused-security-end-to-end-encryption.

32 Curtis, Sophie. "Will WhatsApps really be banned in the UK?" *The Telegraph*, 13 July 2015. http://www.telegraph.co.uk/technology/social-media/11736230/Will-WhatsApp-really-be-banned-in-the-UK.html; Lomas, Natasha. "UK Gov't Must Clarify Its Position On End-To-End Encryption, Says Parliamentary Committee." TechCrunch, 1 February 2016. http://techcrunch.com/2016/02/01/uk-govt-must-clarify-its-position-on-end-to-end-encryption-says-parliamentary-committee/.

33 Perlroth, Nicole. "Security Experts Oppose Government Access to Encrypted Communication." *The New York Time*s, 7 July 2015. http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html; Sanger, David E., and Nicole Perlroth. "Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks." The New York Times. 16 November 2015. Web. 25 November 2015. http://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html?_r=0.

34 "Welcome to CIS Controls." *Center for Internet Security*. https://www.cisecurity.org/critical-controls.cfm. Several governments and enterprises have identified Critical Security Controls as an important tool for effective cyber defence. See National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." Cybersecurity Framework. February 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf; United Kingdom. "Critical Security Controls guidance" Centre for Protection of National Infrastructure http://www.cpni.gov.uk/advice/cyber/Critical-controls; European Union. "Cyber; Critical Security Controls for Effective Cyber Defence." European Telecommunications Standards Institute. May 2015. http://www.etsi.org/deliver/etsi_tr/103300_103399/103305/01.01.01_60/tr_103305v010101p.pdf; Symantec, "Internet Security Threat Report 2015." International Telecommunications Union, 2015. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf; Verizon "2015 Data Breach Investigations Report." 2015. http://www.verizonenterprise.com/DBIR/2015/; Atlantic Council and Zurich Insurance Group. "Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures." Atlantic Council. 2015. http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf. The California State Attorney General recently announced that enterprises not using the Critical Security Controls would be deemed as failing to provide reasonably security, and subject to appropriate legal action. California Dept. of Justice, "California Data Breach Report." Office of Attorney General. February 2016. https://oag.ca.gov/breachreport2016.

for an Information Security Management System (ISMS).[35] And there are best practices relating to cloud security more generally, such as recommendations from the Cloud Security Alliance,[36] and best practices for cloud security on specific platforms, such as the best practices for Amazon's Web Services.[37] Government agencies have also made available sets of best practices, including the Australian Signals Directorate's list of 35 cybersecurity steps[38] and the UK's "10 steps to cybersecurity", covering issues such as user privileges, system configuration, malware prevention and user education.[39]

Additionally, there are known best practices with respect to authentication. Understanding whether a user has the proper credentials and authority to access a service, system, device or network can be critical to ensuring cybersecurity. There is increasing recognition that passwords alone are an insufficient form of authentication. Here, too, there are acknowledged approaches to improving authentication, including biometrics, or two-factor identification, which combines something you know (e.g., a password) with a physical object (e.g., an item unique to the user such as a mobile phone, ID-card etc.).

There is no shortage of best practices and implementing them would have measureable results. The Australian Signals Directorate estimates that 85% of the attacks it observes could be mitigated by simply following four basic steps, including patching applications and patching operating systems.[40] And yet, although many of these best practices are known to mitigate a significant number of cybersecurity risks, many enterprises in the private sector, both large and small, fail to take these steps. In some cases, the limitation is a lack of awareness about available best practices. In many other cases, the obstacle for companies is in balancing the financial, time and human resources that such changes would require against the competitive market pressures that demand quick profits and rapid innovation.

1. Resources and Knowledge Gaps

Key takeaway: Companies face challenging questions about prioritizing the application of financial, time and human resources, necessitating difficult trade-offs between investments in new products and features, securing their own systems, securing end-user systems and data, and securing legacy products, all within a market that rewards rapid innovation and being first to market.

As seen above, there are many best practices and standards that companies could follow for addressing cybersecurity issues within their systems and products. However, on the whole, even with the increase in high-profile breaches, there are still many companies that simply take inadequate steps to secure either their own systems or their users' data, or both. One reason for this gap between concept and implementation is that companies have limited financial, time and human resources and they face many pressures to prioritize issues other than cybersecurity.

Companies often have to balance the market pressures of rapid innovation and shareholder returns with ensuring security. Investments in security can prevent significant losses but may not generate positive returns on investment in the short term when compared to the potential returns from investments in innovation and future product development.[41] Additionally, the market stresses rapid product development and often rewards those first

35 "Information Security Management." ISO 27001. International Organization For Standardization, n.d. Web. 25 Nov. 2015. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

36 "Cloud Security Alliance." *Cloud Security Alliance*. N.p., n.d. Web. 25 November 2015. https://cloudsecurityalliance.org/.

37 Todorov, Dob, and Yinal Ozkan. "AWS Security Best Practices." Amazon Web Services, November 2013. http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf.

38 Id.

39 United Kingdom. Government Communication Headquarters. "10 Critical 10 Steps to Cyber Security." 16 January 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf.

40 Australia. Australian Signals Directorate. "Strategies to Mitigate Targeted Cyber Intrusions." February 2014. http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf.

41 Schneier, Bruce. "Security ROI." Web log post. *Schneier on Security*. 2 September 2008. https://www.schneier.com/blog/archives/2008/09/security_roi_1.html.

to market. In such an environment, it is easy for cybersecurity to become a secondary priority to be addressed only after the product is developed.

Even in the wake of incidents, companies can place a low emphasis on security. For example, in 2011, Sony's PlayStation Network was hacked, exposing the personal information of 77 million accounts.[42] Despite having already suffered a significant breach, when Sony Pictures – another Sony subsidiary – was hacked in 2014, only 11 of Sony's 7000 employees were assigned to the company's information security team.[43] In a 2007 interview with CIO Magazine, Jason Spaltro – then executive director of information security at Sony – stated that the low value placed on security was a "valid business decision to accept the risk" of a security breach, and that investing $10 million to avoid $1 million of penalties was not something he would do.[44]

Even companies seeking to invest in their human resources often face a systemic resource gap: a lack of trained cybersecurity specialists. A 2015 report from Cisco estimated that there were 1 million unfilled cybersecurity jobs.[45] In actuality, the knowledge gap is even greater because the Cisco figure counts only the demand for full-time technical cybersecurity specialists, and does not consider the impact of cybersecurity on numerous non-technical positions. The employees in these non-technical positions, despite a lack of cybersecurity training, are often asked to address cybersecurity challenges. These challenges can include addressing the businesses risks of cybersecurity threats, determining the interaction between physical security and cybersecurity, planning for public responses after a data breach, managing cybersecurity specialists, or engaging with government agencies following a serious cyberattack. Considering that any computer-using employee is a potential cybersecurity risk or a part of the response, a lack of basic cybersecurity training contributes to the expanding knowledge gap.

In general, companies have limited time and resources. They frequently must make a difficult set of balancing decisions prioritizing where those limited resources can be best utilized. Even when putting resources into cybersecurity, companies must balance between dedicating resources to the security of their own systems and dedicating resources to securing end-user products. While large companies may have more resources, they also may face additional challenges and costs of coordinating across various silos within the company. By contrast, smaller companies may not have the financial or human resources capacity for addressing the multitude of complex cybersecurity challenges.

Companies must also make difficult choices in prioritizing the vulnerabilities they choose to patch. For example, companies must decide how much of their limited security budgets should be spent on buying vulnerabilities from security researchers. The vulnerabilities marketplace has become increasingly lucrative, which makes it increasingly expensive for companies to keep vulnerabilities out of the hands of criminals. Some companies have created bug-bounty programmes as a means of participating in that marketplace, but many companies' bounties are not competitive with what governments or criminals might pay for a vulnerability or an exploit. Even when companies know of the vulnerabilities, whether purchased or not, there are more than can possibly be fixed. Companies must allocate their limited resources and choose which bugs and vulnerabilities to address, while risking leaving gaps for attackers to exploit.

Additionally, not every industry has a culture and an upgrade cycle that is compatible with the fast pace of development in the technology and software industries. In some industries, seemingly small changes like a software upgrade might trigger unacceptably large costs.

42 Hill, Kashmir. "How Do We Deal with Data Breaches?" *Forbes*. 9 May 2011. http://www.forbes.com/sites/kashmirhill/2011/05/09/how-do-we-deal-with-data-breaches/.

43 Hill, Kashmir. "Sony Pictures Hack Was a Long Time Coming, Say Former Employees." *Fusion*. N.p., 4 December 2014. http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/.

44 Id.

45 Cisco, "Mitigating the Cybersecurity Skills Shortage." 2015 http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf.

For example, certain utility operators in the US typically depend on their industrial control system software to last for 10 to 15 years, and many of those companies are still using Windows XP on their critical infrastructure. This poses a significant cybersecurity issue as Microsoft ended support for Windows XP in 2014. The industry, however, is locked into this outdated software because the tight integration between the management systems and the software means it would cost more than $100 million and would take several years for them to upgrade to newer systems.[46]

The example of Windows XP in utilities is emblematic of a larger challenge: software and hardware vendors often cannot force their customers to upgrade and secure their systems. Once products are in the hands of customers, product updates can be impossible to fully implement. For example, in May 2015, a vulnerability was found to likely affect millions of routers due to a specific component, NetUSB, that many manufacturers had used in their routers. This vulnerability would allow an attacker to wipe or compromise a router, and potentially install malware to spy on the users, or even compromise the entire network. Patches for the issue were deployed inconsistently. In some cases, the owner of the router might not understand the problem or know how to apply the patch. In other cases, just like with the utilities, the patch or update could cause unacceptable disruptions for the end-users. Even well-intentioned companies can sometimes find that the resources required to provide cybersecurity updates would far outstrip their ability to deliver them.

Finally, resource allocation can be a challenge when it involves allocating resources across companies and industries. In these circumstances, companies and sectors may not be able to agree on who should bear the costs of addressing certain risks. For example, in the US, many retail companies who use point-of-sale terminals have not moved to more secure chip systems for credit card transactions and continue to rely on antiquated and vulnerable magnetic strip technology. This is in large part because the retail companies are not eager to shoulder the cost of upgraded point-of-sale terminals even if it leaves customers insecure.[47]

2. Ecosystem Management Challenges

Key takeaway: Companies face difficult challenges in effectively addressing cybersecurity issues where solutions must be implemented by several independent actors who own and manage different parts of an interoperable system, and where a single product is the result of several components made by different companies or even different silos within the same company.

Software and hardware environments are increasingly complicated ecosystems populated by a complex community of interacting devices, networks, people and organizations. Because no single company can maintain and control every aspect of the ecosystem, trust and cooperation are essential. Companies face challenges in managing these ecosystems both where the ecosystem is the product of many different actors and companies deploying interoperable systems, and in situations where a single product is made up of components from different companies or even different silos within the same company.

Interoperable system complexity:
Highly interoperable systems can create rich ecosystems of services and devices, but they can also create cybersecurity challenges. Without a single point of control over the ecosystem, cybersecurity challenges can be addressed only through a combination of trust and voluntary cooperation between each participant. As the complexity of the ecosystem increases, so, too, do the costs of coordination and the risk of mismatched incentives. These challenges have been apparent in Google's Android mobile operating system, where the lack of central control has led to several cybersecurity breakdowns. Google provides Android as open-source software, and it has gained significant market share, installed on an estimated

46 King, Rachael. "Windows XP in Utilities Could Mean Big Security Problems." *CIO Journal*. *The Wall Street Journal*, 9 March 2014. http://blogs.wsj.com/cio/2014/03/09/windows-xp-in-utilities-could-mean-big-security-problems/.

47 Ziobro, Paul, and Robin Sidel. Target Tried Antitheft Cards." *The Wall Street Journal*. 20 January 2014. http://www.wsj.com/news/articles/SB10001424052702304027204579332990728181278.

80% of smartphones.[48] Although Google maintains the core code, the ecosystem as a whole involves the participation of hundreds of handset manufacturers and carriers which can customize the operating system before loading it on their devices or deploying it on their networks.

Google cannot push security updates directly to end users. Instead, it can take months for users to receive updates to Android, if at all. That delay is because handset manufacturers must first test the update to ensure it is compatible with their devices. Then the wireless carriers must also test each new update. And both the handset manufacturers and the carriers might have modified the Android code or created their own apps, and each new update from Google might require extensive revisions to that custom code, further compounding the delays. For these reasons, wireless service providers and device manufacturers often delay or forgo significant operating system updates to avoid the cost in financial, time and human resources that these updates require. As a result, many older Android smartphones never receive security and feature updates from Google. As of December 2015, only 29.5% of Android devices run the year-old Lollipop version and only 0.5% are running the newest Marshmallow version.[49] By contrast, Apple has much more control over the software that runs on its devices, a model that allows the company to release updates directly to users. Consequently, 70% of iOS devices are using Apple's latest operating system.[50]

This challenge of updating Android devices became a significant security liability when researchers discovered Stagefright in July 2015, which was a major exploit that allowed an attacker to take over a victim's device through a simple SMS message or audio file.[51] When discovered, Google moved quickly to issue a patch to the software. However, the Android device ecosystem took months to propagate out the fix and some older devices were never patched. In response to this security failure, several companies within the Android ecosystem have pledged to change their processes to provide monthly patches.[52]

A similar ecosystem challenge was the Heartbleed vulnerability, which was disclosed in April 2014 and was believed to affect 17% (about half a million) of the internet's secure web servers.[53] The bug compromised any secure connection that utilized OpenSSL, allowing attackers to eavesdrop on communications, steal data directly from services and users, and impersonate services and users. Although a patch for OpenSSL was made available quickly, there was no central point of control that could force updates; individual server owners were responsible for applying the patch to their systems. Some owners patched their servers quickly and others took months.

Single product complexity:
Ecosystem issues can also affect the cybersecurity of a single product. Today's complex devices often rely on the integration of technology from many suppliers. These relationships rely on trust – most companies lack the time, money and resources to check the source code or the design specifications of every component sourced from others. Companies must trust that their vendors and suppliers live up to their security assurances.

The 2015 hack of a Chrysler Jeep Cherokee showed how difficult it can be to secure products made from components from a variety of suppliers and vendors. The Jeep entertainment system utilized Uconnect, a third-party application that connected to the internet. Using Uconnect's IP address, hackers were able to gain access to the Jeep from a remote laptop miles away and seize control of the car's dashboard, steering, braking and transmission

48 IDC Research "Worldwide Quarterly Mobile Phone Tracker." 2015. https://www.idc.com/prodserv/smartphone-os-market-share.jsp.

49 "Dashboards" *Android*. 2015. https://developer.android.com/about/dashboards/index.html.

50 Apple "App Store." (accessed 13 December 2015). https://developer.apple.com/support/app-store/.

51 Z Team. "Experts Found a Unicorn in the Heart of Android." Zimperium Mobile Security, 27 July 2015. https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/.

52 Dreyfuss, Emily. "Big Android Makers Will Now Push Monthly Security Update." Wired. 6 August 2015. http://www.wired.com/2015/08/google-samsung-lg-roll-regular-android-security-updates/

53 Schneier, Bruce. "Heartbleed." *Schneier on Security,* 9 April 2014. https://www.schneier.com/blog/archives/2014/04/heartbleed.html.

functions.[54] In this case, manufacturing a complex product like a car requires trusting that all of the components, when placed together, will not create cascading vulnerabilities. Although companies can conduct supplier and vendor audits or use other controls to try to catch vulnerabilities, that may delay and significantly increase the costs and complexities of developing new products.

Tighter collaboration between or within companies may help to address these ecosystem challenges, but more often than not, company cultures prevent open communication about systems and designs. Within companies, for both competitive and institutional reasons, stovepiping is common within divisions. Although this data siloing can protect product secrecy and trade secrets, it can also prevent collaboration and information sharing. Similar concerns may prevent companies that collaborate on products with suppliers and vendors from sharing critical information. In all cases, these communication gaps may contribute to cybersecurity issues in complex ecosystems.

C. Broader Ecosystem Tensions and Considerations

Key takeaway: Effective collaboration between the public and private sectors requires that they recognize and address the obstacles and limitations to collaboration, including their lack of trust, and difficulties in lawmaking and enforcement, and obstacles to research and information sharing.

It is not enough for the public and private sectors to understand the challenges they face. It is also important for them to recognize and address the challenges and limitations of any efforts at collaboration. Collaboration may not be easy, but it is essential for addressing many cybersecurity issues because the internet is a transnational system spanning jurisdictional boundaries and public and private systems.

Many cybersecurity challenges affect both the public and private sectors and benefit from the expertise and perspectives across governments, companies, academic institutions, industry experts and the general public. Collaboration is critical for five reasons:

1 *Technical gaps*: The private sector controls many of the critical systems and resources that comprise the internet.

2 *Talent gaps:* The private sector captures a stronger current of technical talent and expertise.

3 *Information gaps:* The public sector has greater access to national and international threat information.

4 *Enforcement gaps:* The public sector is better positioned to investigate and prosecute cybercrime and enable cooperation between companies that otherwise might be impeded by concerns over competition and reputation.

5 *Development gaps:* Partnerships can build bridges between mature and developing industries and countries, facilitating knowledge and information sharing.

The public and private sectors are intentionally distinct and their differences are important. However, those same differences can also make partnerships difficult. One of the main challenges to partnerships has been the trust deficit that has grown between public and private entities, particularly after recent revelations about surveillance.

The lack of trust is not the only obstacle to collaboration in the cybersecurity ecosystem. The public and private sectors can attempt to collaborate through information sharing, the creation of standards, incident response, security research and more. However, each of these collaborative approaches requires balancing the multifaceted roles that both public and

54 Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway – With Me In It." *Wired*, 21 July 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

private sector entities play. For example, governments play dual roles as both regulator and collaborator with the private sector. Similarly, companies within an industry play dual roles of both competitors and partners in addressing cybersecurity issues. These multifaceted roles and relationships create tensions and obstacles for effective collaboration.

1. Trust Deficits Between Companies and Governments

Key takeaway: As a result of a backlash to government surveillance, companies are hesitant to collaborate with governments due to fear of negative perceptions, loss of business and liability risks from divulging private information, colluding with competitors, or exposing themselves to additional penalties.

One of the most significant obstacles to building and maintaining effective partnerships between the public and private sectors is the fundamental lack of trust that emerged after the Snowden leaks in 2013. In response to revelations about government surveillance, several major technology companies, including Apple, Facebook, Google, Twitter and Microsoft, expressed concerns over publicly collaborating with government actors. These companies and others have worked together to publicly protest government surveillance and lobby for surveillance reform.

Companies have been particularly hesitant to collaborate with the US government because of the potentially negative financial impacts. Distrust of US government policies and statements regarding surveillance have led several non-US companies and foreign governments to be suspicious of any company that might be aiding intelligence collection. Some analysts have estimated that the Snowden leaks in particular will cost major US technology companies billions of dollars in lost sales.[55] These factors push companies to distance themselves from the negative perceptions of a tight collaboration with government, creating a cold climate in public-private relations.[56]

The debates about the use of end-to-end encryption highlight this lack of trust between the public and private sectors. Because technology companies have been leery of voluntarily cooperating with law enforcement agencies, several government leaders from around the world, including Prime Minister David Cameron of the UK and leaders in China, have sought the legal authority to compel access to online communications for lawful investigations.[57] The public and private sectors have struggled to agree on what is feasible. For example, NSA Director Admiral Michael Rogers proposed that technology companies implement certain technical changes to encryption that would enable government access, such as so-called "golden keys".[58] In response, members of the security technologists and the private sector have claimed such solutions would introduce new vulnerabilities, threaten economic competitiveness and weaken existing security measures.[59]

An additional trust issue is that companies fear sharing information with governments and other companies may expose them to liability, either for divulging private information, inadvertently revealing information that subjects them to regulation or sanction by other government entities, or for antitrust violations for colluding with competitors.

55 Castro, Daniel. "How Much Will PRISM Cost the U.S. Cloud Computing Industry." The Information Technology and Innovation Foundation. August 2013. http://www2.itif.org/2013-cloud-computing-costs.pdf.

56 Germano, Judith, "Cybersecurity Partnership: A New Era of Public-Private Collaboration." The Center on Law and Security. October 2014. http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf.

57 Nicole Perlroth, "Security Experts Oppose."

58 Ellen Nakashima and Barton Gellman. "As encryption spreads, US grapples with clash between privacy and security." *The Washington Post* 10 April 2015. https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.

59 Harold Abelson et al. "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications." Computer Science and Artificial Intelligence Laboratory Technical Report https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

Overcoming these trust deficits is necessary for collaboratively addressing cybersecurity challenges. However, there are other significant obstacles to collaboration between the public and private sectors. The tools that the public and private sectors can use for collaboration each come with their own challenges. As will become apparent, trust (or a lack thereof) is an element of many of those challenges as well.

2. Standards, Regulation and Enforcement

Key takeaway: The public and private sectors, when collaborating in standard-setting, lawmaking and legal enforcement, must find the right balance between government interventions and innovation, and between deliberative legal processes and the need for quick resolutions.

The public and private sectors can and do collaborate on cybersecurity issues through standard-setting, lawmaking (encompassing both legislation and regulation) and legal enforcement. However, when collaborating in any of these ways, it can be difficult for the public and private sectors to find the right balance between government interventions and innovation, and between deliberative legal processes and the need for quick resolutions. This difficulty is apparent in some of the ways in which they collaborate:

- *Standard-setting:* The creation and adoption of standards can help identify best practices, create shared norms, and enable interoperability across complex systems – all crucial to cybersecurity. Collaboration in standard setting can enable the development of norms that reflect diverse perspectives and offer unique solutions to difficult cybersecurity challenges. However, standard-setting has many challenges of its own:

- *Speed:* Standard-setting institutions are slow-moving and often fail to keep pace with technical innovation, a particular problem when trying to address quickly developing cybersecurity threats. By the time a standard is finalized, it may be out of date and fail to fully address emerging issues.

- *Compatibility:* Products that were designed and deployed before or even during the standard-setting process may be incompatible with subsequent standards and impossible or difficult to update.

- *Universality:* Standards benefit from network effects. However, there are a variety of coalitions and institutions that are developing alternative or competing standards for addressing cybersecurity issues. This leaves many standards without a critical mass of adoption and creates a fragmentation that undermines effectiveness.

- *Lawmaking*: The creation of legislation and regulation is another opportunity for public and private sector collaboration. In some cases, lawmaking can be more effective than standards because it offers a mechanism for compelling compliance and uniformity with cybersecurity practices when the market might otherwise be fractured and uncoordinated. For example, several pieces of cybersecurity legislation have been proposed including the recently enacted US Cybersecurity Information Sharing Act (CISA) of 2015, which could stimulate collaboration that would not otherwise occur. Collaboration in the legislative and regulatory processes helps address the public sector's lack of technical and industry knowledge. But lawmaking, like standard-setting, can be ill-equipped at addressing the fast-moving cybersecurity environment. Lawmaking processes can be slow and difficult, and the current political environment in the US has made it difficult to enact legislation.

- *Enforcement:* Legal enforcement of cybersecurity issues is another avenue for public and private sector collaboration. Investigations of cyberattacks, for example, often require such collaboration. However, as described previously, such collaboration requires a difficult balance between public and private interests.

In all of these examples of standard-setting, lawmaking and enforcement, it can be very difficult for the public and private sectors to balance the different roles they must play at different times. For example, sometimes governments act as a defender of cybersecurity

and sometimes governments seek to exploit cybersecurity vulnerabilities. Choosing the correct times and places to play those roles can be difficult, and a trust deficit can exacerbate the problem. For instance, documents from the Snowden revelations indicated that when participating in a public-private process for establishing a new standard for random-number key generations, the NSA championed one in particular – the Dual_EC_DRBG generator. Documents from Snowden indicate that the NSA had used the standard-setting process to urge adoption of a standard that it could break, damaging trust and complicating its role in future collaborations.[60] By contrast, there are times when the public sector in its enforcement role can help companies respond to and recover from attacks in ways that would have been impossible without government assistance. In these circumstances, collaboration can help build trust and confidence in their partnerships.

Enforcement in Action: Cybercrime

At the World Economic Forum, there are efforts under way to improve collaboration between the public and private sectors in improving the investigation and prosecution of cybercrimes. The Future of the Internet Initiative's Cybercrime Project, an effort complimentary to this Global Agenda Council, recognizes that meaningful and effective approaches to combating cybercrime require close collaboration between the public and private sectors. In an effort to foster that collaboration, the Cybercrime Project has identified several recommendations for effective public-private partnerships:[61]

1 Public and private sectors should share more information related to cyber threats, vulnerability and consequences.
2 Public and private sectors should work to create new platforms, strengthen existing platforms and coordinate these platforms to increase information-sharing and improve investigations and prosecutions.
3 Public and private sectors should cooperate to encourage and advance wider adoption of the Budapest Convention on Cybercrime, or, of the principles it promotes.
4 Public and private sectors should work to build trust and discuss contentious topics related to cybercrime, such as encryption, cloud servers, data access and protection of privacy, to find appropriate solutions.
5 Public and private sectors can engage in other initiatives aimed at reducing cybercrime.

3. Knowledge and Information Sharing

Key takeaway: Knowledge and information sharing is a critical tool in addressing cybersecurity challenges and, by definition, it requires participation from both the public and private sector. However, trust deficits, secrecy obligations, ineffective frameworks for sharing and liability risks all constrain and limit sharing.

Information and knowledge are key currencies in cybersecurity, as they are critical to both prevention and response, including:

- *Balancing resources:* The public and private sectors have different perspectives, skill sets and time horizons, and information sharing is critical to addressing the complete array of cybersecurity challenges. The government is in a unique position to think about long-term threats and the types of actors who are capable of carrying them out, as well as to aggregate information from a variety of sources. By contrast, the private sector is in a unique position to implement and respond to many security threats.

- *Building expertise*: Not only do the public and private sectors have different perspectives and expertise, but they have different levels of maturity and experience. Fostering a knowledge exchange from governments and companies with experience addressing

60 Perlroth, Nicole, "Government Announces Steps to Restore Confidence on Encryption Standards." *The New York Times*. 10 September 2013. http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/.

61 World Economic Forum "Recommendations for Public-Private Partnership Against Cybercrime." Cybercrime Project – Future of the Internet Initiative. January 2016. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf.

cybersecurity issues to those without those experiences is important for sharing best practices and preventing cybersecurity breaches. In fact, cybersecurity knowledge sharing has been identified as a central component of sustainable development more broadly.[62]

- *Attribution*: After an attack, identifying who caused an incident and how is critical for patching vulnerabilities and deterring future incidents. In attributing incidents, sometimes, private and public entities receive an overwhelming amount of complex, difficult-to-decipher information. Other times they receive too little information. In either case, both sectors receive only one perspective, necessitating information sharing for proper attribution. On several occasions, companies and governments have made mistakes in attributing attacks, often due to bad or insufficient information sharing.

Information and knowledge sharing is an important form of collaboration, but it faces many challenges. The most significant is the trust deficit described above, which creates resistance to collaboration of any kind, and concern about the accuracy of any information that is shared. In addition to the trust deficit, several other challenges exist, including:

- *Secrecy obligations:* Governments must balance their obligations with respect to secrecy in national security, intelligence and grand jury information with the need for bi-directional information sharing. Government secrecy obligations can restrict the extent and depth to which governments can share information with the private sector. For companies, these secrecy issues raise the concern that information sharing flows in one direction – from companies to governments, with limited reciprocity.

- *Institutional reforms:* Certain organizations exist to help facilitate open information sharing, such as the National Cyber Security and Communications Integration Center (NCCIC)[63] in the US and the Cyber Security Information Sharing Partnership (CISP) [64] in the UK. However, many of these institutional initiatives are created within silos, without input from other stakeholders, or as "quick fixes" to fill gaps temporarily. They often place an emphasis on some aspects of reorganization, such as agency-to-agency coordination, over other issues like improving existing communication with the private sector. For that reason, there is significant scepticism over whether these reforms will be successful, whether they address the correct issues, and whether they serve the best interests of the private sector and the public at large.

- *Liability risks:* Companies fear they may be held liable either by directly revealing information that violates a statute, or indirectly by revealing information that leads to liability for unrelated offences. For example, a well-intentioned disclosure to one government entity might subject those records to public records requests, which may in turn lead to further investigations by a different government agency or civil lawsuits. To address this issue, in the US, for example, the Cyber Security Information Sharing Act (CISA) contains a strong liability safe harbour that immunizes companies from private rights of action and regulatory enforcement actions that arise from certain types of information sharing. While the law has been criticized for a lack of user privacy protections and limitations on the downstream use of the disclosures, public and private stakeholder groups will have voluntary tools and standards for sharing information and protecting privacy.[65]

Knowledge and information sharing is a key tool in addressing cybersecurity challenges, and by definition it requires participation by both the public and private sectors. The

62 United Nations "Transforming our world: the 2030 Agenda for Sustainable Development" Sustainable Development Knowledge Platform. 21 October 2015. https://sustainabledevelopment.un.org/post2015/transformingourworld.

63 US Department of Homeland Security "Information Sharing." http://www.dhs.gov/topic/cybersecurity-information-sharing.

64 CERT-UK. "Cybersecurity Information Sharing Partnership (CiSP)." https://www.cert.gov.uk/cisp/.

65 Andy Greenberg and Yael Grauer. "CISA Security Bill Passes Senate with Privacy Flaws Unfixed." *Wired* 27 October 2015. http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/.

development of effective laws, regulations and standards, as well as prevention and attribution, all require careful calibration of public and private interests and perspectives. However, in the absence of knowledge and information sharing, that calibration and balancing of interests may be impossible. Unfortunately, there are significant challenges that impede effective knowledge and information challenge.

4. SECURING THE FUTURE

With so many difficult tensions making it hard to address cybersecurity, it is clear that systemic changes are necessary to realign the culture and incentives that shape cybersecurity. This a complex and evolving space and no single solution can adequately address the full spectrum of challenges. However, there are a variety of approaches that can help. What follows is not an exhaustive list but a starting place for how the public and private sectors can begin to change the culture on cybersecurity.

There are steps that companies can and should begin to take right now to improve cybersecurity. We identify below several of these steps. But while they are crucial, they are not sufficient. The private sector cannot address cybersecurity on its own. Changing the underlying market pressures and culture, improving trust with the public sector, and improving public-private information and knowledge sharing, can only be done through collaboration between the public and private sectors. For that reason, the remainder of this report looks at some things the public and private sectors can do to help address these larger structural challenges. These approaches include: (1) the use of blended governance models; (2) the targeted application of limited regulation; (3) the use of independent security organizations to enable informed purchasing; and (4) expanding security professionals' skill sets to encompass critical non-technical skills. While each of these approaches can potentially address some of the cybersecurity challenges, no single recommendation here can change culture and perceptions. Only time, education and communication can realign cultural approaches to cybersecurity.

A. Immediate Steps the Private Sector Can Take to Emphasize Cybersecurity

Key takeaway: It is critical for enterprises across the private sector to implement best practices throughout all operations, and throughout product lifecycles, as a foundational step to greater cybersecurity – a difficult challenge in a market that rewards rapid product development.

The private sector must directly confront the cultural and incentive challenges that make many of the cybersecurity issues so challenging. In short, companies must work to change the default attitudes that exist in order to place a clear and ongoing emphasis on security. Without addressing these cultural and incentive issues, companies will continue to ignore basic security best practices.

For companies, this shift entails emphasizing security throughout the entire product or service lifecycle, including: (1) planning for security early in the product development cycle, (2) taking into account the security of legacy systems, and (3) ensuring resiliency in the event of an attack. For many companies, this lifecycle approach is a significant departure from their current approach to security. In a market that stresses rapid product development and often rewards those first-to-market, there can be enormous pressure to deliver quickly at the expense of investments in cybersecurity. This pressure was evident in Facebook's early motto of "move fast and break things".[66] Importantly, Facebook also shows that companies can adjust their approach, as its motto changed in 2014 to "move fast with stable infrastructure" in order to reflect a commitment to balancing quick innovation with security and stability.[67]

A cultural shift on the part of private sector entities to better address cybersecurity would involve numerous changes, but we identify three in particular as a starting place:

66 Kelly, Samantha Murphy. "Facebook Changes its 'Move Fast and Break Things' Motto." *Mashable*. 30 April 2014. http://mashable.com/2014/04/30/facebooks-new-mantra-move-fast-with-stability/#FWTrQ4zOAsqV.

67 Id.

Adoption of best practices: There are basic steps that companies should follow that, although not a complete solution to cybersecurity issues, would have a demonstrable positive impact. Several examples of these are included in the appendix, and include:

- The CIS Critical Security Controls to enhance enterprise cybersecurity defences and incident response[68]
- The Australian Signals Directorate's list of 35 mitigation steps for reducing the risks from targeted computer network attacks, including application whitelisting, applying application and operating system patches, and enforcing a strong password policy[69]
- The UK's "10 steps to cybersecurity" covering topics such as setting user privileges, malware prevention and user education[70]

Improved authentication: Authentication is critically important for cybersecurity, and particularly challenging in the internet of things(IoT). Companies should move beyond insecure passwords to mechanisms such as two-factor authentication or multi-factor authentication that uses other forms of verification like biometric data. Online services could also enable the use of authentication technologies, including fingerprint and iris scanners, voice and facial recognition, and a variety of technologies, such as embedded Secure Elements (eSE), that help verify identities in more secure ways.[71] And companies should explore new methods of continuous authentication that continually reaffirm authentication throughout the time of access – something that will become increasingly important with the need to continually re-authenticate IoT devices connected to a network or a system.

Preparation for attacks: No one is immune from cyberattacks. It is critical that companies take steps before they are attacked. Most importantly, companies must: (1) examine and enhance their forensic capabilities to determine the scope of an attack, inform affected customers and entities, and assist law enforcement; (2) develop a business continuity plan to determine whether, how and when to continue or resume business operations after an attack; and (3) develop a plan for regaining customer trust after an attack. Waiting to do these things until after an attack has already happened will be too late.

Changing corporate culture on security is not just a one-time thing – it is a commitment that must be made repeatedly over the course of a product or company's lifecycle. Such a cultural shift is not easy, as it requires a significant investment of financial, time and human resources. During the development phase, workers must devote time and effort testing and securing existing features when that effort could be spent iterating new features. Similarly, such an investment must be remade continually over the lifecycle of the product instead of spending time on new products. In order to make this change, companies must find a balance between rapid innovation and ensuring security. Companies must also find a balance between the costs of investing in security and the ultimate cost of their products. Additionally, companies with limited resources must find the right balance between innovating new products sustainably and supporting existing devices in the future. This latter balancing will be particularly challenging in the industrial IoT, where products may be expected to remain both operational and connected for decades.

One reason why companies have not made such a culture change previously is that the financial incentives simply did not support such a change. While some companies, such as Apple, have used their investment in security as a product differentiator in selling their iOS products,[72] they have done so at a price premium, which serves to commoditize and stratify security. Changing these underlying financial incentives is not something the private sector can do on its own, which is why blended governance models that encourage collaboration between the public and private sectors will be critical.

68 "Cyber Hygiene Toolkit." *Center for Internet Security* https://www.cisecurity.org/cyber-pledge/tools.cfm; "About." Center for Internet Security http://www.cisecurity.org/about/.

69 Id.

70 United Kingdom. Government Communication Headquarters. "10 Critical 10 Steps to Cyber Security."

71 "FIDO Alliance." *FIDO Alliance Home Comments*. https://fidoalliance.org/.

72 "iOS Security" *Apple*. Sept. 2015 https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

Private Sector in Action: Cyber Insurance [73]

Although cyber insurance is frequently mentioned as a mechanism that businesses could use to mitigate cyber threats, the insurance industry has undertaken the barest of beginnings in this space. Insurance companies have to this point demonstrated little native understanding of the cyber risks posed to enterprises, making it difficult for them to offer effective products. In order to offer useful products, the insurance industry must establish a reliable way to value a company's cyber and cyber-dependent assets, beginning with data, which can include intellectual property, client/customer data and employee data. In the more traditional areas, e.g., fire, auto, home, etc., the insurance industry is the marketplace expert on risk, with centuries of actuarial data on which to base risk-pricing decisions and to guard insurers against accepting more risk than they can effectively cover.

By contrast, for cyber insurance, the risk profile is far less clear, observable and measureable. Standards are fewer and actuarial data hardly exists. Threats also come from every quarter and create unimaginable consequences – for example, when intemperate executive emails are provided to the press – that can cause considerable loss of reputation, customer loyalty and market share. However, no best practice standard exists to guide the insurance industry in gauging risk. Instead, every major insurer uses its own proprietary scheme of varying degrees of sophistication. Many insurance companies seem to treat total revenue as the primary differentiating factor for categorizing cybersecurity risk. In other words, both a small medical office with voluminous files of intimate personal data and an automated car wash chain of equivalent market value with customer financial records are assessed at the same risk level. While both kinds of data are sensitive, the obvious differences in function, business processes, regulatory requirements and risk exposures distinguish the chances or consequences of a cyber event.

Despite these challenges in assessing risk, insurance carriers have begun to heavily promote their cyber insurance products and the current insurance marketplace provides some coverage for certain specific cyber risks, such as a data breach. For cyber insurance to succeed, this model must change. Insurers must take on the challenge of realistically evaluating the cyber risks they are underwriting, including accounting for the unique cyber risk factors of individual enterprises.

B. Blended Governance

Key takeaway: It is necessary to experiment with new paradigms for distributed and collaborative governance that will enable cybersecurity challenges to be addressed jointly by the public and private sectors.

The challenges to cybersecurity underscore again and again the critical need for collaboration between the public and private sectors. However, many of the existing institutions and mechanisms for collaboration are simply inadequate. Particularly when addressing complex and quickly evolving cybersecurity threats, current approaches are often too slow, too inflexible, or too prone to distrust or dysfunction. There are, of course, exceptions, such as governments hiring "technologists-in-residence" to bridge technical gaps, public-private partnerships such as the World Economic Forum facilitating cross-sector relationships, fusion centres to coordinate public and private intelligence sharing, joint research endeavours, and more.[74]

Addressing the next evolution of cybersecurity threats requires exploring new paradigms and institutions that fundamentally retrain and readjust how the public and private sectors collaborate, and build stronger and deeper connections between them. Such approaches go beyond traditional multistakeholder governance models to build relationships that are flexible

73 Analysis based on a forthcoming work by Jane Holl Lute.

74 One of the newest of these public-private partnerships is the US Commission on Enhancing National Cybersecurity, which is composed of "top strategic, business, and technical thinkers from outside of Government" who will make detailed recommendations to Congress and the President. Fact Sheet: Cybersecurity National Action Plan." Office of the Press Secretary, The White House. 9 February 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

and can be adjusted quickly and responsively to address evolving challenges and conflicts.[75] Through working collaboratively to solve pressing problems, such partnerships can even help build reservoirs of trust between the public and private sectors that are currently lacking.

There is no one-size-fits-all model for such collaboration. Instead, effective groups remain sensitive throughout their entire lifecycle to their dynamic contextual and cultural conditions, the availability of support systems and resources, and the opportunities for and trade-offs related to inclusion, transparency and accountability. Most importantly, these groups are instrumental and dynamic, changing over time to adapt to new circumstances and needs, something that is crucial for groups addressing cybersecurity and its evolving threats.

Such blended governance approaches will build important bridges between the private sector and governments and society as a whole. For example, operating with greater input from the private sector will better enable governments to make critical and targeted investments in cybersecurity that will ultimately help change the cultural and financial incentives for cybersecurity. These investments include:

- *Procurement*: Governments can use their procurement powers to help recalibrate private sector approaches to cybersecurity by purchasing from companies that build security into the entire lifecycle of their products and services. Not only would this help change private sector attitudes but it would also improve the security of public sector systems and services.[76]

- *Research*: Governments can fund research into vulnerabilities and cybersecurity, which ultimately makes it easier and less costly for the private sector to commit to best practices and address issues early on in the process.

- *Education*: Governments can educate both the private sector about best practice and users about safe behaviour and cyber hygiene.

Governments have been particularly adept at using education to advance cybersecurity objectives. For example, Germany, Finland, the Republic of Korea, Israel, Estonia and Austria have all developed university programmes in partnership with the private sector to advance cybersecurity research and develop a new generation of experts.[77] Similarly, several countries, including the UK, Germany, and France, have all worked with the private sector to develop educational programmes to help smaller businesses understand cybersecurity threats.[78]

Public-private partnerships with civil society and academia can also help educate consumers about cybersecurity. If consumers are better educated about cybersecurity and understand the basic steps to help ensure their own security, they will be more likely to reflect that knowledge in their purchasing decisions. Consumers who practise cyber hygiene at the personal level and take their own digital security seriously may reward companies that take security seriously when purchasing products. By making security a higher priority in purchasing decisions, consumers will help the private sector view prioritizing cybersecurity as beneficial to their bottom line.

75 Verhulst, Stephen et. al. "Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem." *Centre for International Governance Innovation,* December 2014. https://www.cigionline.org/sites/default/files/gcig_paper_no5.pdf; Gasser, Urs et. al. "Multistakeholder as Governance Groups: Observations from Case Studies" *Berkman Center for Internet & Society,* 14 January 2015 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549270.

76 These investments can be substantial; the Obama Administration 2017 budget proposed spending $3.1 billion simply to start modernizing the outdated and difficult to secure IT systems that the government currently uses. Fact Sheet: Cybersecurity National Action Plan." Office of the Press Secretary, The White House. 9 February 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

77 Radunovi, Vladimir and Rüfenacht, David. "Cybersecurity Competence Building Trends." November 2015. DiploFoundation http://www.diplomacy.edu.

78 Id.

Blended Governance in Action: The Energy Sector

The energy sector is often defined by public and private sectors working in close collaboration, making it an ideal place to address cybersecurity through blended governance approaches. The energy sector manages critical infrastructure, making cybersecurity a serious concern. There have already been several high-profile cybersecurity incidents, including:

- The 2010 Stuxnet worm that destroyed nearly one-fifth of Iran's nuclear centrifuges
- The 2011 "Night Dragon" attack that stole sensitive competitive information about oil and gas field bids and operations from international oil companies
- An attack in 2012 on Saudi Arabia's Aramco that damaged 30,000 personal computers in an attempt to halt all oil production.

The threats against the energy sector are only going to get worse. According to the *Wall Street Journal*, "a survey of 625 IT executives in the US, UK, France and Germany by Intel Security and the Aspen Institute found that 48% said they think it's likely there will be a cyberattack on critical infrastructure in the next three years that will result in loss of life." To date, adversaries have generally been state-sponsored, but dissident groups and terrorist organizations continue to seek ways to cause disruption, including attacks on energy infrastructure.

The energy sector is up against two major cyber threats. The first are vulnerabilities in the information technology (IT) enterprise systems. These are vulnerabilities in the commonly used systems and tools that can affect any commercial enterprise. The approaches for addressing these threats, including best practices and cyber hygiene, are well understood.

The energy sector, also faces threats tailored to the unique operational technology (OT) that is critical to energy production and transmission. Refineries, power plants, transmission and distribution grids and pipelines all rely on specific software and other control technologies. The best ways to protect and defend these specialized systems is not nearly as well understood. Additionally, these OT systems are often difficult or expensive to upgrade as they are typically designed to run for decades. Updates or other threat mitigations can require significant coordination between customers, vendors and others.

C. Regulation and Government Leadership

Key takeaway: Carefully tailored government interventions can help tip the scales toward greater cybersecurity, but such actions must be weighed against the potential impact on innovation.

Aside from the financial and educational interventions described above, there are additional steps the public sector can take to bolster cybersecurity practices. Some approaches, while possible, would be unacceptable: establishing a strict liability regime, for example, in which companies are liable for vulnerabilities in their code would certainly incentivize companies to invest in greater cybersecurity, but it would also significantly reduce investments in innovation, make entire industries unprofitable and generally cripple businesses by rendering risk unaffordable. Similarly, mandating back-door access to encrypted devices and communications, while possible, would fundamentally weaken the security afforded by systems with encryption, introducing more risks than security. However, other government interventions can help the private sector find the right balance between cybersecurity and innovation.

One form of government intervention is through the development of carefully tailored regulations. In fact, there are already several examples of approaches to regulation, addressing several aspects of cybersecurity:

- *Data-breach notifications*: Several countries have regulations that require companies to notify customers after certain kinds of security breaches. In the US, most states have some form of security breach notification law, and in 2015 the White House proposed a national breach notification standard, though it has not yet been enacted.[79] The EU is reaching the final stages of finalizing the new General Data Protection Regulation (GDPR), set to replace the1995 Data Protection Directive, which will include a 72-hour limit for breach notifications.[80]

- *Critical infrastructure:* The EU has established provisional rules compelling critical service companies in the key industries of energy, transport, banking, financial markets, health and water supply to ensure that their digital infrastructure is resilient enough to withstand online attacks.[81] Similarly, the US National Institute of Standards and Technology's (NIST) Cyber Security Framework is designed to help organizations charged with providing the nation's financial, energy, healthcare and other critical systems to better protect their information and physical assets from cyberattack. The order established a process for identifying high-priority infrastructure and required agencies to follow a series of steps to determine the adequacy and ability of the agency to address risk.

- *Information sharing*: The NIST Cyber Security Framework directed the US Secretary of Homeland Security and the Director of National Intelligence to consistently share unclassified reports with the private sector after cyberattacks.

In addition to regulation, governments also can alter behaviour through encouraging the creation and adoption of norms. This can happen at the national, regional or global level:

- *National and regional norms:* Regional and national cybersecurity strategy statements are one mechanism through which governments can reshape norms about cybersecurity, as an articulation of consensus or aspirational principles.[82] Some of these cybersecurity strategies are targeted toward readjusting the way government agencies relate to each other on issues of cybersecurity[83] or toward improving public and private sector information sharing. Others focus on cybersecurity as a component of encouraging innovation, entrepreneurship and commercial exchange. For example, the EU's comprehensive Digital Agenda includes creating public-private partnerships to address cybersecurity as part of a broader agenda of achieving a digital single market in Europe.

- *International norms*: It can be difficult for norms at the international level to reshape behaviour in the absence of enforcement mechanisms. However, political scientist Joseph Nye has argued that even in the absence of enforcement mechanisms, countries can establish effective norms bilaterally or even unilaterally. According to Nye, bilateral agreements that bar states from attacking certain aspects of the civilian cyber infrastructure during peacetime could encourage a norm of self-restraint.[84] In some cases, new norms can even be unilateral. For example, governments may stockpile a certain set of undisclosed vulnerabilities in software for offensive use, leaving software vulnerable

79 US Government "The Personal Data Notification & Protection Act." Press Release. https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

80 "Interinstitutional File: 2012/0011 (COD)" *Council of the European Union* http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

81 European Parliament. "MEPs close deal with Council on first ever EU rules on cybersecurity." 12 July 2015. http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity.

82 *See* World Economic Forum, "Digital Economy and Cyber Security in Latin America and the Caribbean" in Cybersecurity Observatory, "Cybersecurity: Are We Ready in Latin America and the Caribbean?" 2016. https://digital-iadb.leadpages.co/publicacion-cibersecurity/ (noting how regional norms on cyber security can improve cooperation, particularly in responding to cyber threats).

83 "Cyber Security Strategy," Australian Government, 2011. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AGCyberSecurityStrategyforwebsite.pdf; "France's Strategy: Information systems defence and security," Agence Nationale de la Sécurité des Systémés d'Information, 2011. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf.

84 Nye, Joseph. "The World Needs New Norms on Cyberwarfare." *The Washington Post*, 1 October 2015. https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html.

to potential attacks were those vulnerabilities to be discovered by another party. A norm of unilaterally disclosing vulnerabilities instead of stockpiling them would serve to disarm any adversaries who had also discovered that weakness. In turn, a new international norm could emerge in which countries disclose rather than stockpile vulnerabilities.

Government interventions, from regulation and norms to authentication, often struggle to match the speed of innovation and the changing security landscape. Another challenge is that there are often tricky jurisdictional issues between a variety of potential government actors. For example, in the US, several government agencies have already attempted to unilaterally expand their authority to cover cybersecurity, including the Federal Trade Commission, the Federal Communications Commission and Department of Homeland Security. For these reasons, blended governance approaches will be critical for helping governments respond quickly, sidestep jurisdictional issues within governments and ensure that government action is informed and balanced by private sector perspectives and expertise. This will be particularly true in order to address the cross-disciplinary nature of cybersecurity in IoT, which will require a combination of skills and expertise to be brought to bear in the regulatory process. Effective government intervention will require a careful balancing between private and public interests and processes, coordination and cooperation between various actors and agencies.

Government Leadership in Action: Authentication

One example of where governments can advance cybersecurity is through supporting the creation of effective authentication systems. Governments are already the most important issuer of credentials in the physical world by issuing documents confirming identity, name, citizenship, date of birth and more. Governments can play a similar role in the digital world. The development of effective and efficient digital identity management enables the migration of economic and social interactions online, and strengthens trust-based digital services. Several countries and regions have already begun enabling the next generation of services through comprehensive national authentication and digital ID systems.

- *Estonia:* Most notably, in 2002, Estonia became one of the first countries to introduce a comprehensive national ID system.[85] From birth, Estonian citizens are given a digital birth certificate that is linked to an online health insurance account. After citizens turn 15, they apply for an electronic ID card that provides proof of identity and enables access to a wide range of government e-services, from electronic banking and shopping to encrypted email. These digital tools are increasing efficiency and are saving the time-equivalent of one working week per person.[86]

- *Japan:* After meetings with Estonian leaders, the Japanese government announced its own MyNumber National Identification system, which was launched in January 2016. The government hopes the cards will help streamline information sharing between governmental agencies administering tax, social security and disaster mitigation programmes.[87]

- *India:* In 2010, India began creation of a database of unique IDs that included the fingerprint and iris scans of all 1.2 billion residents. The country's leaders say the programme can streamline India's current bureaucratic process and help solve development problems by ensuring that the benefits of services like welfare spending reach the intended recipients. The unique identities will also allow a sizable population of poor Indians to access services like banking.[88]

85 Hammersley, Ben. "Why you should be an e-resident of Estonia." *Wired*, 4 February 2015. http://www.wired.co.uk/magazine/archive/2015/07/features/estonia-e-resident.

86 "Estonia and Finland become first in the world to digitally sign international agreement." *Estonian World*. 23 December 2013. http://estonianworld.com/technology/estonia-finland-become-first-world-digitally-sign-international-agreement/.

87 "Japan to implement ID cards following Estonia's example." *Estonian World*. 24 October 2015. http://estonianworld.com/technology/japan-to-implement-id-card-following-estonias-example/.

88 Sharma, Awol. "India Launches Project to ID 1.2 Billion People." *The Wall Street Journal*. 29 September 2010. http://www.wsj.com/articles/SB10001424052748704652104575493490951809322.

- *European Union:* The EU encourages European countries to establish digital ID systems and to also accept the digital IDs of other countries. The EU's Digital Agenda for Europe contains rules designed to encourage and support the use of digital IDs for more efficient electronic interactions between businesses, citizens and public authorities.[89]

- *United States:* Instead of creating a single, national authentication system, the US government announced a partnership with technology companies and civil society to promote the use of multiple-factor authentication and to make it easier for users to enable those protections.[90]

Many of these digital IDs, including those from Estonia[91] and the United Arab Emirates[92], have built-in public key cryptography to help secure online transactions and promote the use of the IDs in non-government applications such as banking and e-commerce. One example of this is public key infrastructure (PKI), which is a system of policies, procedures and software that helps secure data through the use of public and private cryptographic keys, enabling both secure communications and authentication.

National digital ID systems, however, are not without their risks. The systems often create a linked dossier of sensitive information about individuals ranging from voting to health documents to tax issues. Governments must ensure the security of such a vast collection of personal data. Additionally, governments must be transparent with citizens about how such information is to be used, both nationally and internationally. A failure to do either of these things will erode trust in the system.

D. Independent Security Organizations

Key takeaway: Independent security organizations can play a critical educational role, helping transform any consumer (corporate, institutional, or individual) into a high-information purchaser with respect to cybersecurity, which will reward and encourage cybersecurity best practices.

In order to change the culture and incentives relating to cybersecurity, we need both greater transparency and high-information consumers. Independent security organizations can help do both.

Transparency can be a powerful tool for reshaping the culture and incentives on cybersecurity. If companies believe they will not be held liable for producing insecure products or services, they have little incentive to secure their products, particularly if securing the product or services incurs high costs. One way to generate accountability for cybersecurity is through the creation of independent security organizations focused on cybersecurity. Such an organization would test products and services and give them a seal of approval if they meet certain, independently verified, criteria.

Such a mechanism for introducing accountability to product development is not revolutionary. Independent testing laboratories have been used previously to improve the quality of consumer electrical devices. The Underwriters Laboratories (UL) was established in 1894 as a response to the notoriously unsafe consumer electric products available at the time. The UL, as it is known, is now a global safety and certification company that analyses, tests, inspects and validates new products, ensuring they meet a certain uniform level of safety. The UL Certification mark, found on many home electrical appliances, indicates to consumers that the product has been tested and certified. The same kind of approach, a kind of CyberUL, has been suggested for advancing cybersecurity accountability.

89 "Trust Services and eID," European Commission, 2015

90 "Fact Sheet: Cybersecurity National Action Plan." Office of the Press Secretary, The White House. 9 February 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

91 Tamkivi, Sten. "Lessons from the World's Most Tech-Savvy Government," *The Atlantic*, 24 January 2014. http://www.theatlantic.com/international/archive/2014/01/lessons-from-the-worlds-most-tech-savvy-government/283341.

92 Al-Khouri, Ali M. "PKI in Government Identity Management Systems," *International Journal of Network Security & Its Applications,* 2011. http://arxiv.org/pdf/1105.6357.pdf.

Several initiatives are already under way to create various elements of a CyberUL. For example, in October 2015, the noted security expert Peiter Zatko announced plans to create the Cyber Independent Testing Laboratory (Cyber-ITL).[93] The goal of the Cyber-ITL is to quantify the security hygiene of pieces of software and to help the consumer understand how safe a piece of software is, much in the same way that a nutritional label describes the calories, fat or allergens in food.[94] The hope is that such information will help consumers, governments and businesses identify products with better cybersecurity to make informed decisions. Similarly, the US government recently announced that the Department of Homeland Security would collaborate with UL to develop the Cybersecurity Assurance Program, which will conduct tests on IoT devices to certify their security.

Just as independent product ratings in Consumers Reports help consumers make educated purchasing decisions, so, too, would a CyberUL. Having high-information consumers – across sectors – will enable better decision-making; for example, when agencies or companies are considering purchasing from a vendor, they could consult the reviews of an independent security organization. Not only would this improve the quality of purchasing decisions but it would also incentivize companies to improve their ratings of their products and services.

A CyberUL, however, is unlikely to be able to fully identify and highlight all cybersecurity gaps in every product. Software and network security is extremely complex and context-dependent, and the complexity of IoT devices will only continue to increase as those devices gain more computational power, sensors and network interfaces. In a laboratory environment with a limited amount of time, there are only so many devices and vulnerabilities that can be tested. Furthermore, it is challenging in a laboratory to simulate the real world. For example, it is difficult to simulate attacks by adversaries who may respond in unpredictable ways and it is difficult to recreate the array of interconnected systems may coexist with a device in the real world. For these reasons, CyberUL proposals are unlikely to be a panacea. However, they may still help reward and encourage good cybersecurity practices.

E. Holistic Cybersecurity Education

Key takeaway: The public and private sectors should together build and support educational programmes that bridge the knowledge gap, enabling cybersecurity professionals to address both the technical and non-technical aspects of future cybersecurity challenges and provide basic cybersecurity training to non-technical experts.

Bridging the cybersecurity knowledge gap requires improving the educational programmes for both technical and non-technical employees. For cybersecurity professionals, it is important that educational programmes provide more than just technical education. A recent report of the National Academies noted that the cybersecurity workforce needs a wide variety of non-technical skills, in addition to strong technical training.[95] Non-technical training is critical because much of cybersecurity threat prevention and response is about human behaviour. Adversaries are human and they often seek to exploit human weaknesses in addition to technical weaknesses. And when attacks succeed, they often have significant human impacts. Because cybersecurity is inherently concerned with human behaviour, it is important for cybersecurity professionals to have non-technical training in the behavioral aspects of cybersecurity. Similarly, training in the management aspects of cybersecurity – including economics, anthropology and psychology – can help cybersecurity professionals advocate for resource investments within their organization to overcome the incentive and cultural hurdles that often hinder investments in cybersecurity. Cybersecurity professionals responding to an incident may need to coordinate activities across multiple organizational elements or job functions and interact with vendors, security consultants,

93 Hesseldahl, Arik. "Famed Security Researcher Mudge Leaves Google." *re/code*. 29 June 2015. http://recode.net/2015/06/29/famed-security-researcher-mudge-leaves-google-for-white-house-gig/.

94 Knake, Robert. "Q&A with Peiter Zatko (aka Mudge): Setting Up the Cyber Independent Testing Laboratory." *Council on Foreign Relations*. 18 December 2015. http://blogs.cfr.org/cyber/2015/12/18/qa-with-peiter-zatko-aka-mudge-setting-up-the-cyber-independent-testing-laboratory/.

95 National Research Council, "Professionalizing the Nation's Cybersecurity Workforce: Criteria for Decision-Making, National Academies Press." 2013 http://www.nap.edu/download.php?record_id=18446.

law enforcement or other outside actors. These roles require more than pure technical knowledge, necessitating the development of a variety of non-technical skills.

Conversely, non-technical managers and employees increasingly need more training in cybersecurity. Although non-technical employees need not become cybersecurity professionals, they do need a basic foundation of technical knowledge and training. This basic knowledge will help these employees avoid critical security mistakes, ask managers and decision-makers the right cybersecurity questions and generally support realigning the incentives that shape cybersecurity decisions.

The public and private sectors can work to ensure that both technical and non-technical employees are given the skills they need. Currently, this holistic training is difficult to find. For example, university programmes educating cybersecurity specialists are overwhelmingly tilted toward the technical dimensions. To address this, the public and private sectors should collaborate to develop and support programmes that will address these knowledge gaps. Working together, the private sector can identify the cybersecurity skills that technical and non-technical employees need, and the public sector can offer courses through public institutions that develop those skills.

5. CONCLUSION

The stakes for cybersecurity have never been higher. With increased data centralization in remote data centres, expanding reliance on cloud computing, the explosion of the IoT, and the growth in both the number and severity of cyberattacks, cybersecurity must be addressed throughout business, industry, government and civil society.

The challenge of addressing cybersecurity should not, and cannot, be addressed by the private or public sectors acting alone or independently. Ultimately, actors across sectors, industries, backgrounds and experiences will need to work together in novel ways that may seem difficult given the trust deficits in today's security ecosystem.

There are steps that companies and government can take immediately to reduce the threats, including the implementation of best practices and cyber hygiene. However, it is equally important for the public and private sectors to understand why their counterparts often struggle to take these steps. This report tries to bridge that gap, to help the public and private sectors better understand the systemic challenges each other faces, and then move past those barriers to change. In order to change the culture and incentives that make addressing cybersecurity so difficult, the public and private sectors must work together to rebuild trust, improve communication, knowledge and information sharing, and more.

Cybersecurity is a complex, quickly evolving field, and there is no silver bullet or turnkey solution that will solve all of these challenges today. Moreover, even if there were, there is no guarantee that such solutions would be equally effective against emergent threats. Ultimately, a combination of these potential solutions will need to be applied and adjusted over time to address these significant issues.

APPENDIX A

Basic Cyber Hygiene

1 Know what is connected to your network

2 Properly configure key security settings

3 Properly manage user accounts and settings to limit unauthorized access

4 Install timely patches to applications and operating systems

5 Automate and monitor the foregoing to keep foundation cybersecurity posture current

Drawn from: Center for Internet Security, Cyber Hygiene Toolkit,
https://www.cisecurity.org/cyber-pledge/tools.cfm

Australia's 35 Strategies to Mitigate Targeted Cyber Intrusions

1 Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including DLL files, scripts and installers.

2 Patch applications, e.g., Java, PDF viewers, Flash, web browsers and Microsoft Office. Patch or mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.

3 Patch operating system vulnerabilities. Patch or mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system. Avoid Windows XP.

4 Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.

Once organizations have implemented the Top 4 mitigation strategies, first on the computers of users who are most likely to be targeted by cyber intrusions and then on all computers and servers, additional mitigation strategies can be selected to address security gaps until an acceptable level of residual risk is reached.

5 User application configuration hardening, disabling the running of internet-based Java code, untrusted Microsoft Office macros, and undesired web browser and PDF viewer features.

6 Automated dynamic analysis of email and web content run in a sandbox to detect suspicious behavior, including network traffic, new or modified files, or configuration changes.

7 Operating system generic exploit mitigation mechanisms, e.g., Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).

8 Host-based Intrusion Detection/Prevention System to identify anomalous behaviour such as process injection, keystroke logging, driver loading and persistence.

9 Disable local administrator accounts to prevent network propagation using compromised local administration credentials that are shared by several computers.

10 Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication by Microsoft Active Directory.

11 Multi-factor authentication especially implemented for remote access or when the user is about to perform a privileged action or access a sensitive information repository.

12 Software-based application firewall, blocking incoming network traffic that is malicious or otherwise unauthorized, and denying network traffic by default.

13 Software-based application firewall, blocking outgoing network traffic that is not generated by whitelisted applications, and denying network traffic by default.

14 Non-persistent virtualized sandboxed trusted operating environment, hosted outside the organization's internal network, for risk activities such as web browsing.

15 Centralized and time-synchronized logging of successful and failed computer events with automated immediate log analysis, storing logs for at least 18 months.

16 Centralized and time-synchronized logging of allowed and blocked network events with automated immediate log analysis, storing logs for at least 18 months.

17 Email content filtering allowing only business-related attachment types. Preferably analyse/convert/sanitize links, PDF and Microsoft Office attachments.

18 Web content filtering of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.

19 Web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.

20 Block spoofed emails using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organization's domain.

21 Workstation and server configuration management based on a hardened Standard Operating Environment with unrequired functionality disabled, e.g. IPv6, autorun and LanMan.

22 Antivirus software using heuristics and automated internet-based reputation ratings to check a program's prevalence and its digital signature's trustworthiness prior to execution.

23 Deny direct internet access from workstations by using an IPv6-capable firewall to force traffic through a split DNS server, an email server or an authenticated web proxy server.

24 Server application security configuration hardening e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.

25 Enforce a strong passphrase policy covering complexity, length and expiry, and avoiding both passphrase re-use and the use of a single dictionary word.

26 Removable and portable media control as part of a data-loss prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.

27 Restrict access to Server Message Block (SMB) and NetBIOS services running on workstations and on servers where possible.

28 User education, e.g., internet threats and spear-phishing socially-engineered emails. Avoid weak passphrases, passphrase re-use, exposing email addresses and unapproved USB devices.

29 Workstation inspection of Microsoft Office files for potentially malicious abnormalities, e.g., using the Microsoft Office File Validation or Protected View features.

30 Signature-based antivirus software that primarily relies on up-to-date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.

31 TLS encryption between email servers to prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.

32 Block attempts to access web sites by their IP address instead of by their domain name, e.g., implemented using a web proxy server, to force cyber adversaries to obtain a domain name.

33 Network-based Intrusion Detection/Prevention System using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.

34 Gateway blacklisting to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous internet users.

35 Capture network traffic to/from internal critical-asset workstations and servers, as well as traffic traversing the network perimeter, to perform post-intrusion analysis.

From: http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf

United Kingdom: Reducing the Cyber Risk in 10 Critical Areas

1 Information risk-management regime

2 Secure configuration

3 Network security

4 Managing user privileges

5 User education and awareness

6 Incident management

7 Malware prevention

8 Monitoring

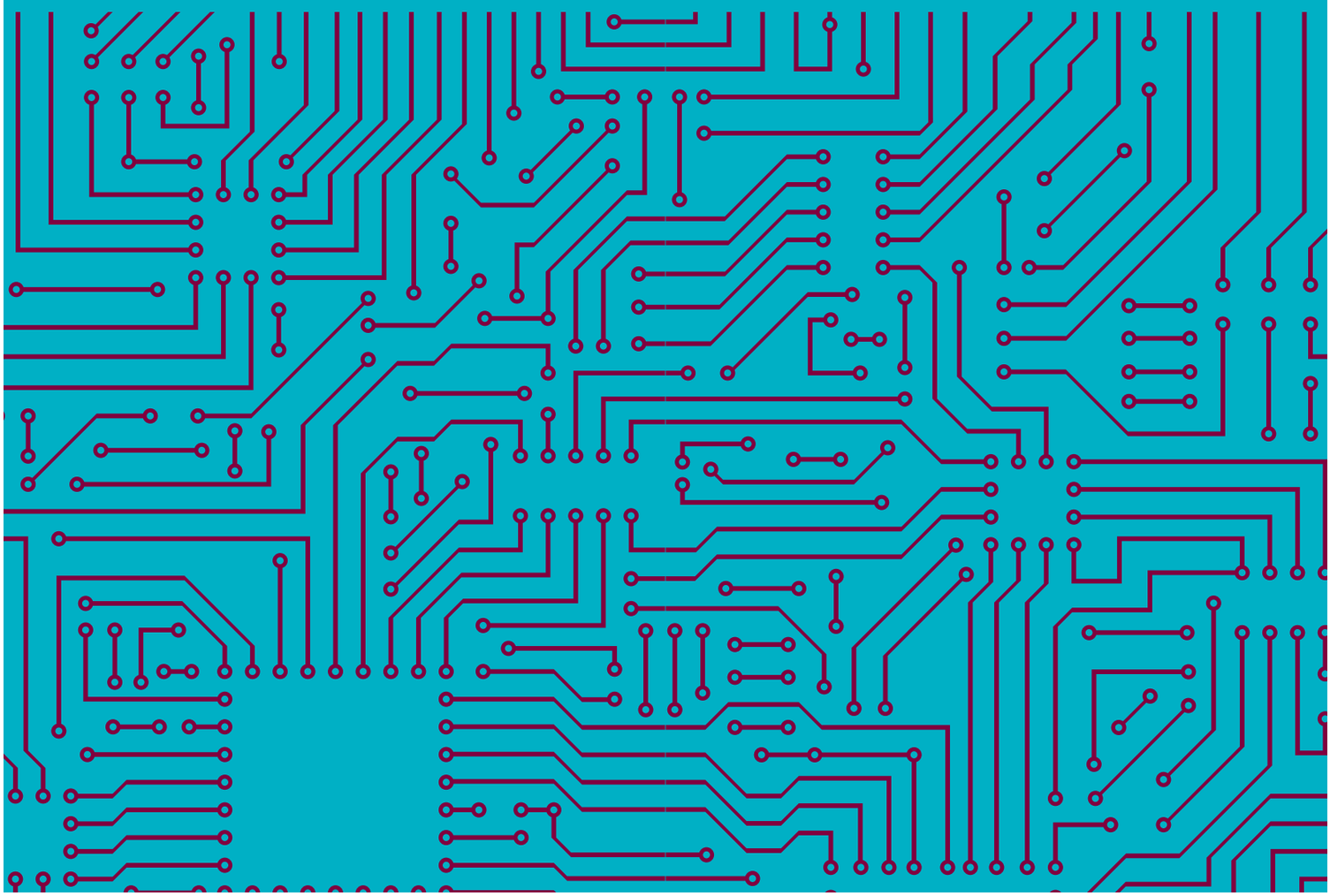
9 Removable media controls

10 Home and mobile working

From: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf

12 THE OPPORTUNITIES AND RISKS OF THE INTERNET OF THINGS: PERSPECTIVES FOR ACTION

Dutch Cyber Security Council



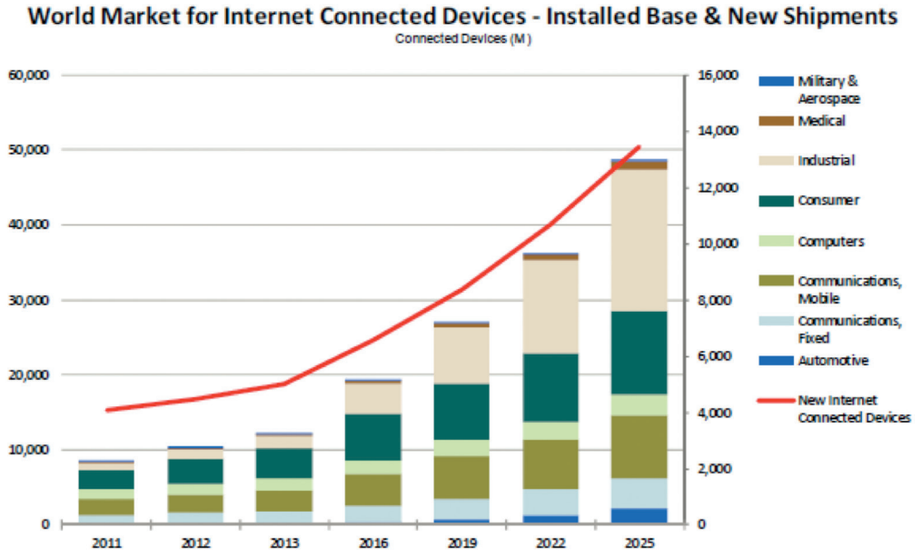
CSR Cyber Security Council

The CSR advises the government on various strategic cyber security issues. The Council focuses on the most prominent future technological developments and cyber security consequences. To exploit opportunities and mitigate risks, the digital resilience of individuals, organizations and society should be increased. The Internet of Things heightens the tensions around these issues.

It is important to raise awareness among citizens, businesses and governments regarding the opportunities and risks of the IoT. Good cooperation and swift exchange of knowledge and information between public and private parties and science at national and international level, is of great importance.

INTRODUCTION

The Internet of Things (IoT) is an emerging trend that affects all areas of our economy and society. Everyday objects are becoming connected to networks and databases and thus can exchange data. Due to the IoT, the possibility arises to combine physical objects and the virtual world. Think of a motor vehicle involved in an accident that warns the emergency services itself, a washing machine that automatically detects that it is leaking and signals the repair unit, or a sensor that knows exactly where your pet is. The IoT is not just about consumer technology and the provision of services, it is also about the basic architecture of the Internet and industrial applications in healthcare, logistics, commerce, education, and so on. Often, the focus of IoT seems to be at the level of communication between machine and consumer, however, machine-to-machine communication is at least as important. Many manufacturers are now working on developing applications and platforms in the area of IoT. These new applications include all kinds of technologies, such as sensors, biometric readers, microphones and speakers. Because existing issues in security and privacy seem to be more urgent in our digitalizing society, the IoT brings with it new challenges. Through the possibility of infinitely linking devices, we are creating new dependencies and interdependencies. This phenomenon will have unknown effects, making it difficult to estimate potential security risks.

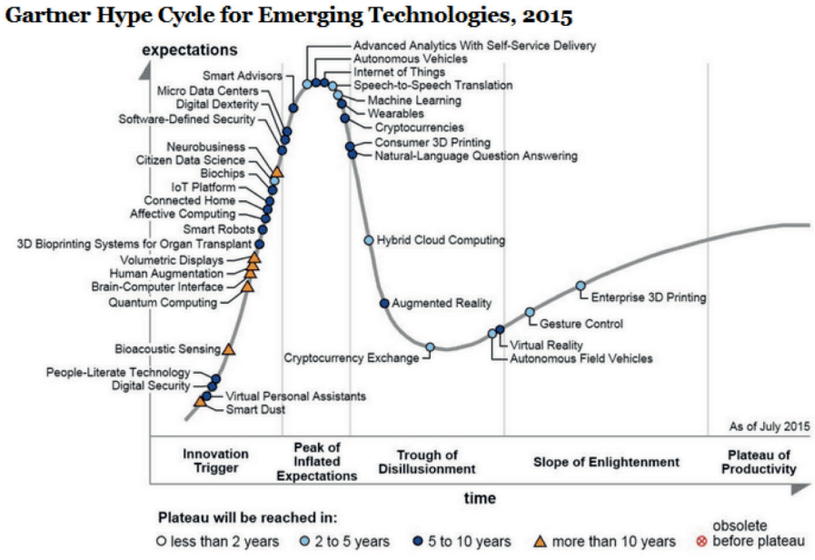


Bron: blog.echelon.com: bit.ly/1T3VsFJ

The IoT is networked technology of the near future that connects all digital devices to the internet:

- networked technologies are omnipresent, meaning that they will be located everywhere and form an ecosystem in which ownership is hard to discern due to the broad spectrum of actors and links;
- networked technologies can communicate and operate independently from user intervention:
- networked technologies are context-aware and proactive, they can offer users personalized services, such as delivering information and entertainment based on personal preferences in a way that is relevant and appropriate to the context of the user, such as their geographical GPS location.

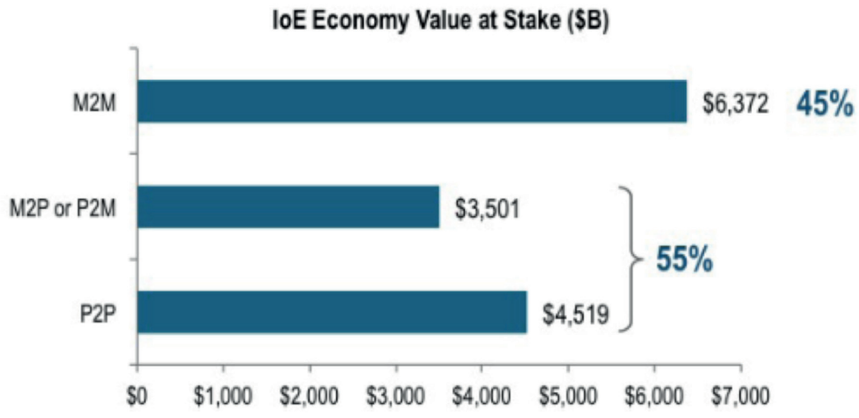
The IoT brings opportunities, such as living comfort, efficient operations, innovation (e-health) and it creates new forms of employment. However, the IoT also brings certain risks and dilemmas. This raises the question of what possible actions are there to facilitate the chances of IoT, and to mitigate and reduce these to acceptable levels? If we do not answer these questions and let IoT developments come over us, guidance on the safe implementation of the IoT in society will be hardly possible.



Source: Gartner

OPPORTUNITIES

The rise of IoT is an unstoppable trend and source of innovation for the economy and society. The economic benefits of IoT are big. Cisco (2015) estimates that the implementation of IoT in the European public sector and private sector will bring 2.1 and 4.3 trillion dollars in economic advantage respectively. Other studies estimate that the global economic value for businesses and private industry to be in the range of 1.9 to 14.4 trillion dollars by 2020. Cybersecurity and privacy are important preconditions for exploiting these opportunities.



Source: Cisco IBSG, 2013

The IoT brings four specific opportunities:

1. Living comfort

The IoT can make life easier and more comfortable. Consumers may continue to benefit in several ways. Companies may offer products that are customized to the specific preferences of their consumers. Products and services can be tailored and personalized much more to the preferences of consumer. Since the IoT is a new source of innovation and competition, it offers opportunities and new possibilities for smart living. The use of using mobile devices for controlling heating, lighting, and temperature are a great example of how IoT will affect users at home.

Samsung introduces a smart washing machine. This machine does not have the traditional buttons and knobs, but only a touchscreen. This is in fact compatible with the recently launched Samsung Smart Home Protocol. This app makes it possible to operate all domestic Samsung devices with your smartphone. The machine is also equipped with a number of sensors. These sensors allow smartphone users to understand the quantity, material and dirtiness of their own laundry. http://www.wasmachines.nl/nieuws/samsung-introduceert-slimme-wasmachine/

2. Efficient management

Using IoT applications enables companies to improve their processes. Consider the real-time monitoring by sensors. This allows a business to intervene quickly when necessary. IoT applications also make it possible to map logistic chains in detail and to optimize inventory management and distribution patterns. A third example of process efficiency is the automatic irrigation of arable land by smart sprayers. Weather sensors may also be implemented to indicate agricultural machines that the farmer-land is too dry.

3. Innovation

The IoT can be a driving force for innovation, through new technological applications. A key example can be seen in the health sector. The IoT offers patients and other health consumers the possibility to better understand their health with real-time monitoring of their blood pressure, heart rate and the blood sugar level. A smart-watch that collects these data, can map the life of its user in great detail.

4. New forms of employment

While the emphasis of the public debate often focusses on the disappearance of certain kinds of jobs; other forms of employment will also emerge from the rising trend of IoT. This shift can be seen in the short term with the growing need for data analysts to make optimum use of the data being collected by the IoT. Additionally, there will also be a need for security experts, software specialists and engineers as they are needed to respond effectively to the opportunities and threats of the IoT.

One of the busiest highways in the UK will be equipped with sensors and become a "smart highway." The road which contains sensors, can keep track of the amount of traffic by interacting with passenger mobile phones. According to the Guardian, this technology does not use mobile networks, it uses frequencies that are in between television channels. A centralized system will have the capability to adjust the speed limit of the highway based on the traffic density. In the near future, the system could also directly communicate with self-driving cars in order to redirect them. The speed of self-driving cars could even be adjusted, enables telecom watchdog organizations. http://www.nu.nl/tech/3592102/slim-me-weg-groot-brittannie-kan-met-autos-communiceren.html

RISKS

In addition to the opportunities listed before, the IoT also brings potential risks. These risks mainly concern issues regarding security and privacy . These perceived risks can be clustered into five categories:

1. Manageability

The IoT playing field is vast, limitless and has a complex composition of international, national and regional contributors making it difficult to shape controllability. For example, a local service can have a strong international character. The IoT field often misses oversight and an insight into who is responsible for what. For example, a local provider in the Netherlands can store client data in a cloud, however, this data may be hosted in another country and would thus apply different laws and regulation to those data than those applicable in the Netherlands.

Nest is the smart thermostat from Google. Thousands of people could no longer change the temperature in their home by default in the cloud component. This underlines a growing dependence on IoT. This gives way to globalized interdependence as while the gas supply and the boiler work fine, home users may have no heating in their homes due to a software failure on another continent. http://www.nu.nl/gadgets/4195396/urenlange-storing-bij-slimme-huisapparatuur-van-nest.html

2. Lack of security incentives

There is a lack of incentives to produce secure hardware, software and maintenance. For the vast majority of manufacturers, low cost prices are more important than the security of the product. A short time-to-market and the addition of new features comes at the expense of implementing adequate security mechanisms. IoT devices are small and inexpensive, making them difficult to patch. They often have little to no update capabilities. This lack of security-by-design does not have legal nor financial consequences for manufacturers, enabling a situation where it is not economically rewarding to improve the situation. The damage of compromised security will be borne by other stakeholders and by society at large. Given the lifespan of these devices and their high costs, replacement is not a logical choice for consumers. The continuity of networks, enterprises and society is affected by IoT devices that can hardly be patched. Manufacturers have insufficient incentives to design their products with security in mind.

At the start of their research, Ethical Hackers Charlie Miller and Chris Valasek tried to hack the multimedia system of a Jeep Cherokee through Wi-Fi connection as Chrysler, the manufacturer of the vehicle, was offering this option on subscription. As Miller and Valasek found out, it is not that difficult to hack this car's Wi-Fi as the password is generated automatically, based on the time the car and its multimedia system, also its head unit, is turned on for the very first time. https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/

The quality of software is often limited. Developers design their own implementations of the most basic components without testing their code extensively thus rendering it to be easily manipulated and exploited by potential attackers.

By using Shodan, an open-source search engine that searches for vulnerable devices, is able to find access links to poorly protected baby monitoring webcams and can also find more serious vulnerabilities such as exploitable process control systems. If these vulnerabilities fall into the wrong hands, the consequences could be disastrous. This underlines the current threats and vulnerabilities of IoT as the majority of the devices are unboxed with default passwords, thus rendering these devices vulnerable to common exploits.

3. Impact on behavior

The large amount of IoT devices makes it possible to collect and analyze large amounts of data, providing users with more data that is tailored to their personal needs and uses. Although this is part of the major benefits of IoT technology, it also possesses a downside to the user's freedom of choice. IoTs are part of what is known as the so-called "persuasive technologies". The amount of data on human behavior is a new form of intelligence, which can influence and human behavior without anyone noticing and without underlying transparent interests. Insight on the use of IoT and its consequences should be done with the consent of the user and with their freedom of choice in mind.

4. Surveillance and industrial espionage

The large number of devices that will be connected to the Internet in the near future presents new avenues for the communication to be intercepted and monitored by governments and malicious parties. Targeted surveillance and spying are becoming much easier to achieve as unprotected devices are intrinsically easy to hack. Vulnerable devices are a major gateway to access recorded communication and real-time information. Digital espionage is becoming increasingly more difficult to counter as a problem and digital investigations and prosecution are amounting to be complex matters as often, the culprits of espionage are state actors. Most digital espionage focuses on business information and intellectual property. Protecting intellectual property is of great importance to the Dutch economy. The question of encryption is also not an easy matter as it touches upon the "privacy vs. security" debate and thus encompasses various societal interests.

Though James Clapper did not name any specific agency as being involved in surveillance via smart-home devices in congressional testimony, he stated that it was a possibility. As increasing numbers of devices connect to the internet and to each other, the so-called internet of things promises consumers increased convenience, such as the Nest (see par.1). But as home computing migrates away from the laptop, the tablet and the smartphone, experts warn that the security features on the coming wave of automobiles, dishwashers and alarm systems lag far behind. http://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

5. Big Data and privacy

The current privacy legislation is under pressure of the rise of Big Data. The purpose limitation principles of the current privacy laws are at odds with the uses of Big Data. It is currently unclear whether the majority of the data collected by IoT devices are covered or not by existing data protection laws. It is difficult to determine the concerns of personal data. That does mean, however, that this data provides a huge insight into the daily lives of end-users, especially when several data streams from multiple devices are connected. Citizens do not know where their data is stored .The terms of use for data storage services are not

sufficiently clear and explicit, creating the potential risk of loss of confidence amongst end-users.

Taiwan-based computer hardware maker ASUSTeK Computer Inc. has agreed to a legal case with the settle Federal Trade Commission on charges that critical security flaws in its routers put the home networks of hundreds of thousands of consumers at risk. The administrative complaint also stipulates that the routers' insecure cloud services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal information on the open internet. The proposed consent order will require ASUS to establish and maintain a comprehensive security program subject to independent audits for the next 20 years.https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

ACTION PERSPECTIVES

In order to facilitate opportunities for IoT issues and mitigate risks, various perspectives can be explored. Prior to the release of new devices, much can be improved by investing in the production of the quality of products and in services. This includes the fulfillment of the relevant duties of care. After releasing devices, monitoring of compliance with the duties of care and product liability, must be properly organized.

1. Awareness

For businesses, organizations and government, awareness can be enhanced by developing and practicing (emergency) scenarios to determine the risks and opportunities of the community. Creating awareness does not mean that the user is to blame for everything that goes wrong in the (production) chain. The chain should take responsibility and fulfill the duties of care towards the end-user. With the implementation of cybersecurity measures and taking their own responsibilities into account, users can rely on a secure and prosperous digital future. Information campaigns can help raise awareness in society and a begin a comprehensive public debate with citizens, businesses, researchers and other relevant parties on where the balance lies between security, freedom and the digital economy.

2. Transparency

It must be clear to the user what the security level of a product or service is. It should also be clear for what purpose information is being collected and where it is stored, and what is it being used for.

Users themselves should have access to what data they can delete or edit. By setting up a monitoring function on IoT networks, better detection mechanisms can aid in mitigating the risks association with these devices, thus leading to improvement measures. Manufacturers need to be transparent about the risks inherent to their products. Also, supervisory authorities should broaden and deepen their expertise in order to incorporate cybersecurity to their activities.

3. Standards and labels

In the IoT landscape, cybersecurity and privacy should be key issues in the delivery of products and services. Manufacturers can connect to previously existing standards in this area and issue assurances for customers. New standards are being developed and they should contain cybersecurity and privacy from the beginning, enabling security and privacy-by-design. The same standard applies to the realization of interoperability, for example, over open sources The use of such open standards improves technical interoperability and boosts the market as it reduces the risk of vendor-lock-in by manufacturers with proprietary standards. Organizations such as the IEEE IETF are working on open standards. The risk still exists that manufacturers work with proprietary standards, which now often occurs at the device level. In addition to this, more and more organizations are using cloud providers. The IoT will generally be based on this infrastructure, thus sufficient attention is needed for securing cloud computing. There are voices that emphasizing the development of certified quality logos to enable manufacturers . The question is whether the label is connected to the process or product. One of the set backs of such a label is the rapid pace of technological

developments, as it is difficult to keep the standards up to date in such a volatile environment. The question of an effective and reliable label should be thoroughly explored.

4. Liability

Distinction should be made in regards to duty of care and product liability. Duties of care are applicable prior to the launch of a product. This may include security and privacy-by-design. The government can help protect businesses and consumers by changing institutional frameworks around liability, including legislation, monitoring and law enforcement. Duties of care should be arranged in such order that it also covers new developments and insights in advance.

Product liability applies after launching a product, which guarantees tailored IoT applications and services. Liability can be arranged for compensation.

Duties of care and product liability can be incentives for manufacturers to make their products as digitally secure as possible in that point in time. An extra incentive can be the possibility of a cyber risk insurance that can be issued if manufacturers have their affairs in order and can prove to be implementing security and privacy solutions in to the design and production of their products. The responsibility for cyber security should no longer be passed on to the end-user by technology manufacturers.

5. Intermediary liability

ISPs and other internet intermediaries might provide natural control points to fight security issues associated with IoT. Equipment is accessing the Internet through an access provider, for example. It is technically traceable which ISP or network operator provides access to a device or individual. When these devices are involved in attacks on people, companies etc., measures could be taken by the intermediaries. Discussions with the ISPs and other intermediaries could clarify their potential role in this ecosystem. This should fit within the legal framework. More generally, it seems sensible to agree to examine the applicable laws and regulations. A question worth pondering is whether current legislation sufficiently focuses on the new IoT developments.